Installation Guide for the Cisco 1120 Secure Access Control Server 4.2

License and Warranty
April 2009

Americas 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: 408 527-0883

Text Part Number: OL-19455-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Installation Guide for the Cisco 1120 Secure Access Control Server 4.2
© 2003–2009 Cisco Systems, Inc. All rights reserved

CONTENTS

Preface

This guide describes how to install and initially configure the Cisco 1120 Secure Access Control Server (CSACS 1120), and includes upgrade, and migration information for the Cisco 1111, Cisco 1112, and Cisco 1113 platforms. It also details administrative functions that you can perform from the command line interface. This guide covers the CSACS-1120-K9 hardware platform also referred to as the CSACS 1120 version. Throughout this guide, the term CSACS 1120 refers to the Cisco 1120 Secure Access Control System Series appliance, and the term ACS refers to the ACS 4.2 software.

Warranty, service, and support information is located in the *Cisco Information Packet* that shipped with your appliance.

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:

- Preface
- Chapter 1, “Cisco 1120 Secure Access Control Server Overview”
- Chapter 2, “Preparing for Installation”
- Chapter 3, “Installing and Configuring the Cisco 1120 Secure Access Control Server 4.2”
- Chapter 4, “Administering the Cisco 1120 Secure Access Control Server”
- Chapter 5, “Upgrading and Migrating to Cisco 1120 Secure Access Control Server”
- Appendix A, “Site Log”
- Appendix B, “Windows Service Advisement”
- Appendix C, “Command Reference”
- Appendix D, “Troubleshooting”
- Appendix E, “Maintaining the Cisco 1120 Secure Access Control Server”

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.

Safety Warnings

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, might harm you. A warning symbol precedes each warning statement. The safety warnings provide safety guidelines that you should follow when working with any equipment that connects to electrical power or telephone wiring. Included in the warnings are translations in several languages. For detailed information about compliance guidelines and translated safety warnings, see *Regulatory Compliance and Safety Information for the Cisco 1120 Secure Access Control Server 4.2*.

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

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. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

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. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡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. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

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. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

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!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

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、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel **VIGTIGE SIKKERHEDSANVISNINGER**

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير **إرشادات الأمان الهامة**

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.

قم بحفظ هذه الإرشادات

Upozorenje **VAŽNE SIGURNOSNE NAPOMENE**

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění **DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY**

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie

DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Documentation Updates

Table 1 Updates to Installation Guide for the Cisco 1120 Secure Access Control Server 4.2

Date	Description
12/10/2009	• Added a note in LEDs • Added a note in Front-Panel LEDs
12/07/2009	• Updated the table Front-Panel LEDs • Updated the table Front-Panel LED Descriptions
11/12/2009	• Updated NIC 1 and NIC 2 LEDs • Updated NIC 1 and NIC 2 LED Descriptions

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 4.2	• Printed document with the product. • PDF on the product CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/roadmap/DGuide42.html
User Guide for Cisco Secure Access Control Server 4.2	• PDF on the ACS Recovery CD-ROM. • You can also access the user guide by clicking **Online Documentation** in the ACS navigation menu. The user guide PDF is available on this page by clicking **View PDF**. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/ACS4_2UG.html
Configuration Guide for Cisco Secure ACS 4.2	• PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs42_config_guide.html

Table 2 Product Documentation (continued)

Document Title	Available Formats
Installation Guide for Cisco Secure ACS for Windows 4.2	• PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/IGwn42.html
Installation Guide for Cisco Secure ACS Solution Engine 4.2	• PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/solution_engine/SE42.html
Installation and User Guide for Cisco Secure ACS User Changeable Passwords 4.2	• PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/user_passwords/ucpNW42.html
Installation and Configuration Guide for Cisco Secure ACS Remote Agents 4.2	• PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/remote_agent/RA42.html
Installation Guide for the Cisco 1120 Secure Access Control Server 4.2	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/csacs_1120/csacs1120_4.2.html
Cisco Secure Access Control Server Troubleshooting Guide	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/trouble/guide/ACSTrbG42.html
Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine 4.2	• Shipped with product. • PDF on the product CD-ROM. • Printed document available by order (part number DOC-7817259). • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/regulatory/compliance/RCSI_42.html
Regulatory Compliance and Safety Information for the Cisco 1120 Secure Access Control Server 4.2	• Shipped with the product. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/regulatory/compliance/ACS1120_RCSI_42.html

Table 2 Product Documentation (continued)

Document Title	Available Formats
Supported and Interoperable Devices and Software Tables for Cisco Secure ACS 4.2	• PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/device/guide/sdt42.html
Release Notes for Cisco Secure ACS 4.2	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/release/notes/ACS42_RN.html
Online Documentation	In the ACS HTML interface, click Online Documentation.
Online Help Help topics for all pages in the ACS HTML interface.	In the ACS HTML interface, online help appears in the right pane when you are configuring a feature.
Short help	Select an option from the ACS web interface; the help appears in the right pane.

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.

For more information, or for additional information about the CSACS 1120, see:

- Regulatory Compliance and Safety Information for the Cisco 1120 Secure Access Control Server 4.2.
- Release Notes for the Cisco Secure Access Control Server 4.2.
- Supported and Interoperable Devices and Software Tables for the Cisco Secure Access Control Server4.2.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Cisco 1120 Secure Access Control Server Overview

This chapter gives a functional overview of the Cisco 1120 Secure Access Control Server, hereafter referred to as CSACS 1120. This chapter covers the appliance hardware, major components, controls, connectors, and front- and rear-panel LED indicators.

This chapter contains:

System Description

The Cisco 1120 Secure Access Control Server (CSACS 1120) 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+). CSACS 1120 controls the authentication, authorization, and accounting (AAA) of users accessing corporate resources through the network.

You use CSACS 1120 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.

CSACS 1120 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. CSACS 1120 includes additional features specific to operating and managing the ACS appliance.

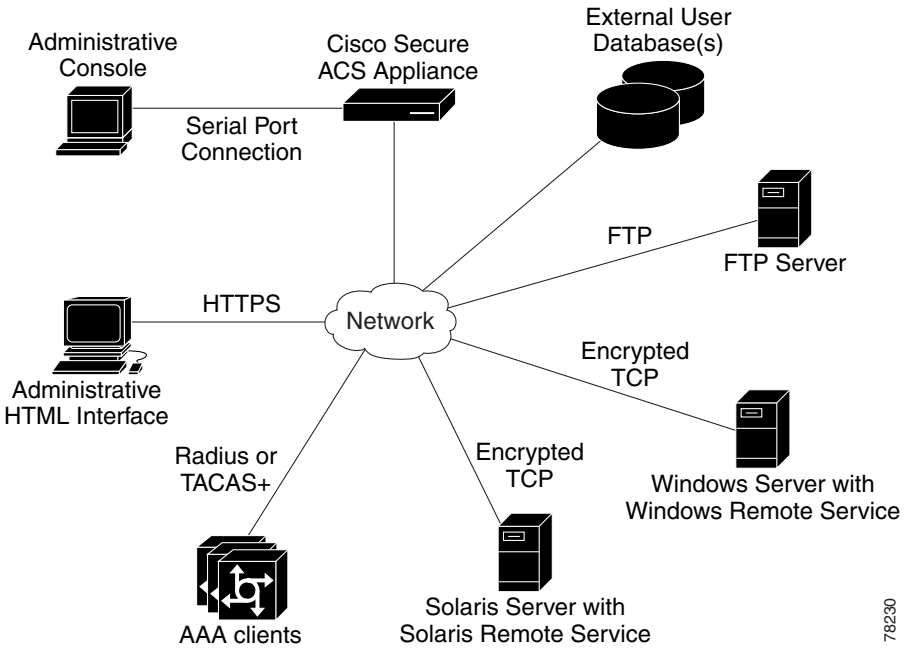
To ensure a highly secure posture, CSACS 1120:

- 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 CSACS 1120 operating context.

Figure 1-1 CSACS 1120 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.

Product Overview

This section describes the power requirements, rack-mount hardware kit, and features of the CSACS 1120 Series appliance.

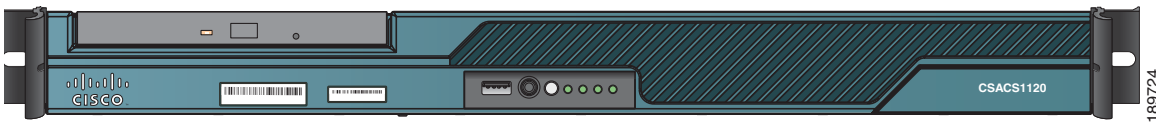
This section contains:

- Specifications for the CSACS 1120 Series Appliance, page 1-3
- Product Serial Number Location, page 1-4
- Cisco Product Identification Tool, page 1-4

Specifications for the CSACS 1120 Series Appliance

The CSACS 1120 Series appliance (see Figure 1-2) is contained in a standard shelf-rack enclosure. The appliance weighs from 15 lb (9.071 kg) to 33 lb (14.96 kg) depending on what options are installed in the appliance. It measures 1.69 inches high x 17 inches wide x 20 inches deep (4.29 cm x 43.18 cm x 50.80 cm). These dimensions do not include the rack handles.

Figure 1-2 Cisco 1120 Secure Access Control System Front View



The CSACS 1120 Series appliance is configured for AC-input power and has a single auto-ranging AC-input power supply, mounted in a standard 19-inch (48.3 cm), 4-post equipment rack (using the rack-mount brackets provided). The CSACS 1120 features include:

- Microprocessor—Intel Core 2 Duo 2.13-GHz processor with an 800-MHz front side bus (FSB) and 2 MB of Layer 2 cache.
- Four synchronous dynamic RAM (SDRAM) slots that support up to 4 GB.
- Support for up to 2 x 250-GB SATA hard drives.
- Two fixed RJ-45 10BASE-T/100BASE-TX/1000BASE-T network interface connectors (located on the rear panel).
- One slimline DVD-ROM drive (located on the front-panel).
- One DB-9 serial (console) port (located on the rear-panel).
- Front-to-rear airflow blowers using two 40-mm exhaust fans and ducting for the CPU and memory, two 40-mm exhaust fans built into the power supply, and one PCI exhaust fan.
- Expansion slot support—One PCI-X (located on the rear panel).
- Three USB 2.0 ports (two located on the rear panel, one on the front-panel).
- One PS/2 keyboard port (located on the rear panel).
- One PS/2 video monitor port (located on the rear panel).
- One DB-15 serial (video) port (located on the rear panel).
- Rear-access cabling.

- Four green, front-panel appliance LEDs:
  - Power (indicates whether the power supply is operational).
  - Hard disk drive activity (indicates whether the drive is functioning properly).
  - Network Interface connector (NIC) 1 and NIC 2 activity (indicates whether interrupts or packet transfers are running).

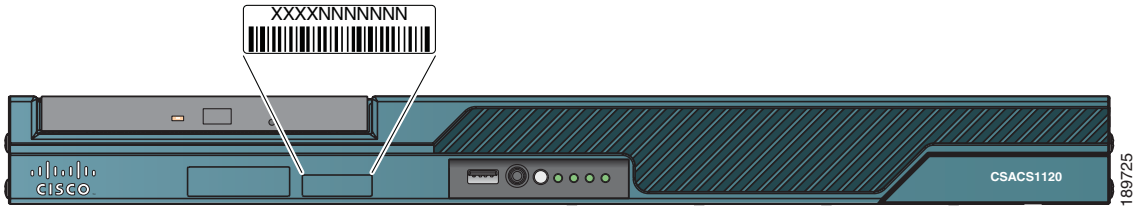
  For a description of the LEDs, see CSACS 1120 Appliance Front-Panel View, page 1-5.
- The CSACS 1120 appliance is normally shipped with a rack-mount hardware kit which includes either brackets or rails that allow the CSACS 1120 to be positioned in a 4-post equipment rack. For more information, see Chapter 3, "Installing the Cisco 1120 Secure Access Control System Hardware."

Note The rack-mount hardware kit does not include a 2-post equipment rack.

Product Serial Number Location

The serial number label is located on the front-panel of the CSACS 1120 Series appliance, at the lower Left. Figure 1-3 shows the location of this label.

Figure 1-3 CSACS 1120 Appliance Serial Number Location



Note The serial number for the CSACS 1120 Series appliance is 11 characters long.

Cisco Product Identification Tool

The Cisco Product Identification (CPI) tool helps you retrieve the serial number of your Cisco products.

Before you submit a request for service online or by phone, use the CPI tool to locate your product serial number. You can access this tool from the Cisco Support website.

To access this tool:

Step 1 Click the **Get Tools & Resources** link.

Step 2 Click the **All Tools (A-Z)** tab.

Step 3 Select **Cisco Product Identification Tool** from the alphabetical drop-down list.

This tool offers three search options:

- Search by product ID or model name.

- Browse for Cisco model.
- Copy and paste the output of the **show** command to identify the product.

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 you place a service call.

You can access the CPI tool at:

http://tools.cisco.com/Support/CPI/index.do

To access the CPI tool, you require 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:

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

Hardware Features

This section describes the front- and rear-panel controls, ports, and LED indicators on the CSACS 1120 Series appliance.

This section contains:

- CSACS 1120 Appliance Front-Panel View, page 1-5
- CSACS 1120 Appliance Back-Panel View, page 1-6
- Input/Output Ports and Connectors, page 1-8

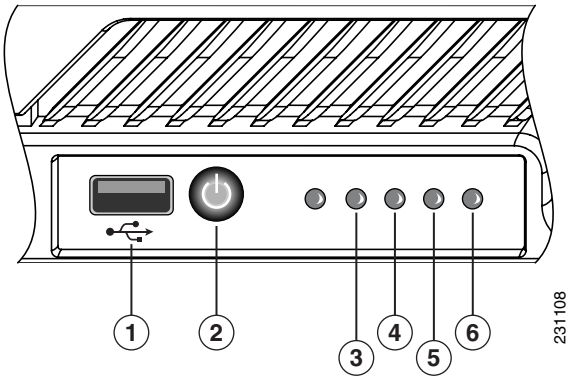
CSACS 1120 Appliance Front-Panel View

The front-panel of the CSACS 1120 Series appliance contains:

- USB 2.0 port
- Power button
- Various LEDs (appliance and NICs)

Figure 1-4 shows the components of the front-panel.

Figure 1-4 CSACS 1120 Series Appliance Front View



The following table describes the callouts in Figure 1-4.

1	USB port	**4**	Hard disk drive activity LED
2	Power button	**5**	NIC 1 LED
3	Appliance power LED	**6**	NIC 2 LED

LEDs

Table 1-1 describes the LEDs located on the front-panel of the CSACS 1120 Series appliance.

Table 1-1 Front-Panel LEDs

LED	Color	State	Description
Appliance power	Green	On	Power on
	Green	Blinking	Sleep (standby)
	Off	Off	Power off
Hard disk drive	Green	Random blinking	Hard disk drive activity
	Off	Off	No hard disk drive activity
NIC 1 and NIC 2	Green	On	NIC link, no access
	Green	Blinking	LAN access

Note Since ACS does not support Sleep (standby) mode, LED for Sleep (standby) is not applicable.

CSACS 1120 Appliance Back-Panel View

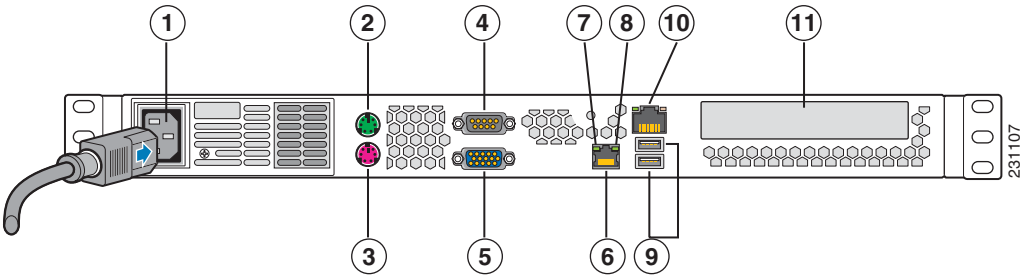
The back panel of the CSACS 1120 Series appliance contains:

- AC power connector
- Two PS/2 connectors (video monitor and keyboard)
- One serial (DB-9) connector
- One video connector
- Two NIC (RJ-45) ports
- Two USB 2.0 ports
- One PCI adapter card slot (expansion slot)
- NIC LEDs

Figure 1-5 shows the components of the back panel.

Note The locations of the rack-mounting brackets are also shown on the left and right sides of the appliance. (See Rack-Mounting Configuration Guidelines, page 3-1 for instructions on how to install the mounting brackets.)

Figure 1-5 CSACS 1120 Series Appliance Rear View



The following table describes the callouts in Figure 1-5

1	AC power receptacle	**7**	NIC 2 port LED (activity)
2	PS/2 connector (video monitor)	**8**	NIC 2 port LED (link)
3	PS/2 connector (keyboard)	**9**	Two USB 2.0 ports
4	Serial (EIA/TIA-232) console port	**10**	NIC 1 port (10/100/1000 Mb/s) or Ethernet 0
5	Video Graphics Array (VGA) port	**11**	PCI adapter card slot (expansion)
6	NIC 2 (10/100/1000 Mb/s) port or Ethernet 1		

Note ACS must use only the NIC 1 port on the appliance. Using NIC 2 may lead to software configuration problems.

LEDs

The back panel of the CSACS 1120 Series appliance contains LEDs that indicate the connection activity and speed of the NIC ports. Figure 1-6 shows these LEDs.

Figure 1-6 NIC 1 and NIC 2 LEDs

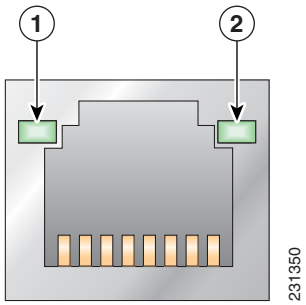


Table 1-2 describes the activity and connection speed associated with each LED state.

Table 1-2 NIC 1 and NIC 2 LEDs

LED	Color	State	Description
Left (1)	—	Off	No network connection
	Amber	Solid	Network connection
	Amber	Blinking	Transmit/receive activity
Right (2)	—	Off	10-Mb/s connection (if left LED is on or blinking)
	Amber	Solid	1000-Mb/s connection
	Green	Solid	100-Mb/s (or 1-Gb/s) connection

Input/Output Ports and Connectors

The back panel of the CSACS 1120 Series appliance supports the following types of I/O connectors:

- Ethernet
- Serial
- Video monitor
- Keyboard

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

Ethernet Port (NIC 1 and NIC 2)

The CSACS 1120 Series appliance comes with two integrated dual-port Ethernet controllers. These controllers provide an interface for connecting to 10-Mb/s, 100-Mb/s, or 1000-Mb/s networks and provide full-duplex (FDX) capability, which enables simultaneous transmission and reception of data on the Ethernet LAN.

To access the Ethernet port, connect a Category 3, 4, 5, 5E, or 6 unshielded twisted-pair (UTP) cable to the RJ-45 connector on the back of the appliance.

Table 1-3 describes the UTP cable Categories.

Table 1-3 Ethernet Cabling Guidelines

Type	Description
10BASE-T	EIA Categories 3, 4, or 5 UTP (2 or 4 pair) up to 328 ft (100 m)
100BASE-TX	EIA Category 5 UTP (2 pair) up to 328 ft (100 m)
1000BASE-T	EIA Category 6 UTP (recommended), Category 5E UTP or 5 UTP (2 pair) up to 328 ft (100 m)

Ethernet Port Connector

Figure 1-7 shows the Ethernet RJ-45 port and plug.

Figure 1-7 RJ-45 Port and Plug

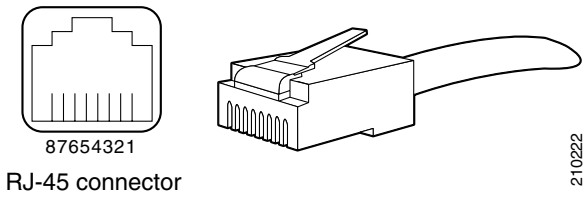


Table 1-4 lists and describes the RJ-45 pin signals used on the connector.

Table 1-4 Ethernet Port Pinout

Ethernet Port Pin	Signal	Description
1	TxD+	Transmit data +
2	TxD–	Transmit data –
3	RxD+	Receive data +
4	Termination network	No connection
5	Termination network	No connection
6	RxD–	Receive data –
7	Termination network	No connection
8	Termination network	No connection

Serial (Console) Port

The CSACS 1120 Series appliance has one standard serial (console) port. Use the configuration or setup utility program to change the port address assignments.

Note The configuration or setup utility program is located in the CSACS 1120 Series appliance ROM and can be accessed through the serial (console) port.

Serial (Console) Port Connector

The CSACS 1120 Series appliance has one serial port connector located on the back panel of the appliance.

Figure 1-8 shows the pin number assignments for the 9-pin, male D-shell serial port connector located on the back panel of the appliance. These pin number assignments conform to industry standards.

Figure 1-8 Serial Port Connector

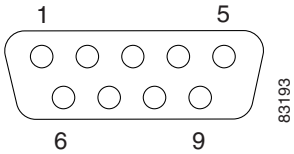


Table 1-5 lists and describes the serial (console) port pinout.

Table 1-5 DB-9 Serial (Console) Port Pinout

Serial Port Pin	Signal	Description
1	DCD	Carrier Detect
2	DSR	Data Set Ready
3	RXD	Receive Data
4	RTS	Request To Send
5	TXD	Transmit Data
6	CTS	Clear To Send
7	DTR	Data Terminal Ready
8	RI	Ring Indicator
9	GND	Ground

Environmental Monitoring

The CSACS 1120 Series appliance has protection circuits that monitor and detect overcurrent, overvoltage, and overtemperature conditions inside the appliance. If the power supply shuts down, or latches off, an AC cycle switches off for 15 seconds and switches on for 1 second to reset the power supply.

This section contains:

- Overcurrent Protection (OCP), page 1-10
- Overvoltage Protection (OVP), page 1-11
- Overtemperature Protection (OTP), page 1-11

Overcurrent Protection (OCP)

The power supply shuts down and latches off after an overcurrent condition occurs. This latch is cleared by an AC power interruption.

Note The power supply will not be damaged from repeated power cycling.

Overvoltage Protection (OVP)

The power supply shuts down and latches off after an overvoltage condition occurs. This latch is cleared by an AC power interruption.

Overtemperature Protection (OTP)

The power supply is protected against overtemperature conditions caused by the loss of fan cooling or excessive ambient temperature. In an OTP condition, the power supply will shut down. When the power supply temperature drops to the rated safety limit, the power supply restores power automatically.

Regulatory Compliance

For regulatory compliance and safety information, see *Regulatory Compliance and Safety Information for the Cisco 1120 Secure Access Control Server 4.2*. This document is available online at Cisco.com:

For more information, see Obtaining Documentation and Submitting a Service Request, page -xv.

CHAPTER 2

Preparing for Installation

This chapter describes the safety instructions, site requirements, and tasks you must perform before installing the CSACS 1120 Series appliance.

This chapter contains:

Note Read the *Regulatory Compliance and Safety Information for the Cisco 1120 Secure Access Control Server 4.2* and the *Site Preparation and Safety Guide* that came with your CSACS 1120 Series appliance before you begin the installation.

Safety Guidelines

Before you begin installing the CSACS 1120 Series appliance, review the safety guidelines in this chapter and Rack-Mounting Configuration Guidelines, page 3-1 to avoid injuring yourself or damaging the equipment.

In addition, before replacing, configuring, or maintaining the appliance, review the safety warnings listed in Safety Warnings, page viii and in the *Cisco Regulatory Compliance and Safety Information for the Cisco 1120 Secure Access Control Server 4.2* document.

This section contains:

General Precautions

Observe the following general precautions for using and working with your appliance:

- Observe and follow service markings. Do not service any Cisco product except as explained in your appliance documentation. Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock. Components inside these compartments should be serviced only by an authorized service technician.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part, or contact your authorized service provider:
  - The power cable, extension cord, 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.
- Keep your appliance away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your appliance, and never operate the product in a wet environment.
- Do not push any objects into the openings of your appliance. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with other equipment approved by Cisco.
- Allow the product to cool before removing covers or touching internal components.
- Use the correct external power source. Operate the product only from the type of power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service representative or local power company.
- Use only approved power cables. If you have not been provided with a power cable for your appliance or for any AC-powered option intended for your appliance, purchase a power cable that is approved for use in your country. The power cable must be 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 appliance and 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. If you must use an extension cord, use a three-wire cord with properly grounded plugs.
- Observe extension cord and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cord or power strip does not exceed 80 percent of the extension cord or power strip ampere ratings limit.
- Do not use appliance, or voltage converters, or kits sold for appliances with your product.
- To help protect your appliance from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position cables and power cords carefully; route cables and the power cord and plug so that they cannot be stepped on or tripped over. Be sure that nothing rests on your appliance cables or power cord.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local or national wiring rules.

Safety with Equipment

The following guidelines will help ensure your safety and protect the equipment. However, this list does not include all potentially hazardous situations, so be *alert*.

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

- Always disconnect all power cords and interface cables before moving the appliance.
- Never assume that power is disconnected from a circuit; *always* check.
- Keep the appliance chassis area clear and dust-free before and after installation.
- Keep tools and assembly components away from walk areas where you or others could trip over them.
- Do not work alone if potentially hazardous conditions exist.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Do not wear loose clothing that may get caught in the appliance chassis.
- Wear safety glasses when working under conditions that may be hazardous to your eyes.

Safety with Electricity

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 **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.** Statement 1021

Warning **Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.** Statement 4

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

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.** Statement 12

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

Warning **This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.** Statement 39

Warning **When installing or replacing the unit, the ground connection must always be made first and disconnected last.** Statement 1046

Follow these guidelines when working on equipment powered by electricity:

- Locate the room's emergency power-off switch. Then, if an electrical accident occurs, you can quickly turn off the power.
- Disconnect all power before doing the following:
  - Working on or near power supplies.
  - Installing or removing an appliance.
  - Performing most hardware upgrades.
- Never install equipment that appears damaged.
- Carefully examine your work area for possible hazards, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Never assume that power is disconnected from a circuit; *always* check.
- Never perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Never work alone when potentially hazardous conditions exist.
- If an electrical accident occurs, proceed as follows:
  - Use caution, and do not become a victim yourself.
  - Turn off power to the appliance.
  - If possible, send another person to get medical aid. Otherwise, determine the condition of the victim, and then call for help.
  - Determine whether the person needs rescue breathing, external cardiac compressions, or other medical attention; then take appropriate action.

In addition, use the following guidelines when working with any equipment that is disconnected from a power source but still connected to telephone wiring or network cabling:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for it.
- Never touch uninsulated telephone wires or terminals unless the telephone line is disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. ESD can occur when electronic printed circuit cards are improperly handled and can cause complete or intermittent failures. Always follow ESD-prevention procedures when removing and replacing modules:

- 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 appliance. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads.
- Ensure that the CSACS 1120 Series appliance is electrically connected to earth ground.
- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the appliance to channel unwanted ESD voltages safely to ground. To guard against ESD damage and shocks, the wrist strap and cord must operate effectively.
- If no wrist strap is available, ground yourself by touching a metal part of the appliance.

Caution For the safety of your equipment, periodically check the resistance value of the antistatic wrist strap. It should be between 1 and 10 Mohm.

Lifting Guidelines

The CSACS 1120 Series appliance weighs between 15 lb (9.071 kg) and 33 lb (14.96 kg) depending on what hardware options are installed in the appliance. The appliance is not intended to be moved frequently. Before you install the appliance, ensure that your site is properly prepared so you can avoid having to move the appliance later to accommodate power sources and network connections.

Whenever you lift the appliance or any heavy object, follow these guidelines:

- Always disconnect all external cables before lifting or moving the appliance.
- Ensure that your footing is solid, and balance the weight of the object between your feet.
- Lift the appliance slowly; never move suddenly or twist your body as you lift.
- Keep your back straight and lift with your legs, not your back. If you must bend down to lift the appliance, bend at the knees, not at the waist, to reduce the strain on your lower back muscles.
- Lift the appliance from the bottom; grasp the underside of the appliance exterior with both hands.

Preparing Your Site for Installation

Before installing the CSACS 1120 Series appliance, it is important to prepare the following:

1. Prepare the site (see Site Planning, page 2-6) and review the installation plans or method of procedures (MOPs).
2. Unpack and inspect the appliance.
3. Gather the tools and test equipment required to properly install the appliance.

This section contains:

Site Planning

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

Typically, you should have prepared the installation site beforehand. As part of your preparation, obtain a floor plan of the site and the equipment rack where the CSACS 1120 Series appliance will be housed. Determine the location of any existing appliances and their interconnections, including communications and power. Following the airflow guidelines (see Airflow Guidelines, page 2-8) ensures that adequate cooling air is provided to the appliance.

All personnel involved in the installation of the appliance, including installers, engineers, and supervisors, should participate in the preparation of a MOP for approval by the customer. For more information, see Method of Procedure, page 2-9.

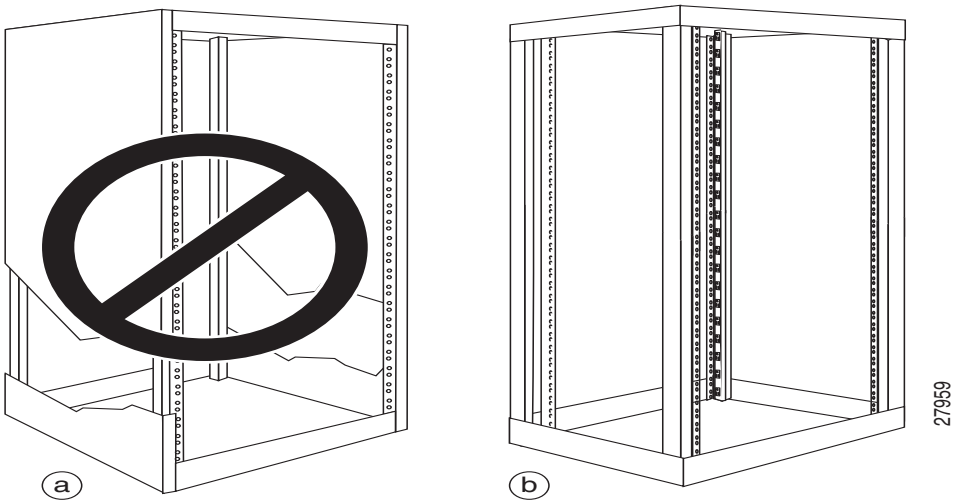
The following sections provide the site requirement guidelines that you must consider before installing the appliance:

Rack Installation Safety Guidelines

The CSACS 1120 Series appliance can be mounted in most 4-post (telco-type), 19-inch equipment racks that comply with the Electronics Industries Association (EIA) standard for equipment racks (EIA-310-D). The rack must have at least two posts with mounting flanges to mount the appliance. The distance between the center lines of the mounting holes on the two mounting posts must be 18.31 inches +/- 0.06 inch (46.50 cm +/- 0.15 cm). The rack-mounting hardware included with the appliance is suitable for most 19-inch equipment racks or telco-type frames.

Figure 2-1 shows examples of a 4-post (telco-type) equipment racks.

Figure 2-1 Equipment Rack Types



Enclosed Rack (Do Not Use)

Figure 2-1a shows a freestanding, enclosed rack with two mounting posts in the front. The CSACS 1120 Series appliance should *not* be installed in this type of enclosed rack, because the appliance requires an unobstructed flow of cooling air to maintain acceptable operating temperatures for its internal components. Installing the appliance in any type of enclosed rack—*even with the front and back doors removed*—could disrupt the airflow, trap heat next to the appliance, and cause an overtemperature condition inside the appliance.

4-Post (Open) Rack

Figure 2-1b shows a freestanding, 4-post open rack with two mounting posts in front and two mounting posts at the back. The mounting posts in this type of rack are often adjustable so that you can position the rack-mounted unit within the depth of the rack rather than flush-mount it with the front of the rack.

Before installing your CSACS 1120 Series appliance in a rack, review the following guidelines:

- Two or more people are required to install the appliance in a rack.
- Ensure that the room air temperature is below 95°F (35°C).
- Do not block any air vents; usually, 6 inches (15 cm) of space provides proper airflow.
- Plan the appliance installation starting from the bottom of the rack.
- Do not extend more than one appliance out of the rack at the same time.
- Connect the appliance to a properly grounded outlet.
- Do not overload the power outlet when installing multiple devices in the rack.
- Do not place any object weighing more than 110 lb (50 kg) on top of rack-mounted devices.

Site Environment

The location of your appliance and the layout of your equipment rack or wiring room are extremely important considerations for proper operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause malfunctions and shutdowns, and can make maintenance difficult. Plan for access to front- and rear-panels of the appliance.

The following precautions will help you plan an acceptable operating environment for your appliance and will help you avoid environmentally caused equipment failures:

- Ensure that the room where your appliance operates has adequate circulation. Electrical equipment generates heat. Without adequate circulation, ambient air temperature may not cool equipment to acceptable operating temperatures. For more information, see Airflow Guidelines, page 2-8.
- Ensure that the site of the rack includes provisions for source AC power, grounding, and network cables.
- Allow sufficient space to work around the rack during the installation. You need:
  - At least 3 feet (9.14 m) adjacent to the rack to move, align, and insert the appliance.
  - At least 24 inches (61 cm) of clearance in front of and behind the appliance for maintenance after installation.
- To mount the appliance between two posts or rails, the usable aperture (the width between the *inner* edges of the two mounting flanges) must be at least 17.7 inches (45.0 cm).

Note The rack-mount kit does not include a 2-post equipment rack.

- Use appropriate strain-relief methods to protect cables and equipment connections.
- To avoid noise interference in network interface cables, do not route them directly across or along power cables.
- Always follow ESD-prevention procedures as described in Preventing Electrostatic Discharge Damage, page 2-5 to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.

Airflow Guidelines

To ensure adequate airflow through the equipment rack, it is recommended that you maintain a clearance of at least 6 inches (15.24 cm) at the front and the rear of the rack. If airflow through the equipment rack and the appliances that occupy it is blocked or restricted, or if the ambient air being drawn into the rack is too warm, an overtemperature condition within the rack and the appliances that occupy it can occur.

The site should also be as dust-free as possible. Dust tends to clog the appliance fans, reducing the flow of cooling air through the equipment rack and the appliances that occupy it. This reduction increases the risk of an overtemperature condition.

Additionally, the following guidelines will help you plan your equipment rack configuration:

- Besides airflow, you must allow clearance around the rack for maintenance.
- When mounting an appliance in an open rack, ensure that the rack frame does not block the front intakes or the rear exhausts.

Temperature and Humidity Guidelines

Table 2-1 lists the operating and non-operating environmental site requirements for the CSACS 1120 Series appliance. The appliance normally operates within the ranges listed; however, a temperature measurement approaching a minimum or maximum parameter indicates a potential problem. Maintain normal operation by anticipating and correcting environmental anomalies before they approach critical values by properly planning and preparing your site before you install the appliance.

Table 2-1 Operating and Nonoperating Environmental Specifications

Specification	Minimum	Maximum
Temperature, ambient operating	50°F (10°C)	95°F (35°C)
Temperature, ambient nonoperating and storage	-40°F (°C)	158°F (70°C)
Humidity, ambient (noncondensing) operating	10%	90%
Humidity, ambient (noncondensing) nonoperating and storage	5%	95%
Vibration, operating	5–500 Hz, 2.20 g RMS random	—

Power Considerations

You configure the CSACS 1120 Series appliance with AC-input power only. Ensure that all power connections conform to the rules and regulations in the National Electrical Codes (NECs), as well as local codes. When planning power connections to your appliance, the following precautions and recommendations must be followed:

- Check the power at your site before installation and periodically after installation to ensure that you are receiving clean power (free of spikes and noise). Install a power conditioner if necessary.
- The AC power supply includes the following features:
  - Autoselect feature for 110-V or 220-V operation.
  - An electrical cord for all appliances. (A label near the power cord indicates the correct voltage, frequency, current draw, and power dissipation for the appliance.)

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).** Statement 13

- Install proper grounding to your host equipment rack to avoid damage from lightning and power surges.

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

- The AC-input power supply that operates on input voltage and frequency within the ranges of 100 to 240 VRMS and 50/60 Hz without the need for operator adjustments.

Method of Procedure

As described previously, part of your preparation includes reviewing installation plans or MOPs. An example of a MOP (a pre-installation checklist of tasks and considerations that need to be addressed and agreed upon before proceeding with the installation) is as follows:

1. Assign personnel.
2. Determine protection requirements for personnel, equipment, and tools.
3. Evaluate potential hazards that may affect service.

4. Schedule time for installation.
5. Determine any space requirements.
6. Determine any power requirements.
7. Identify any required procedures or tests.
8. On an equipment plan, make a preliminary decision that locates each CSACS 1120 Series appliance that you plan to install.
9. Read this hardware installation guide.
10. Verify the list of replaceable parts for installation (screws, bolts, washers, and so on) so that the parts are identified.
11. Check the required tools list to make sure the necessary tools and test equipment are available. For more information, see Required Tools and Equipment, page 2-12.
12. Perform the installation.

Unpacking and Checking the Contents of Your Shipment

The shipping package for the CSACS 1120 Series appliance is designed to reduce the possibility of product damage associated with routine material handling experienced during shipment. To reduce the potential for damage to the product, transport the appliance in its original Cisco packaging. Failure to do so may result in damage to the appliance. Also, do not remove the appliance from its shipping container until you are ready to install it.

The appliance, cables, and any optional equipment you ordered may be shipped in more than one container. When you unpack the containers, check the packing list to ensure that you received all the parts listed in Table 2-2. A *Notes* section has been provided to record damaged or missing items.

Note Do not discard the packaging materials used in shipping your CSACS 1120 Series appliance. You will need the packaging materials in the future if you move or ship your appliance.

Table 2-2 CSACS 1120 Series Appliance Packing List

✓	Item	Cisco Part Number
❑	Cisco 1120 Secure Access Control Server Series appliance	CSACS-1120-K9
❑	4-post server rack-mount kit (for kit contents, see 4-Post Rack-Mount Hardware Kit, page 3-3.)	CSACS-1U-RAILS
❑	*Cisco Information Packet*	78-5235-03G0
❑	Cisco 90-Day Limited Hardware Warranty Terms	78-5236-01C0
❑	*Regulatory Compliance and Safety Information for the Cisco 1120 Secure Access Control Server 4.2*	78-19077-01
❑	*Installation Guide for the Cisco 1120 Secure Access Control Server 4.2*	OL-19455-01
Notes		

Table 2-2 CSACS 1120 Series Appliance Packing List

✓	Item	Cisco Part Number

Inspect all items for shipping damage. If anything appears to be damaged, or if you encounter problems installing or configuring your appliance, contact your customer service representative.

Note The rack-mount kit does not include a 2-post equipment rack.

Cisco Information Packet and Warranty

The *Cisco Information Packet* provides warranty, service, and support information.

To access and download the *Cisco Information Packet* and your warranty and license agreements from Cisco.com:

Step 1 Launch your Internet browser and go to:

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

The Warranties and License Agreements page appears.

Step 2 To read the *Cisco Information Packet*:

a. Click the **Information Packet Number** field, and ensure that the part number 78-5235-03G0 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.

Note You must have Adobe Acrobat Reader to view and print PDF files. You can download the reader from the Adobe website.

Step 3 To read translated and localized warranty information about your product:

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 PDF.

Step 4 You can also contact the Cisco Service and Support website for assistance at:

http://www.cisco.com/en/US/support/

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 the 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 which 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 and website location	—
Product model number	—
Product serial number[1]	—
Maintenance contact number	—

1. See the "Product Serial Number Location" section on page 1-3 and the "Product Serial Number Location" section on page D-7 for more information.

Required Tools and Equipment

Caution The fastener pack in the rack-mount kit, contains eight rack screws. You must check these screws to ensure that they are the appropriate size for the holes in your rack. Using the wrong-sized screws for your threaded rack holes can damage the rack.

You need the following tools and equipment to install the CSACS 1120 Series appliance in a 4-post rack:

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

- ESD-preventive cord and wrist strap.
- Number 2 Phillips screwdriver.

- Flat-blade screwdrivers (small, 3/16-inch (0.476 cm) and medium, 1/4-inch [0.625 cm]) to remove the cover if you are upgrading memory or other components.
- Rack-mount Kit. For more information on kit contents, see 4-Post Rack-Mount Hardware Kit, page 3-3.
- Cables for connection to the LAN ports (depending on the configuration).
- Ethernet hub or PC with a network interface card for connection to the Ethernet (LAN) port or ports.
- Console terminal (an ASCII terminal or a PC running terminal-emulation software) that is configured for 9600 baud, 8 data bits, no parity, 1 stop bit, and no hardware flow control.
- Console cable for connection to the serial (console) port. A null-modem cable is recommended.

Installation Checklist

To assist you with your installation and to provide a historical record of what was done, and by whom, use the following installation checklist. Make a copy of this checklist and mark the entries as you complete each task. When the checklist is completed, include a copy of it for each CSACS 1120 Series appliance in your site log (see Creating a Site Log, page 2-14 for information about creating a site log) along with other records for your new appliance.

Installation Checklist for Site:

CSACS 1120:

Task	Verified by	Date
Installation checklist copied	—	—
Background information placed in site log	—	—
Site power voltages verified	—	—
Installation site power check completed	—	—
Required tools availability verified	—	—
Additional equipment availability verified	—	—
CSACS 1120 Series appliance received	—	—
Cisco Information Packet publication received	—	—
Appliance components verified	—	—
Initial electrical connections established	—	—
ASCII terminal (for local configuration) verified	—	—
Signal distance limits verified	—	—
Startup sequence steps completed	—	—
Initial operation verified	—	—

Creating a Site Log

The site log (see Appendix A, "Site Log"for a sample site log) provides a record of all actions related to installing and maintaining the CSACS 1120 Series appliance. Keep the log in an accessible place near the appliance so that anyone who performs tasks has access to it. Use the installation checklist (see Installation Checklist, page 2-13) to verify the steps in the installation and maintenance of your appliance. Site Log entries might include the following:

- Installation progress—Make a copy of the appliance installation checklist, and insert it into the site log. Make entries as you complete each task.
- Upgrade, removal, and maintenance procedures—Use the site log as a record of ongoing appliance maintenance and expansion history. Each time a task is performed on the appliance, update the site log to reflect the following information:
  - Installation of new adapter cards.
  - Removal or replacement of adapter cards and other upgrades.
  - Configuration changes.
  - Maintenance schedules and requirements.
  - Maintenance procedures performed.
  - Intermittent problems.
  - Comments and notes.

Ethernet and Console Port Considerations

There are two network interface connectors (NIC 1 and NIC 2) on the rear panel of the CSACS 1120 Series appliance. Both ports use UTP cable. Cisco recommends Category 5 UTP cable. The maximum segment distance is 328 feet (100 meters). The UTP cables look like the cables used for ordinary telephones; however, UTP cables meet certain electrical standards that telephone cables do not. Cables are not included.

Note The ACS Server must use only the NIC 1 port on the appliance. Using NIC 2 it may lead to software configuration problems.

The appliance includes an asynchronous serial console port, which enables you to access the appliance locally (using a console terminal). This section describes important cabling information that must be considered before connecting a console terminal—either an ASCII terminal or a PC running terminal-emulation software—to the console port.

Note The console cable is not included with the CSACS 1120 Series appliance.

This section contains:

NIC 1 and NIC 2 (RJ-45) Ethernet Connections

The NIC 1 and NIC 2 connections support 10BASE-T, 100BASE-TX, and 1000BASE-T standards. The transmission speed of the Ethernet ports is autosensing by default and is user configurable.

Figure 1-6 shows the pin orientation of the RJ-45 Ethernet port and the modular cable plug it accepts.

Note The ACS Server must use only the NIC 1 port on the appliance. Using NIC 2 may lead to software configuration problems.

Console Port Connections

The console port on the CSACS 1120 Series appliance includes an EIA/TIA-232 asynchronous serial (DB-9) connector. This serial console connector (port) allows you to access the appliance locally by connecting a terminal—either a PC running terminal-emulation software or an ASCII terminal—to the console port.

To connect a PC running terminal-emulation software to the console port, use a DB-9 female to DB-9 female null-modem cable.

To connect an ASCII terminal to the console port, use a DB-9 female to DB-25 male straight-through cable with a DB-25 female to DB-25 female gender changer. The default parameters for the console port are 9600 baud, 8 data bits, no parity, 1 stop bit, and no hardware flow control.

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

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.

CHAPTER 3

Installing and Configuring the Cisco 1120 Secure Access Control Server 4.2

This chapter describes how to install your CSACS 1120 Series appliance and connect it to the network.

This chapter contains:

Before you begin the installation, read the *Regulatory Compliance and Safety Information for the Cisco 1120 Secure Access Control Server 4.2* and the *Site Preparation and Safety Guide* that is shipped with your appliance.

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

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

Rack-Mounting Configuration Guidelines

Each CSACS 1120 Series appliance has a set of rack handles (installed at the factory). You will use these handles later when you install the appliance in a 4-post rack. You can front (flush) mount or mid-mount the appliance in a 19-inch (48.3-cm) equipment rack that conforms to the 4-post rack specification (the inside width of the rack should be 17.5 inches [44.45 cm]). Mount the appliance in the brackets. When the appliance is installed in the rack, it requires one EIA 1.75-inch (4.4-cm) vertical mounting space or 1 rack unit (RU) for mounting.

Caution You must leave clearance in the front and rear of the CSACS 1120 Series appliance, to allow cooling air to be drawn in through the front and circulated through the appliance and out the rear of the appliance.

The Rack Installation Safety Guidelines, page 2-6 and the following information will help you plan the equipment rack configuration:

- When mounting an appliance in an equipment rack, ensure that the rack is bolted to the floor.
- Because you may install more than one appliance in the rack, ensure that the weight of all the appliances installed does not make the rack unstable.

Caution Some equipment racks are also secured to ceiling brackets due to the weight of the equipment in the rack. If you use this type of installation, make sure that the rack you are using to install the appliances is secured to the building structure.

- As mentioned in Airflow Guidelines, page 2-8, maintain a 6-inch (15.2-cm) clearance at the front and rear of the appliance to ensure adequate air intake and exhaust.
- Avoid installing appliances in an overly congested rack. Air flowing to or from other appliances in the rack might interfere with the normal flow of cooling air through the appliances, increasing the potential for overtemperature conditions within the appliances. For more information about overtemperature conditions, see Overtemperature Protection (OTP), page 1-10.
- Allow at least 24 inches (61 cm) of clearance at the front and rear of the rack for appliance maintenance.

Caution To prevent appliance overheating, never install an appliance in an enclosed rack or a room that is not properly ventilated or air conditioned.

- Follow your local practices for cable management. Ensure that cables to and from appliances do not impede access for performing equipment maintenance or upgrades.

Note The rack-mount hardware kit does not include a 2-post equipment rack.

Mounting the CSACS 1120 Series Appliance in a 4-Post Rack

Warning **When the appliance is installed in a rack and is fully extended on its slide rail, it is possible for the rack to become unstable and tip over, which could cause serious injury. To eliminate the risk of rack instability from extending the rail or in the event of an earthquake, you should affix the rack to the floor.**

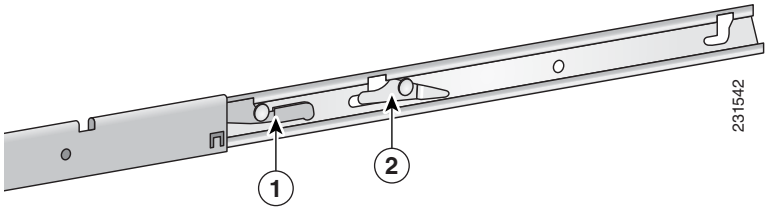
This section contains:

- 4-Post Rack-Mount Hardware Kit
- Installing the Slide Rails into a Rack with Square Holes
- Installing the Slide Rails into a Rack with Round Holes
- Installing the Appliance into the Slide Rails

4-Post Rack-Mount Hardware Kit

Figure 3-1 shows the rails and release levers that you need to install the CSACS 1120 Series appliance in a 4-post rack.

Figure 3-1 Release Levers on the Slide Rail Hardware



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

1	Slide release lever	**2**	Component release lever

Table 3-1 lists the contents of the rack-mount hardware kit (Cisco part number CSACS-1U-RAILS).

Table 3-1 Rack-Mount Hardware Kit

Item	Quantity
Slide rails	2
Multi-pin adapters	4
Fastener screws	4

Depending on the type of holes that your rack has, you will use different hardware to attach the appliance to the rack:

- For racks with square holes, you use the multi-pin adapters to attach the appliance to the rack. The installation kit includes four fastener screws that secure the multi-pin adapters after you install them in the rack. Table 3-1 lists the contents of the installation kit.

- For racks with round holes, you use rack screws, rather than the multi-pin adapters. Rack screws are not included in the installation kit.

Note Each rail consists of three pieces that slide to extend the rail to its full length. To access the features of the innermost piece, such as the release levers, you must grasp the end of the innermost piece and pull it firmly out of the piece that contains it. Figure 3-2 shows you the release levers.

Proceed to the next section, Installing the Slide Rails into a Rack with Square Holes, page 3-4, to continue the installation process.

Installing the Slide Rails into a Rack with Square Holes

This section contains:

Setting the Multi-Pin Adapters for the Rack Type

The multi-pin adapters allow the slide rails to be used in racks that have square mounting holes or round mounting holes.

To set the adapters for the rack type:

Step 1 On each slide rail, reverse the multi-pin adapter position to match the rack-mounting hole type, if necessary. Remove the multi-pin adapter by rotating the swivel lock upward, pressing the mounting pins together, and then pulling the adapter from the multi-pin bracket.

Step 2 Install the multi-pin adapter by pressing the pins together while inserting the adapter into the bracket. The multi-pin adapter must be fully locked in the bracket. Ensure that both mounting pins on the multi-pin adapter are fully engaged in the multi-pin bracket, then lock the multi-pin adapter in place using the swivel lock.

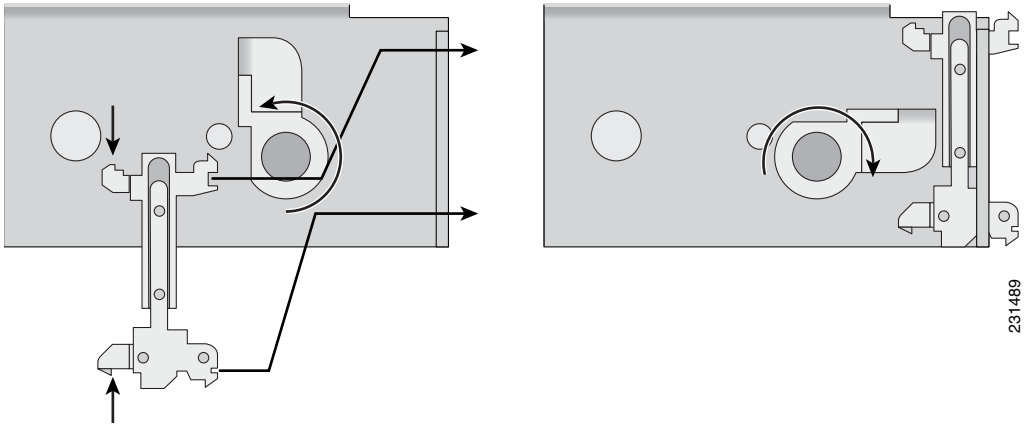
Step 3 Repeat Steps 1 and 2 for both ends of each slide rail.

Step 4 To lock the adapters in place:

a. Rotate the swivel lock to the up position. position, as shown in the illustration at the left in Figure 3-2. Press the pins together and insert the rack-mounting end of the multi-pin adapter through the corresponding holes in the bracket.

Note Insert the adapter into the bracket with the slotted pin in the up position, as shown in Figure 3-2.

Figure 3-2 Locking the Adapter into Place



b. When the multi-pin adapter is fully seated in the bracket, close the swivel lock, as shown in the illustration to the right in Figure 3-2.

If the adapter is seated properly, you should be able to easily rotate the swivel lock to the fully locked (closed) position.

Proceed to the next section, Installing and Securing the Slide Rails in a Rack, page 3-5, to continue the installation.

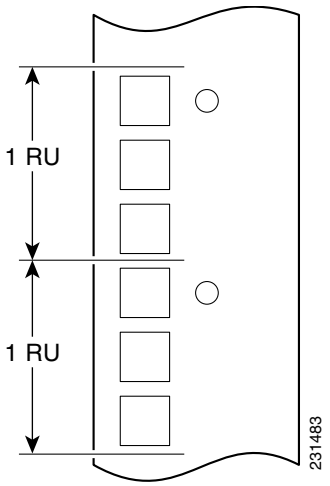
Installing and Securing the Slide Rails in a Rack

Caution If you mount the slide rail in holes that are not vertically aligned from front to back, you could damage the slide rail, and your mounting may not be secure.

To install the slide rails into the rack:

Step 1 At all four upright racks, determine the vertical position in the rack where the slide rails are to be installed. The top-most mounting hole for a particular RU mounting position is typically identified by a mark or hole, as shown in Figure 3-3.

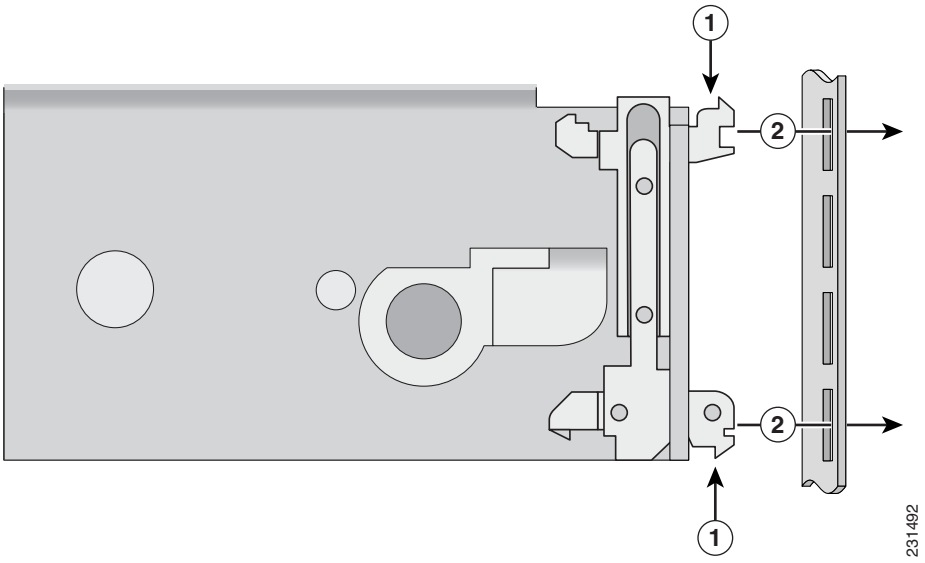
Figure 3-3 Mounting Position Marks on a Rack



Step 2 Noting the holes that you located in Step 1, align the left slide rail with its mounting holes.

Step 3 Hold the slide rail in the desired rack-mounting position. At the rear of the slide rail, press the multi-pin adapter mounting pins together (see location 1 in Figure 3-4) and insert the slide rail into the rack post (see location 2 in Figure 3-4).

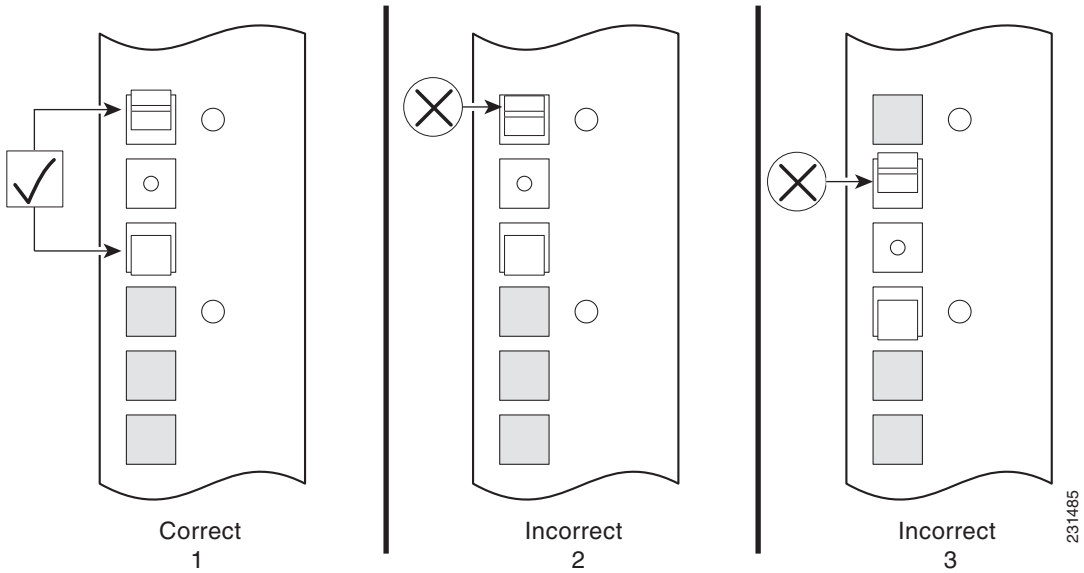
Figure 3-4 Inserting the Adapter Pins into the Mounting Holes



The following table describes the callouts in Figure 3-4.

1	Appliance mounting kit lock	**2**	Rack holes

Figure 3-5 Correct and Incorrect Adapter Pin Insertion



The following table describes some of the correct and incorrect ways to insert the adapter pins into the rack as shown in Figure 3-5.

1	Correct	The multi-pin adapter pins are fully engaged in the rack holes. Also, the rack hole into which the top pin was inserted aligns with one of the round RU holes.
2	Incorrect	Note that the multi-pin adapter pins are not fully engaged in the rack holes.
3	Incorrect	The rack hole into which the top pin was inserted does not align with one of the RU holes.

Step 4 After ensuring that the proper mounting holes on the rack upright are selected, repeat Step 2 at the slide rail front-mounting position. Ensure that the slide rail is level.

Step 5 Extend the slide rail to its fully extended (locked) position. Press the slide extension release levers to release the lock. Move the slide rail in and out throughout its entire range of motion and make certain it does not bind. If you notice some binding, recheck the mounting positions.

Step 6 Repeat Steps 2 through 5 for the right slide rail, ensuring that it is parallel and level with the left slide rail.

Proceed to Installing the Slide Rails into a Rack with Round Holes, page 3-7 to continue the installation process.

Installing the Slide Rails into a Rack with Round Holes

Installing the slide rails into a rack with round holes requires rack screws (not included in the rack-mount installation kit). Before you begin the installation, obtain the appropriate rack screws.

Caution If you mount the slide rail, in holes that are not vertically aligned from front to back, you could damage the slide rail and your mounting may not be secure.

Note When you install the rail hardware into a rack with round holes, you must position the rails so that they are inside the rack with the brackets facing outward. This placement decreases the amount of space between the posts into which you will slide the appliance. Ensure that you have adequate space for the appliance to slide into the rack. The required clearance is approximately 17.4 inches (44.2 cm).

Installing the slide rails on a round-hole rack does not require the multi-pin adapters. If the multi-pin adapters are already installed in the slide rails, remove them by rotating the swivel lock upward, pressing the mounting pins together, and then pulling the adapter from the multi-pin bracket, as shown in Figure 3-2.

To install the slide rails into the rack:

Step 1 At all four rack uprights, determine the vertical position in the rack where the slide rails are to be installed. The top-most mounting hole for a particular RU mounting position is typically identified by a mark or hole.

Step 2 After noting the holes that you located in Step 1, align the left slide rail with its mounting holes.

Step 3 Hold the slide rail in the desired rack-mounting position, with the rail on the inside of the rack and the brackets facing outward. At the rear of the slide rail, press the rear bracket against the rear post of the rack and secure the bracket to the rack with rack screws.

Step 4 After ensuring that you selected the proper mounting holes on the front rail post (by verifying that the rail is level), place the front bracket against the front post and secure the bracket to the rack with rack screws.

Step 5 Extend the slide rail to its fully extended (locked) position. Press the slide extension release levers to release the lock. Move the slide rail in and out throughout its entire range of motion and ensure that it does not bind. If you notice any binding, recheck the mounting positions.

Step 6 Repeat Steps 2 through 5 for the right slide rail, ensuring that it is parallel and level with the left slide rail.

Proceed to the next section, Installing the Appliance into the Slide Rails, to continue the installation.

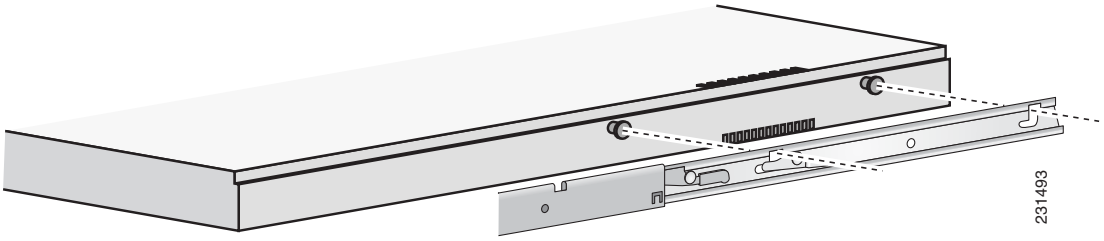
Installing the Appliance into the Slide Rails

To install the CSACS 1120 Series appliance into the slide rails:

Step 1 Extend both slide rails to their fully extended (locked) position.

Step 2 Align the mounting studs with the mounting channels on the slide rails, as shown in Figure 3-6.

Figure 3-6 Aligning the Slide Rail with the Mounting Studs



Step 3 Carefully place the component's mounting studs in the mounting channels on the slide rails. Allow the component mounting studs to fully seat in the mounting channels.

The component release levers (one on each slide rail) pivot to lock when the studs are fully engaged in the mounting channels, and then to release the studs when you press the release. Ensure that the component release levers are in the locked position.

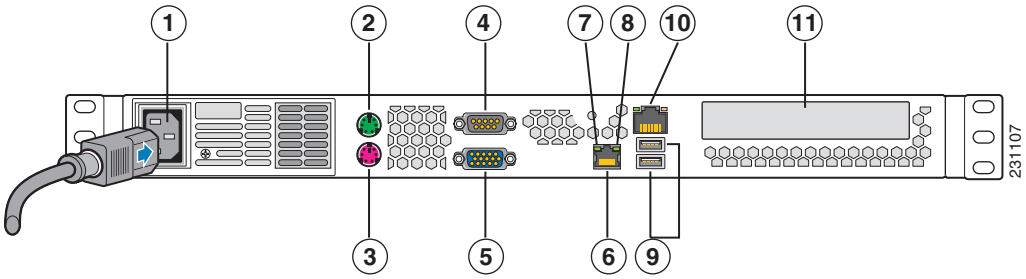
Step 4 Press and hold the left and right slide extension release levers, and slowly slide the component and the slide rails into the fully retracted position.

Connecting Cables

This section describes how to connect your CSACS 1120 Series appliance to the network and the appliance console. This section includes:

- Connecting the Network Interface
- Connecting the Console, page 3-11
- Connecting the Keyboard and Video Monitor, page 3-11
- Cable Management, page 3-12

Figure 3-7 CSACS 1120 Series Appliance Rear View



The following table describes the callouts in Figure 3-7.

1	AC power receptacle	**7**	NIC 2 port LED (activity)
2	PS/2 connector (video monitor)	**8**	NIC 2 port LED (link)
3	PS/2 connector (keyboard)	**9**	Two USB 2.0 ports

4	Serial (EIA/TIA-232) console port	**10**	NIC 1 port (10/100/1000 Mb/s) or Ethernet 0
5	Video Graphics Array (VGA) port	**11**	PCI adapter card slot (expansion)
6	NIC 2 (10/100/1000 Mb/s) port or Ethernet 1		

Note ACS must use only the NIC 1 port on the appliance. If NIC 2 is used, it may lead to software configuration problems.

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 the Network Interface

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

This section describes how to connect the CSACS 1120 Series appliance NIC port.

The RJ-45 port supports standard straight-through and crossover Category 5 unshielded twisted-pair (UTP) cables. Cisco does not supply Category 5 UTP cables; these cables are available commercially.

To connect the cable to the appliance NIC port:

Step 1 Verify that the appliance is turned off.

Step 2 Connect one end of the cable to the NIC 1 port on the appliance. For cable pinouts, see Ethernet Port Connector, page 1-8.

Note ACS must use only NIC 1 port on the appliance. If NIC 2 is used, it may lead to software configuration problems.

Step 3 Connect the other end to a hub or switch in your network.

Connecting the Console

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

Your CSACS 1120 Series appliance has a DCE-mode console port for connecting a console terminal to your appliance. The appliance uses a DB-9 serial connector for the console port. For more information, see Serial (Console) Port, page 1-8.

To connect a terminal or a PC running terminal-emulation software to the console port on the CSACS 1120 Series appliance:

Step 1 Connect the terminal using a null-modem cable to the console port. For cable pinouts, see the Serial (Console) Port Connector, page 1-8.

Step 2 Configure your terminal or terminal-emulation software for 9600 baud, 8 data bits, no parity, 1 stop bit, and no hardware flow control.

Connecting the Keyboard and Video Monitor

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

This section describes how to connect a keyboard and video monitor to the CSACS 1120 Series appliance.

The CSACS 1120 supports two PS/2 connector ports which can be used to connect a keyboard and video monitor directly to the appliance.

To connect a keyboard and video monitor to the appliance:

Step 1 Verify that the appliance is turned off.

Step 2 Connect the end of the keyboard cable to the PS/2 (keyboard) port which is located on the back panel of the appliance. For cable pinouts, see CSACS 1120 Appliance Back-Panel View, page 1-5.

Step 3 Connect the end of the video monitor cable to the PS/2 (video monitor) port which is located on the back panel of the appliance. For cable pinouts, see CSACS 1120 Appliance Back-Panel View, page 1-5.

Step 4 Power on the appliance.

Cable Management

Cable management is the most visual aspect of your appliance setup. However, cable management is often overlooked because it can be time consuming.

Equipment racks and enclosures house more equipment today than ever before. This growth has increased the need for organized cable management both inside and outside the rack. Poor cable management not only leads to damaged cables or increased time for adding or changing cables, but also blocks critical airflow or access. These problems can lead to inefficiencies in the performance of your equipment or even downtime.

There are many solutions to address cable management. They can range from simple cable management rings, to vertical or horizontal organizers, to troughs and ladders.

All CSACS 1120 Series appliance cables should be properly dressed so as not to interfere with each other or other pieces of equipment. Use local practices to ensure that the cables attached to your appliance are properly dressed.

Proceed to the next section, Powering Up the CSACS 1120 Series Appliance, to continue the installation process.

Powering Up the CSACS 1120 Series Appliance

Warning **Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.** Statement 4

Warning **This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.** Statement 39

This section contains:

Checklist for Power Up

You are ready to power up the CSACS 1120 Series appliance if:

- The appliance is securely mounted.
- Power, network, and interface cables are properly connected.

Power-Up Procedure

To power up the CSACS 1120 Series appliance and verify its initialization and self-test, follow this procedure. When the procedure is completed, the appliance is ready to be configured.

Step 1 Review the information in Safety Guidelines, page 2-1.

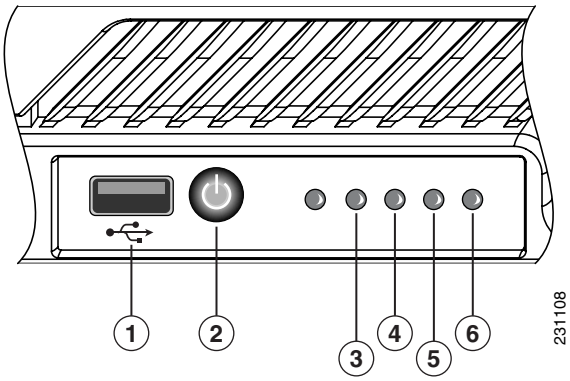
Step 2 Plug the AC power cord into the power cord receptacle at the rear of the appliance. (See location 1 in Figure 3-7.)

Step 3 Connect the other end of the power cord to a power source at your installation site.

Step 4 Press the power button on the front of the appliance. (See location 2 in Figure 3-8.)

The appliance should begin booting. Once the operating system boots, you are ready to initialize the basic software configuration.

Figure 3-8 CSACS 1120 Series Appliance Front View



The following table describes the callouts in Figure 3-8.

1	USB port	**4**	Hard disk drive activity LED
2	Power button	**5**	NIC 1 LED
3	Appliance power LED	**6**	NIC 2 LED

Checking the LEDs

When the CSACS 1120 Series appliance is up and running, observe the front-panel LEDs. The following LEDs provide power, activity, and status information:

CSACS 1120 Appliance Front-Panel LEDs

- Appliance power, green:
  - On when power is on.
  - Off when power is off or an error condition has been detected in the operating voltages.

- Hard disk activity, green:
  - On when appliance software has booted up and the appliance is operational.
  - Off when appliance has not yet booted or an error condition has been detected in the boot process.
- NIC 1 or NIC 2, green:
  - On when packets are being transferred.
  - Off when no packets are being transferred.

For more detailed information about the LEDs, see Appendix D, "Troubleshooting."

Removing or Replacing the CSACS 1120 Series Appliance

Warning **Before working on a system that has an On/Off switch, turn OFF the power and unplug the power cord.** Statement 1

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

This section contains:

Removing a CSACS 1120 Series Appliance

To remove a CSACS 1120 Series appliance from your network:

Step 1 Power down the appliance.

Step 2 Disconnect the power cords and network cables.

Step 3 Physically remove the appliance from the rack.

The appliance is in constant communication on your network; thus, when the network notices that the appliance is no longer responding to it, the network stops sending requests to the appliance. This change is visible to users.

Note If other appliances are attached to the network, the network continues sending requests to the other appliances.

Replacing a CSACS 1120 Series Appliance

To replace an appliance:

Step 1 Remove the appliance from the network.

Step 2 Install a new appliance using the same installation procedures that you used for the previous appliance.

Configure the new appliance using the same configuration parameters that you used for the removed appliance.

Initial Configuration

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

- Establishing a Serial Console Connection
- Configuring CSACS 1120
- Verifying the Initial Configuration
- Setting Up a GUI Administrator Account

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. For more information, see *User Guide for Cisco Secure ACS 4.2*.

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:

If you performed the procedure in Connecting Cables, 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 CSACS 1120. For the location of the serial port, see Figure 1-5.

c. Use an RJ-45 cable (provided) to connect the console to the CSACS 1120.

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

Step 2 Power on CSACS 1120 and the console, and open your terminal emulation communication software on the console.

Tip See Figure 1-4 for the location of the power switch on CSACS 1120.

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

Note CSACS 1120 works with only a baud rate of 9600. CSACS 1120 does not support a baud rate of 115200 which other appliances use.

- Baud = 9600
- Databits = 8
- Stops = 1
- Flow control = None
- Terminal emulation type = ANSI

Result: The `login`: prompt appears.

Configuring CSACS 1120

You must configure the CSACS 1120 when you boot the system for the first time and whenever you re-image the system. For more information on re-imaging the system, see Upgrade Scenarios.

Table 3-2 lists the essential configuration tasks that are unique to SE.

Table 3-2 SE Configuration Tasks

Task	Available Resources
Remote Agent configuration	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/NetCfg.html#wp386216
System Configuration	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/SCBasic.html
ACS Back up	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/SCBasic.html#wp222373
ACS Restore	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/SCBasic.html#wp330795

Table 3-2 SE Configuration Tasks

Task	Available Resources
Certificate setup	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/SCAuth.html#wp373226
EAP-FAST PAC files configuration	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/SCAuth.html#wp419531
Date/Time configuration	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/SCBasic.html#wp288064
SNMP setup	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/SCBasic.html#wp288047

Before you begin to configure the CSACS 1120, you should have the following information:

- Network hostname of the CSACS 1120.
- DNS domain name.
- Administrator name and password.
- Database password.
- GUI administrator name and password.
- Whether you will enable DHCP (enabling DHCP is not recommended).
- IP, netmask, and gateway addresses you will assign to the .
- Whether you will be using NTP synchronization and, if yes, the address of the NTP server.

To configure CSACS 1120:

Step 1 Establish a serial console connection to the CSACS 1120.

Note If CSACS 1120 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.
```

Note If this information does not appear and only the `login` prompt appears, you must reboot the appliance and then log in.

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

Note When you boot the system for the first time, it is not configured. You must log in as the command line interface (CLI) administrator to configure the system.

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

Note The password is case sensitive.

Result: The console displays:

```
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, enter the name that you intend to use for your CSACS 1120, and press **Enter**.

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

Result: The console displays:

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

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

Result: The console displays:

```
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, enter the ACS administrator account name, and press **Enter**.

Tip Only one ACS CLI administrator account can exist at a time. This account allows access only through a serial cable and CLI commands. You can change the account's credentials. For more information, see Resetting the CSACS 1120 Administrator Password.

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

Note The new password must be unique and should not be identical to the last ten passwords that have been used. It 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, enter the new ACS password again, and press **Enter**.

Result: The console displays:

```
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.
```

Note It 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:`** prompt, enter the new database password, and press **Enter**.

Step 12 At the **`Enter new password again:`** prompt, enter new database password again, and press **Enter**.

Result: The console displays:

```
Password is set successfully.
```

Step 13 At the **`Would you like to add GUI Administrator now?:`** prompt, type **y** for yes or **n** for no, and press **Enter**.

Note If you do not enter **y** or **n** and press enter, the default value is (yes) is used.

Step 14 If you entered **y**, complete these steps:

a. When the `Enter new GUI administrator name: prompt appears,` enter the new GUI administrator name.

The following prompt appears:

```
Enter new password:
```

b. Enter the new password.

Note The password can only contain a maximum of 32 characters and a minimum of 4 characters.

The following prompt appears:

```
Enter new password again:
```

c. Enter the new password again.

Result: The console displays:

```
GUI Administrator added successfully.
```

For more information on adding a GUI administrator account, see Setting Up a GUI Administrator Account.

Step 15 At the `Use Static IP Address [Yes]:` prompt, enter **`Y`** for yes or **`N`** for no, and press **Enter**.

Note To set or change the IP address of your CSACS 1120, it must be connected to a working Ethernet connection.

Note A static IP address must be assigned to your CSACS 1120. You can set the IP address directly by answering **Y** to this step and performing the substeps detailed in Step 16. Alternatively, you may use a DHCP address if it assigns a single IP address that does not change.

Step 16 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 CSACS 1120 IP address, at the `IP Address [xx.xx.xx.xx]:` prompt, enter the IP address, and press **Enter**.

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

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

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

Note If you do not intend to use a DNS server, enter the IP address of the CSACS 1120 at the `DNS Servers` **[xx.xx.xx.xx]** prompt. If you do not configure the CSACS 1120 to use a DNS server, you must respond to all prompts for hostname or IP address only with an IP address.

Result*:* The console displays:

```
IP Address is reconfigured.
```

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

Result*:* The console displays:

```
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 `Accept network setting:` prompt, enter **Y**, and press **Enter**.

Result: The IP address for the appliance will be set.

g. At the `Test network connectivity [Yes]:` prompt, enter **Y**, and press **Enter**.

Tip This step executes a **ping** command to ensure the connectivity of the .

h. At the `Enter hostname or IP address:` prompt, enter the IP address or hostname of a device connected to the , and press **Enter**.

Result*:* If successful, the system displays the ping statistics and displays the **Test network connectivity** prompt.

i. If network connectivity is validated in the previous two steps, at the `Test network connectivity [Yes]:` prompt, enter **N**, and 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 17 If the settings appear correctly, at the `Accept network setting [Yes]:` prompt, enter **Y**, and press **Enter.**

Result*:* The console displays:

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

Step 18 To set the time and date of the CSACS 1120, at the `Change Date & Time Setting [N]:` prompt, enter **Y**, and press **Enter**.

Result: The console displays a numbered list of time zones.

Step 19 At the `Enter desired time zone index (0 for more choices):` prompt, enter the index number of the appropriate time zone for your geography and, press **Enter**.

Result: The console displays the new time zone.

Step 20 At the `Synchronize with NTP server? [N]:` prompt, do one of the following:

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

Tip Only if you choose to use an NTP server, can you subsequently use the **ntpsync** command.

Result: The console displays a confirmation message reflecting your choice.

Step 21 At the `Enter date [mm/dd/yyyy]:` prompt, enter the date in the given format, and press **Enter**.

Step 22 At the `Enter time [hh:mm:ss]:` prompt, enter the current time in the given format, and press **Enter**.

Result: The console displays:

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

The system reboots.

Verifying the Initial Configuration

To verify that you have correctly completed the CSACS 1120 initial configuration:

Before You Begin

Establish a serial console connection to the CSACS 1120. For details, see Configuring CSACS 1120.

Step 1 Reboot the CSACS 1120. For more information, see Rebooting the CSACS 1120 from a Serial Console.

Result: When the system boots, a `login` prompt appears on the console.

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

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

Step 4 At the `system` prompt, enter **`show`** and press **Enter**.

Result: The console displays the status information.

Step 5 Verify that the information on the screen is correct.

Setting Up a GUI Administrator Account

After initial installation or re-imaging, unless you specified a GUI administrator account during the initial configuration using the *setup* script, only one administrator account exists: the *CLI administrator* account. This account allows access only through a serial console log in and CLI commands.

If you specified a GUI administrator account when prompted for one by the *setup* script, a GUI administrator account exists. However, before the designated GUI administrator user can use this account, you must unlock it by entering the **unlock guiadmin** command.

You can also set up an additional GUI administrator account that can access the CSACS 1120.

To set up an initial web GUI account:

Step 1 Log in as the CLI administrator.

Step 2 If a GUI administrator account was specified during initial configuration using the setup script, enter the **unlock guiadmin** command to unlock the GUI administrator account:

unlock guiadmin *<Admin> <Password>*
where *Admin* is the name of the GUI administrator account and *Password* is the password for the account.

Step 3 If no GUI administrator account has been set up or you want to add additional GUI administrator accounts, at the command prompt, enter:

add guiadmin

Result: The console displays:

```
Adding new GUI Administrator
Note! All ACS services will be restarted.
GUI Administrator password policy is:
Password must be at least 4 character(s) long.
```

Step 4 At the `Enter new GUI administrator name:` prompt, enter the new GUI administrator name, and press **Enter**.

Step 5 At the `Enter new password:` prompt, enter the new password, and press **Enter**.

Note The password can only contain a maximum of 32 characters and a minimum of 4 characters.

Step 6 At the `Enter new password again:` prompt, enter the new password again, and press **Enter**.

Result: The console displays:

`GUI Administrator added successfully.The new GUI administrator account is not usable until you unlock it by entering the` **`unlock guiadmin`** `command.`
Now, you can now use the GUI administrator account to remotely access the ACS GUI running on the CSACS 1120.

Next Steps

After you have successfully performed the procedures in this guide, CSACS 1120 is installed and initially configured. The next step is to log in using the GUI administrator account and use a browser and the web interface to fully configure the CSACS 1120 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 4.2*.

Note The CSACS 1120 automatically creates an entry called *Self* in the AAA Servers Table. This entry identifies the CSACS 1120 machine. However, in the Proxy Distribution Table and the AAA Server Table for RDMS synchronization, the CSACS 1120 creates an entry for the hostname of the device that is running the CSACS 1120.

CHAPTER 4

Administering the Cisco 1120 Secure Access Control Server

This section describes the major CSACS 1120 system administration tasks that you can perform using the CLI in the serial console connection. For all other configuration and administration tasks, that is, those performed from the ACS web interface, see the *User Guide for Cisco Secure Access Control Server 4.2*.

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

This section contains:

- Basic Command Line Administration Tasks
- Working with System Data
- Reconfiguring CSACS 1120 System Parameters
- Patch Rollback
- Recovery Management

Basic Command Line Administration Tasks

This section details basic administrative tasks you can perform from a serial console connected to the . This section contains:

- Logging In to the CSACS 1120 from a Serial Console
- Shutting Down the CSACS 1120 from a Serial Console
- Logging Off the CSACS 1120 from a Serial Console
- Rebooting the CSACS 1120 from a Serial Console
- Determining the Status of CSACS 1120 System and Services from a Serial Console
- Tracing Routes
- Stopping ACS Services from a Serial Console
- Starting ACS Services from a Serial Console
- Restarting ACS Services from a Serial Console
- Getting Command Help from the Serial Console

Logging In to the CSACS 1120 from a Serial Console

To log in to the CASACS 1120 from a serial console:

Step 1 Establish a serial console connection to the CSACS 1120. For details, see Configuring CSACS 1120.

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

Step 3 At the `password:` prompt, enter the password, and press **Enter**.

Result: The system prompt appears:

name

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

Shutting Down the CSACS 1120 from a Serial Console

You can use the serial console to shut down the CSACS 1120.

Caution Powering off the CSACS 1120 by using only the power switch may cause the loss or corruption of data.

To use the serial console to shut down the:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`shutdown`**, and press **Enter**.

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

Result: The console displays:

```
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 CSACS 1120.

For the location of the power switch see Figure 1-2.

Result: The CSACS 1120 powers OFF.

Logging Off the CSACS 1120 from a Serial Console

To log off the CSACS 1120 from a serial console:

At the system prompt, enter **`exit`**, and press **Enter**.

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

Rebooting the CSACS 1120 from a Serial Console

To reboot the CSACS 1120 from the serial console:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`reboot`**, and press **Enter**.

Step 3 At the `Are you sure you want to reboot? (Y/N):` prompt, enter **`Y`** for yes, and press **Enter**.

Result: The CSACS 1120 reboots. When the reboot is finished, the `login` prompt appears.

Determining the Status of CSACS 1120 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 CSACS 1120 web interface. For more information, see "Determining the Status of Cisco Secure ACS Services" in the *User Guide for Cisco Secure Access Control Server 4.2*.

To determine the status of the CSACS 1120 and it's services:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`show`**, and press **Enter**.

Result: The console displays:

```
  Name
  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.

To trace the network route that the CSACS 1120 takes to a given destination:

At the system prompt, enter **tracert**, followed by **zero (0)** or more optional arguments, and the IP address of the target destination, and press **Enter**.

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

```
Trace complete
```

Stopping ACS Services from a Serial Console

Note You typically stop ACS services in the web interface.

You can stop any of the ACS services from the serial console. The CSACS 1120 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 CSACS 1120 System and Services from a Serial Console.

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

To stop an ACS service:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **stop** followed by a single space and the name of the ACS service that you want to stop, and press **Enter**.

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

Result: The console displays:

```
Stopping service: [service name]. . . .
[service name] is not running
```

Starting ACS Services from a Serial Console

Note You typically start ACS services in the web interface.

You can start any of the ACS services from the serial console. The ACS 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 CSACS 1120 System and Services from a Serial Console.

To start an ACS service:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **start** followed by a single space and the name of the ACS service that you want to start, and press **Enter**.

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

Result: The console displays:

```
Starting service: [service name].s. . . .
[service name] is starting
[service name] is running
```

Restarting ACS Services from a Serial Console

Note You typically restart ACS services in the web interface.

You can restart any ACS service from the serial console. ACS 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 CSACS 1120 System and Services from a Serial Console.

To restart an ACS service:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`restart`** followed by a single space and the name of the ACS service that you want to restart, and press **Enter**.

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

Result: The console displays:

```
[service name] is stopping. . .
[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 CSACS 1120 from the serial console:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`help`**, and press **Enter**.

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

Result: The console displays the list of commands and their descriptions, as shown in Table 4-1.

Table 4-1 CSACS 1120 Commands

Command	Description
?	List commands
unlock guiadmin	Unlock GUI administrator
remove guiadmin	Remove GUI administrator
add guiadmin	Adds a GUI administrator account that allows access to the SE using the ACS web GUI.
backup	Back up 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

Table 4-1 CSACS 1120 Commands (continued)

Command	Description
ntpsync	Perform Network Time Protocol synchronization with predefined NTP servers
ping	Verify connections to remote computers
reboot	Soft reboot appliance
restart	Restart ACS services
restore	Restore appliance
rollback	Rollback patched package
set	Set commands
set admin	Set administrator's name
set domain	Set DNS domain
set hostname	Set appliance's hostname
set ip	Set IP configuration
set password	Set administrator's password
set dbpassword	Set database encryption 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	Shut down appliance
start	Start ACS services
stop	Stop ACS services
support	Collect logs, registry, and other useful information
tracert	Determine the route taken to a destination
upgrade	Upgrade appliance (stage II)

For more information on commands, see Appendix C, “Command Reference”

Working with System Data

This section explains basic data-manipulation tasks performed from a serial console connected to the CSACS 1120:

- Obtaining Support Logs from the Serial Console
- Exporting Logs
- Exporting a List of Groups
- Exporting a List of Users

- Backing Up ACS Data from the Serial Console
- Restoring ACS Data from the Serial Console
- Enabling RDBMS Synchronization
- Enabling Remote Invocation for CSDBSync Functionality

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 is then sent to support personnel for analysis.

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

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

This procedure uses the **support** command. For more information on this command, see support. 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 CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`support`** and the necessary arguments, and press **Enter**.

Step 3 To collect user database information, at the `Collect User Data? <Y or N>:` prompt, enter **`Y`** and press **Enter**.

Step 4 At the `Collect Previous days logs? <N or Number of days><1>:` prompt, enter **the number of days for which you want to collect information (from 1 to 9999),** and press **Enter**.

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

Step 6 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 press **Enter**.

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

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

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

Result: The console 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 message on the console:

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

This message indicates that ACS has packaged and transferred the *.cab* file as specified, and restarts services.

Result: The system returns to the system prompt.

Exporting Logs

This section details the procedure for exporting ACS log files to an FTP server for further examination and processing. Using the **exportlogs** command, you can enter the name of the log(s) or 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 .

To export log files to an FTP server:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`exportlogs`** ***logname***, and press **Enter.**

Where *logname* is the name of the 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, and 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.

Step 3 At the `Enter FTP Server Hostname or IP Address:` prompt, enter the IP address or hostname of the FTP server, and press **Enter**.

Step 4 At the `Enter FTP Server Directory:` prompt, enter the FTP server directory pathname, and press **Enter**.

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

Step 6 At the `Enter FTP Server Password:` prompt, enter the FTP server password, and press **Enter**.

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

Exporting a List of Groups

This section details the procedure for exporting a list of ACS 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.

To export a user group list to an FTP server:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`exportgroups`**, and press **Enter**.

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

Result: The console displays:

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

Caution Performing this procedure stops and restarts the **CSAuth** service, and will interrupt use of the ACS.

Step 3 To proceed, enter **y,** and 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 directory pathname, and press **Enter**.

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

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

Result: ACS exports the group list file to the specified location. When this is completed the console displays:

```
Transferring 'groups.txt' completed
```
The system prompt returns.

Exporting a List of Users

This section details the procedure for exporting a list of ACS 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.

To export a list of users to an FTP server:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **exportusers**, and press **Enter**.

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

Result: The console displays:

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

Caution Performing this procedure stops and restarts the **CSAuth** service, and will interrupt use of the ACS.

Step 3 To proceed, enter **Y**, and 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 directory pathname, and press **Enter**.

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

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

Result: ACS exports the file of the list of users to the specified location, When this is completed the console displays:

```
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 data to an FTP server.

Note You typically perform this procedure in the web interface.

During back up, AAA services are interrupted, and ACS 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.

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 ACS for AAA services.

To export ACS data to an FTP server:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`backup`** and press **Enter**.

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

Step 3 At the `Enter FTP Server Hostname or IP Address:` prompt, enter the FTP server IP address or hostname, and press **Enter**.

Step 4 At the `Enter FTP Server Directory:` prompt, enter the FTP server directory pathname, and press **Enter**.

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

Step 6 At the `Enter FTP Server Password:` prompt, enter the FTP server password and, press **Enter**.

Step 7 At the `File:` prompt, enter the name that you want to give the backup file, and press **Enter**.

Step 8 At the `Encrypt Backup file? <Y or N>:` prompt, enter **`Y`** to encrypt the backup file or **`N`** not to encrypt it, and press **Enter**.

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

Step 9 If you entered **y** to encrypt the backup file, at the `Encryption Password:` prompt, enter a password and then press **Enter**.

Result: The console displays:

```
Backing up now . . .
All running services will be stopped and restarted automatically.
Are you sure you want to proceed? <Y or N>
```

Step 10 To proceed, enter **y** and press **Enter**.

Result: ACS exports the backup file to the specified location and displays messages regarding the progress of the back up.

When the backup process is completed, the console displays:

```
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 data from an FTP server after you perform a back up. For more information on backing up ACS data, see Backing Up ACS Data from the Serial Console.

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, the decryption password, if the backup was encrypted.

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

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

To restore ACS data from an FTP server:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`restore`**, and press **Enter**.

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

Step 3 At the `Enter FTP Server Hostname or IP Address:` prompt, enter the FTP server IP address or hostname, and press **Enter**.

Step 4 At the `Enter FTP Server Directory:` prompt, enter the FTP server directory pathname and, press **Enter**.

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

Step 6 At the `Enter FTP Server Password:` prompt, enter the FTP server password, and press **Enter**.

Step 7 At the `File:` prompt, enter the name of the backup file, and press **Enter**.

Step 8 At the `Select Components to Restore: User and Group Database: <Y or N>` prompt, enter **Y** to restore the user and group database, and press **Enter**.

Step 9 At the `CiscoSecure ACS System Configuration: <Y or N>` prompt, enter **Y** to restore the system configuration data, and press **Enter**.

Step 10 At the `Decrypt Backup file? <Y or N>:` prompt, enter **Y**, if you previously encrypted the backup file, and press **Enter**.

Step 11 If you entered **Y** to decrypt the backup file, at the `Encryption Password:` prompt, enter the FTP password, and press **Enter**.

Note The console displays a warning message: on the console:

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

Step 12 At the `Are you sure you want to proceed? <Y or N>:` prompt, enter **Y** and press **Enter**.

Result: ACS 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 has no shared profile components configured, you see a message about Device Command Sets (DCS) not on the backup, which is normal.

When this is completed, the console displays:

```
Done
```

Note You cannot restore ACS 4.1 data from the serial console. You can perform this procedure only through the web interface.

Enabling RDBMS Synchronization

RDBMS Sycnchronisation supports the manipulation and updation of ACS internal database objects. You can Create, Read, Update, and Delete all data items that RDBMS Synchronization can access. This section details the procedure for invoking RDBMS Synchronization on the CSACS 1120.

For more information about RDBMS Synchronization, see http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/user.html

Note You must upload and use the *accountActions.csv* file to perform RDBMS Synchronization on the CSACS 1120.

Before You Begin

You must have the FTP server address and pathname, as well as write permissions to the FTP server directory.

To configure RDBMS Synchronization on the SE:

Step 1 Connect to the CSACS 1120 via the SSH client. Check the connectivity between the SSH client and the SSH server.

Step 2 Log in to the GUI administrator account and enter the administrator name and password.

Step 3 In the navigation bar, click **System Configuration**.

Step 4 Click **RDBMS Synchronization.**

The RDBMS Synchronization setup page appears.

Step 5 In the FTP Setup For Account Actions Download Table, enter:

a. The name of the *accountActions* file that you want to use to update ACS.

b. The IP address or hostname of the FTP server from where CSACS 1120 must download the *accountActions* file.

c. The directory path on the FTP server where the *accountActions* file resides.

d. The username for ACS to access the FTP server.

e. The password for the FTP server.

Step 6 Upload the CSVfile.

CSACS 1120 will automatically create the DSN.

Note The uploaded CSV file must be in a valid format and the values given in the CSV file for RDBMS Synchronization must be valid.

Step 7 Log in to the CLI administrator account and enter the administrator username and password.

Step 8 At the system prompt, enter **`csdbsync -syncnow`** and press **Enter.**

Step 9 The console displays:

```
CSDbSync v4.2(0.113), Copyright 1997-2007, Cisco Systems Inc
Logging mode: FULL
Transaction processing invoked manually

Sync complete: 10 transaction(s) 0 parse error(s) 0 process error(s)
SL:Disconnect Start
DBConnectionPool: 2 Connecion(s) to delete
Going to sleep for 0.5 sec
Going to sleep for 0.5 sec
Going to sleep for 0.5 sec
Going to sleep for 0.5 sec
DBConnectionPool: Destructor Complete
SL:Disconnect Complete
```

CSACS 1120 fetches the CSV file from the database, reads the action codes in the file, and performs the RDBMS Sycnchronisation operations specified in the file.

Enabling Remote Invocation for CSDBSync Functionality

CSDBSync supports the configuring of ACS on the CSACS 1120, via remote systems. The CSDBSync service reads each record from the accountActions file and updates the ACS internal database according to the action code specified in the record. Synchronization events fail if CSDBSync cannot access the accountActions file. In a distributed environment, a single ACS, known as the senior synchronization partner, accesses the accountActions table and sends synchronization commands to its synchronization partners.

For more information about CSDBSync, see http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/user.html

Reconfiguring CSACS 1120 System Parameters

This section details basic reconfiguration tasks performed from a serial console connected to the CSACS 1120. This section contains:

- Resetting the CSACS 1120 Administrator Password
- Resetting the CSACS 1120 CLI Administrator Name
- Resetting the GUI Administrator Login and Password
- Resetting the CSACS 1120 Database Password
- Reconfiguring the CSACS 1120 IP Address
- Setting the System Time and Date Manually
- Setting the System Time and Date with NTP
- Setting the System Timeout
- Setting the CSACS 1120 System Domain
- Setting the CSACS 1120 System Hostname

Resetting the CSACS 1120 Administrator Password

There is always a single ACS administrator username and password 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. This account is called the CLI administrator account and allows access to ACS only through a serial console.

You can reset the ACS CLI 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 CLI administrator name see Resetting the CSACS 1120 CLI Administrator Name.

If you do not have the existing ACS CLI 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.

To reset the ACS administrator login credentials:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`set password`**, and press **Enter.**

Step 3 At the `Enter old password:` prompt, enter the old password, and press **Enter**.

Step 4 At the `Enter new account name:` prompt, enter the new account name, and press **Enter**.

Step 5 At the `Enter new password:` prompt, enter the new password, and press **Enter**.

Note The new password must be unique and should not be identical to the last ten passwords that have been used. It must not contain the administrator account name, must contain a minimum of six characters, and it must include a mix of at least three character types: numerals, special characters, uppercase letters, and lowercase letters. Each of the following examples is acceptable: *1PaSsWoRd, *password44, Pass*word*.

Step 6 At the `Renter new password again:` prompt, reenter the new password, and press **Enter**.

Result: The console displays:

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

Resetting the CSACS 1120 CLI Administrator Name

There is always a single set of ACS CLI 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 CLI 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 CSACS 1120 Administrator Password.

Note The CLI administrator login does not provide access to the CSACS 1120 using the web GUI. You must set up an initial web GUI password using the **add guiadmin** command. For information on setting up an initial web GUI account, see Resetting the GUI Administrator Login and Password.

If you do not have the existing CLI administrator login credentials, you must use 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.

To reset the ACS CLI administrator name:

Step 1 Log in to the CSACS 1120 . For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`set admin`**, and press **Enter**.

Step 3 At the `Set administrator's name:` prompt, enter the new administrator name, and press **Enter**.

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

Result: The console displays:

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

Resetting the GUI Administrator Login and Password

You can reset the ACS GUI administrator name, 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 CSACS 1120 Administrator Password.

After initial installation of the CSACS 1120, the only password that exists is the CLI administrator password. This password allows access only through a serial console login and CLI commands.

To enable an initial administrator account that can access ACS through the web GUI, you must set up a GUI administration account using the **add guiadmin** command.

To set up an initial web GUI account:

Step 1 Log in as the CLI administrator.

Step 2 At the command prompt, enter:

`add guiadmin` `<admin> <password>`

where *admin* is the name of the GUI administrator account and *password* is the password is the password for the GUI administrator.

Step 3 At the `Enter new GUI administrator name:` prompt, enter the new GUI administrator name and press **Enter**.

Step 4 At the `Enter new password`: prompt, enter the new password and press **Enter**.

Note The password can only contain a maximum of 32 characters and a minimum of 4 characters.

Step 5 At the `Enter new password again:` prompt, enter the new password again, and press **Enter**.

Result: The console displays:

```
GUI Administrator added successfully.
```

Now, you can use the GUI administrator account to remotely access the ACS GUI running on the CSACS 1120.

Resetting the CSACS 1120 Database Password

You should change the ACS 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 database password:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`set dbpassword`**, and press **Enter.**

Step 3 At the `Please enter the OLD ACS Database Encryption Password:` prompt, enter the old database password, and press **Enter**.

Step 4 At the `Please enter the NEW ACS Database Encryption Password:` prompt, enter the new password, and press **Enter**.

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

Step 5 At the `Reenter new password:` prompt, enter the new password again, and press **Enter**.

Result: The console displays:

```
Password is set successfully.
```

Reconfiguring the CSACS 1120 IP Address

Typically, you configure the IP address only once, during initial configuration. See Configuring CSACS 1120.

Caution Reconfiguring the IP address may cause other network devices to fail to recognize the CSACS 1120.

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 CSACS 1120, the CSACS 1120 must be connected to a working Ethernet connection.

To reconfigure the IP address:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`set ip`**, and press **Enter**.

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

Step 4 If you entered **No**, the system displays a confirmation of DHCP and the message **IP Address is reconfigured** appears on the console. Continue the procedure with Step 5.

If you entered **Yes**, to specify the CSACS 1120 IP address:

a. At the **IP Address [xx.xx.xx.xx]:** prompt, enter the IP address, and press **Enter**.

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

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

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

Result: The console displays the new configuration information and the following message:

IP Address is reconfigured.

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

Result: The CSACS 1120 restarts. The console displays:

New ip address is set.

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

Tip This step executes a **ping** command to ensure the connectivity of the .

Step 7 At the `Enter hostname or IP address:` prompt, enter the IP address or hostname of a device connected to the CSACS 1120, and 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 successful in the previous two steps, at the `Test network connectivity [Yes]: prompt`, enter **N**, and 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 CSACS 1120 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 CSACS 1120 system time and date by using an NTP, see Setting the System Time and Date with NTP.

To set the CSACS 1120 system time and date manually:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

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

Result: The console displays:

```
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 At the **Change Date & Time Setting? [N]:** prompt, to set the time zone, time, or date enter **Y**, and press **Enter**.

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

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

Step 4 At the `Enter desired time zone index (0 for more choices) [x]:` prompt, enter the desired time zone index number from the time zone setting list, and press **Enter**.

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

Result: The console displays the new time zone.

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

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

Step 7 At the **Enter time [hh:mm:ss]:** prompt, enter the current time, and 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 NTP server with which the system synchronizes its date and time. (You can configure backup NTP servers if you desire.)

To set the CSACS 1120 system time and date manually, see Setting the System Time and Date Manually.

To set the CSACS 1120 system time and date with NTP:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

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

Result: The console displays:

```
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 At the **Change Date & Time Setting? [N]:** prompt, to set the time zone, time, or date enter **Y**, and press **Enter**.

Result: The console display the indexed time zones:

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

Step 4 At the `Enter desired time zone index (0 for more choices) [x]:` prompt, enter the desired time zone index number from the time zone setting list, and press **Enter**.

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

Result: The console displays the time zone setting.

Step 5 At the **Synchronize with NTP Server?** prompt, enter **Y**, and 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 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 console displays:

```
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 which, is the number of minutes that can pass with no activity on the serial console before the console login times out.

To set the CSACS 1120 system timeout:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **set timeout,** and press **Enter**.

Step 3 At the `Enter timeout <minutes>:` prompt, enter the timeout period in minutes followed by a single space, and press **Enter.**

Result: The system sets the new timeout period.

Setting the CSACS 1120 System Domain

You can set the system DNS domain from the serial console. To set the CSACS 1120 system domain:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`set domain`**, and press **Enter**.

Step 3 At the `Enter DNS domain:` prompt, enter the domain name, and press **Enter**.

Result: The console displays:

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

Setting the CSACS 1120 System Hostname

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

You can set the system hostname. To set the CSACS 1120 system hostname:

Step 1 Log in to the CSACS 1120. For more information, see Logging In to the CSACS 1120 from a Serial Console.

Step 2 At the system prompt, enter **`set hostname`**, and press **Enter**.

Step 3 At the `Enter appliance name:` prompt, enter the hostname, and press **Enter**.

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

Result: The console displays:

```
Stopping all ACS Services
Stopping service: CSAdmin.
Stopping service: CSAuth..
Stopping service: CSDbSync.
Stopping service: CSLog.
Stopping service: CSMon.
Stopping service: CSRadius..
Stopping service: CSTacacs.
Starting all ACS Services
Starting service: CSAdmin....
Starting service: CSAuth..
Starting service: CSDbSync.
Starting service: CSLog..
Starting service: CSMon.
Starting service: CSRadius.
Starting service: CSTacacs..
You should reboot appliance for the change to take effect.
```

The system restarts all services, and the hostname is reset. The system then prompts you to reboot the appliance. The hostname is then reset after system reboot.

Patch Rollback

This section contains:

- Removing Installed Patches
- Understanding the CSAgent Patch

Removing Installed Patches

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

To roll back an ACS system patch:

Step 1 Connect a console to the CSACS 1120 console port. For the location of the console port, see Figure 1-2.

Step 2 At the system prompt, enter **`rollback`** and the name of the patch application that you want rolled back, and 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, enter **rollback** followed by the patch application name, and then press **Enter**.

Step 3 At the `Are you sure you want to rollback [patch name]?)(Y/N):` prompt, enter **`Y`**, and press **Enter**.

Result: The console displays:

```
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 CSACS 1120 System and Services from a Serial Console.

Understanding the CSAgent Patch

In ACS 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 the *User Guide for Cisco Secure Access Control Server 4.2*.

Recovery Management

ACS functionality includes two procedures that the administrator can perform by using the CSACS 1120 Recovery CD-ROM:

- Recovering from Loss of Administrator Credentials
- Re-imaging the CSACS 1120 Hard Drive

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 administrator account, perform this procedure. In this procedure you use the CSACS 1120 Recovery CD-ROM to access the system from the serial console and reset the administrator login credentials.

The ACS administrator login credentials:

- Consists of only one set of login credentials at one time.
- Are set (that is, changed from the default) during initial configuration.
- Can be reset at anytime. For more information, see Resetting the CSACS 1120 Administrator Password.

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 CSACS 1120 console port. For the location of the console port, see Figure 1-3.

Step 2 Power on the console.

Step 3 Insert the Recovery CD-ROM into the CSACS 1120 CD-ROM drive.

Step 4 Power on the CSACS 1120. (Or if already running, reboot the CSACS 1120. For more information, see Rebooting the CSACS 1120 from a Serial Console.)

Result: The console displays:

```
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 At the `Enter menu item number: [ ]` prompt, enter `1`, and press **Enter**.

Step 6 At the `Hit the Return key to log in:` prompt, enter `y`, and press **Enter**.

Result: The console displays:

```
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 press **Enter**.

Result: The system reboots, and displays the system version information:

```
Status: The appliance is functioning properly.
Default administrator account can be reset now.
Press enter to change default administrator account and password.
```

Step 8 Press **Enter** to change the default administrator account and password.

Result: The console displays:

```
Enter new account name:
```

Note Press only the **Enter** key at Step 8. If you press any other key it will lead to the faliure of the password recovery process.

Step 9 At the **`Enter new account name:`** prompt, enter the name of the administrator, and press **Enter**.

Result: The console displays:

Enter new password:

Step 10 At the **`Enter new password:`** prompt, enter the new password, and press **Enter**.

Note The new password must be unique and should not be identical to the last ten passwords that have been used. It must contain a minimum of six characters, and it must include a mix of at least three character types: numerals, special characters, uppercase letters, and lowercase letters. Each of the following examples is acceptable: *1PaSsWoRd, *password44, Pass*word*.

Result: The console displays:

Enter new password again:

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

Result: The console displays:

```
Password is set successfully.
```

Note The user name should not be configured as *administrator*. If it is set so, it will lead to the faliure of the password recovery process.

Re-imaging the CSACS 1120 Hard Drive

Use the CSACS 1120 Recovery CD-ROM to re-image the appliance if necessary.

Caution Performing this procedure destroys all data stored on the CSACS 1120.

To re-image your CSACS 1120:

Step 1 Connect a console to the CSACS 1120 console port. For the location of the console port, see Figure 1-3.

Step 2 Put the Recovery CD in the CSACS 1120 CD-ROM drive. See Figure 1-2.

Step 3 Power on the (or, if the CSACS 1120 is already running, reboot it). For more information, see Rebooting the CSACS 1120 from a Serial Console.

Result: The console displays:

```
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 At the `Enter menu item number: [ ]` prompt, enter `2`, and press **Enter**.

Result: The console displays:

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

Caution The next step erases the CSACS 1120 hard drive. You will permanently lose all system data that you have not backed up.

Step 5 Enter `Y`, and press **Enter**.

Result: The appliance processes the new image (this may take several minutes) while displaying odd characters and then displays the following message on the console:

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

Note The reimaging process may take several minutes to complete.

Step 6 Remove the Recovery CD from the CSACS 1120, and press **Enter** to restart the appliance.

Result: The CSACS 1120 reboots, performs some configurations, and reboots again. The configurations that occur after the first reboot take a significant amount of time, during which there is no feedback. This is normal system behavior.

Note After re-imaging the CSACS 1120 hard drive, you must once again perform initial configuration of the CSACS 1120. For detailed instructions, see Configuring CSACS 1120.

CHAPTER 5

Upgrading and Migrating to Cisco 1120 Secure Access Control Server

This chapter details how to:

- Upgrade to Cisco Secure CSACS 1120 4.2.
- Migrate from an ACS for Windows server to CSACS 1120.
- Migrate ACS SE from an earlier hardware platform to the CSACS 1120 platform.

This chapter contains:

Upgrade Scenarios

CSACS 1120 supports the following upgrade scenarios:

- **ACS 3.x to ACS 3.3.x**—You can upgrade ACS 3.2.x or 3.3.x (ACS 3.2.1, 3.2.2, 3.2.3, 3.3.1, 3.3.2) to ACS 3.3.3 or 3.3.4 on all ACS SE hardware platforms (the Cisco 1111 SE appliance, the Cisco 1112 SE appliance, and the Cisco 1113 SE appliance).
- **ACS 3.3.3 to 3.3.4**— You can upgrade ACS 3.3.3 to ACS 3.3.4 on all ACS SE hardware platforms (the Cisco 1111 SE appliance, the Cisco 1112 SE appliance, and the Cisco 1113 SE appliance).
- **ACS 3.3.x to ACS 4.1.1.23 or ACS 4.1.1.24**— You can upgrade from ACS 3.3.x (ACS 3.2.1, 3.2.2, 3.2.3, 3.3.1, 3.3.2, or 3.3.4) to ACS 4.1.1.23 or ACS 4.1.1.24 on all ACS SE hardware platforms (the Cisco 1111 SE appliance, the Cisco 1112 SE appliance, and the Cisco 1113 SE appliance).
- **ACS 4.0 to ACS 4.1.1.23 or ACS 4.1.1.24**— You can upgrade from ACS 4.0 to ACS 4.1.1.23 or ACS 4.1.1.24 on all ACS SE hardware platforms (the Cisco 1111 SE appliance, the Cisco 1112 SE appliance and the Cisco 1113 SE appliance).

- **ACS 4.1.1.23 or ACS 4.1.1.24 to ACS 4.1.3 or ACS 4.1.4**— You can upgrade from ACS 4.1.1.23, 4.1.1.24, to ACS 4.1.3 or 4.1.4 on all ACS SE hardware platforms (the Cisco 1111 SE appliance, the Cisco 1112 SE appliance and the Cisco 1113 SE appliance).
- **ACS 4.1 to ACS 4.2**— You can upgrade from ACS 4.1.1.23, 4.1.1.24, 4.1.2, 4.1.3 or 4.1.4 to ACS 4.2 on all ACS SE hardware platforms (the Cisco 1112 SE appliance and the Cisco 1113 SE appliance) supported by 4.2. You must do a re-image of ACS 4.2 and restore the ACS 4.1 configuration.

Note You cannot directly upgrade ACS 3.2.x or 3.3.x or 4.0 to ACS 4.2.You must upgrade to ACS 4.1 and then do a re-image of ACS 4.2. Before you begin the 4.2 upgrade procedure, you must back up the ACS 4.1 configuration.

Migration Scenarios

ACS Solution Engine supports the following migration scenarios:

- **ACS for Windows to CSACS 1120 Migration**— You can migrate data from an ACS for Windows server to the CSACS 1120 for 4.2.
- **Hardware to Hardware Migration**—You can migrate data from earlier versions of the ACS SE (the Cisco 1111, 1112, and 1113 platforms) to the CSACS 1120 platform.

Note Before you begin any migration process, we recommend that you back up the ACS 4.1 configuration (either from 1111, or 1112, or 1113) and then restore the ACS 4.1 configuration in ACS 4.2. ACS 4.2 does not support the Cisco 1111 platform.

Upgrade Paths

Depending on the ACS version from which you upgrade, you can take different paths for upgrading to CSACS 1120. You only can upgrade to ACS 4.2 from ACS version 3.2.x, 3.3.x, 3.3.3 or 4.0, if you have first upgraded to ACS 4.1.

Note Before you begin any upgrade procedure, we recommend that you back up your existing data and configuration. When, upgrading do a re-image of ACS 4.2 and then restore the ACS 4.1 configuration.

Table 5-1 describes the various upgrade use cases that you can use to decide the appropriate upgrade path to follow.

Note The CSACS 1120 Overall Upgrade CD contains: the 3.3.4 SE upgrade, 4.1.1.24 SE upgrade, and Enable Password-CSCsh32888 patch files. You can use this CD to perform full upgrades with data restores.

Table 5-1 Upgrade Use Cases

Upgrade Path	Results
Full Upgrade for versions Prior to 3.3.3 to 4.2 To perform a full upgrade with data restore from: **1.** ACS SE 3.3.x to ACS SE 3.3.4 **a.** Back up your ACS SE 3.3.x configuration. **b.** Use the ACS 4.2 Overall Upgrade CD. **c.** From the CD, use the ACS SE 3.3.4 upgrade. ACS SE 3.3.4 is installed. For instructions on upgrading to ACS 3.3.3, see the latest version of the *Release Notes for Cisco Secure Access Control Server Solution Engine 3.3* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/3.3/release/notes/RNsol331.html	ACS SE 3.3.4 is installed.
2. ACS SE 3.3.4 to ACS SE 4.1.1.24 **a.** Back up your ACS SE 3.3.4 configuration. **b.** Use the ACS 4.2 Overall Upgrade CD. **c.** From the CD, use the 4.1.1.24 upgrade. ACS SE 4.1.1.24 is installed. For instructions on upgrading to ACS 3.3.3, see the latest version of the *Release Notes for Cisco Secure Access Control Server Solution Engine 3.3* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/3.3/release/notes/RNsol331.html	ACS SE 4.1.1.24 is installed.
3. ACS SE 4.1.1.24 to ACS 4.2 **a.** Back up your ACS 4.1.1.24 configuration. **b.** Use the ACS 4.2 Recovery DVD to re-image the CSACS 1120 with the 4.2 version. ACS 4.2 is installed. **c.** Restore the 4.1.1.24 configuration. For instructions on upgrading to ACS 4.1.1.24, see the latest version of the *Release Notes for Cisco Secure Access Control Server Solution Engine 4.1.1.24* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1.2/release/notes/acs412.html	ACS 4.2 is installed. ACS SE 4.1.1.24 configuration is upgraded to ACS SE 4.2 configuration.

Table 5-1 Upgrade Use Cases

Upgrade Path	Results
Full Upgrade from versions 3.3.3 or 3.3.4 to 4.2 To perform a full upgrade with data restore from: **1.** ACS SE 3.3.3 or 3.3.4 to ACS 4.2 **a.** Back up your ACS SE 3.3.3 or 3.3.4 configuration. **b.** Use the ACS 4.2 Overall Upgrade CD. **c.** From the CD, use the ACS SE 4.1.1.24 upgrade. ACS SE 4.1.1.24 is installed. For instructions on upgrading to ACS 4.1.1.24, see the latest version of the *Release Notes for Cisco Secure Access Control Server Solution Engine 4.1.1.24* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1.2/release/notes/acs412.html	ACS SE 4.1.1.24 is installed.
2. ACS SE 4.1.1.24 to ACS 4.2 **a.** Back up your 4.1.1.24 configuration. **b.** Use the ACS 4.2 Recovery DVD to re-image the CSACS 1120 with the 4.2 version. ACS SE 4.2 is installed. **c.** Restore the 4.1.1.24 configuration. For instructions on upgrading to ACS 4.2, see the latest version of the *Release Notes for Cisco Secure Access Control Server Solution Engine 4.2* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/release/notes/ACS42_RN.html	ACS 4.2 is installed. ACS SE 4.1.1.24 configuration is upgraded to ACS SE 4.2 configuration.

Table 5-1 Upgrade Use Cases

Upgrade Path	Results
Full Upgrade from version 4.0 to 4.2 To perform a full upgrade with data restore from: **1.** ACS SE 4.0 to ACS SE 4.1.1.24 **a.** Install the CSCsh32888 patch before taking a back up of the ACS SE 4.0 configuration. **b.** Back up your ACS SE 4.0 configuration. **c.** Use the ACS 4.2 Overall Upgrade CD. **d.** From the CD, use the ACS SE 4.1.1.24 upgrade. ACS SE 4.1.1.24 is installed. For instructions on upgrading to ACS 4.1.1.24, see the latest version of the *Release Notes for Cisco Secure Access Control Server Solution Engine 4.1.1.24* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1.2/release/notes/acs412.html	ACS SE 4.1.1.24 is installed.
2. ACS SE 4.1.1.24 to ACS 4.2 **a.** Back up your 4.1.1.24 configuration. **b.** Use the ACS 4.2 Recovery DVD to re-image the CSACS 1120 with the 4.2 version. ACS 4.2 is installed. **c.** Restore the 4.1.1.24 configuration. For instructions on upgrading to ACS 4.2, see the latest version of the *Release Notes for Cisco Secure Access Control Server Solution Engine 4.2* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/release/notes/ACS42_RN.html	ACS 4.2 is installed. ACS SE 4.1.1.24 configuration is upgraded to ACS 4.2 configuration.

Note If you use ACS Remote Agents, after any type of upgrade to ACS 4.2, you must uninstall your old version of ACS Remote Agents, and install Remote Agents for ACS 4.2.

Upgrade Procedure

This section contains:

- Performing a Full Upgrade from ACS SE 3.3.3 to ACS SE 4.1.
- Reimaging the CSACS 1120 with the ACS 4.2 Recovery DVD.
- Restoring the ACS SE 4.1.1.24 Configuration.

Performing a Full Upgrade from ACS SE 3.3.3 to ACS SE 4.1

You can use the ACS upgrade mechanism to upgrade from ACS SE 3.3.3, 3.3.4, 4.0.1 to ACS SE 4.1.1.24. This section describes the procedure for performing a full upgrade from ACS SE 3.3.3 to ACS SE 4.1. using the upgrade package mechanism.

Note You can follow the same procedure for all upgrades mentioned in Table 5-1.

Before You Begin

Back up your existing data and configuration. The first back up is for ensuring that you have the 3.3.3 original data backed up.

Caution Back up and restore are supported and tested only when done on the same version. For example, back up on 4.1 and restore on 4.1 is supported; not back up on 3.3.3 and restore on 4.1. However, there is an exception to ACS 4.2 as you can restore the 4.1 configuration after upgrading to 4.2.

To upgrade ACS SE 3.3.3 to ACS SE 4.1:

Step 1 Obtain the ACS SE 4.1.1.24 upgrade CD.

Step 2 If the ACS SE is running CSAgent, you must disable the **CSAgent** service before upgrading. You can do so at the console or in the web interface (ACS GUI). Using the:

- Console, enter `show`. If the **CSAgent** service is running, enter `stop csagent`.
- Web interface, choose **System Configuration** > **Appliance Configuration** and verify that the **CSA Enabled** check box is unchecked. If it is checked, then uncheck the **CSA Enabled** check box and click **Submit**.

Step 3 If you do not have a GUI administrator account on the ACS SE, create a new GUI administrator account from the web interface:

a. Start the web interface.

b. Click **Administration Control**.

   The Administration Control page opens.

c. Click **Add Administrator**.

   The Add Administrator page opens.

d. Add a new administrator and grant all administrative privileges to the administrator.

Note When you create a GUI administrator account, you will have two administrator accounts for the ACS SE: a GUI account and a CLI account.

Warning **If you do not have a GUI administrator account; then, after the upgrade is complete, you will not be able to log in to the ACS SE from the web interface.**

Step 4 Insert the ACS SE 4.1.1.24 Upgrade CD into the CD-ROM drive on the distribution server (the server from which you are performing the upgrade).

Step 5 Download the ACS Management Upgrade package:

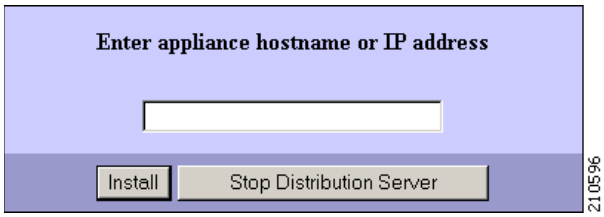
a. Open the upgrade CD.

b. Go to the */Upgrade Appliance management ACS 4.1* folder.

c. Double-click the *autorun.bat* icon.

The download utility starts. You are prompted to enter the hostname or IP address of the appliance, as shown in Figure 5-1.

Figure 5-1 Appliance Prompt



d. Enter the hostname or the IP address of the distribution server and click **Install**.

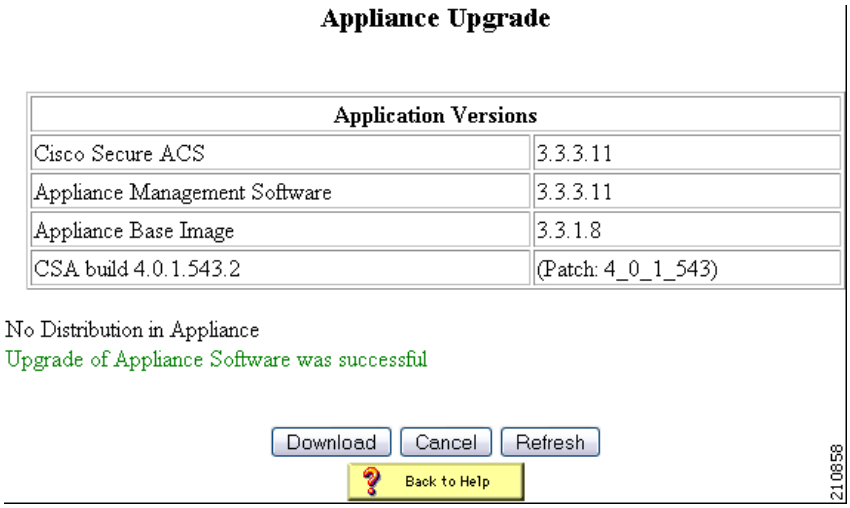
The web interface starts.

e. Log in to the web interface.

f. Choose **System Configuration > Appliance Upgrade Status**.

The Appliance Upgrade page opens, as shown in Figure 5-2.

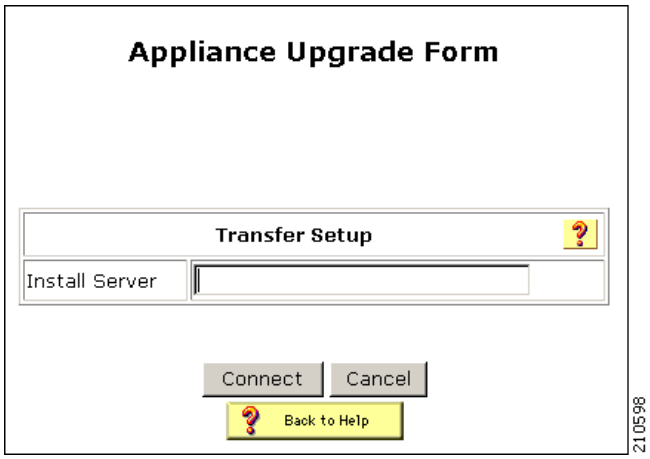
Figure 5-2 Appliance Upgrade Page



g. Click **Download**.

The Appliance Upgrade Form page opens, as shown in Figure 5-3. On this page, enter the IP address of the distribution server.

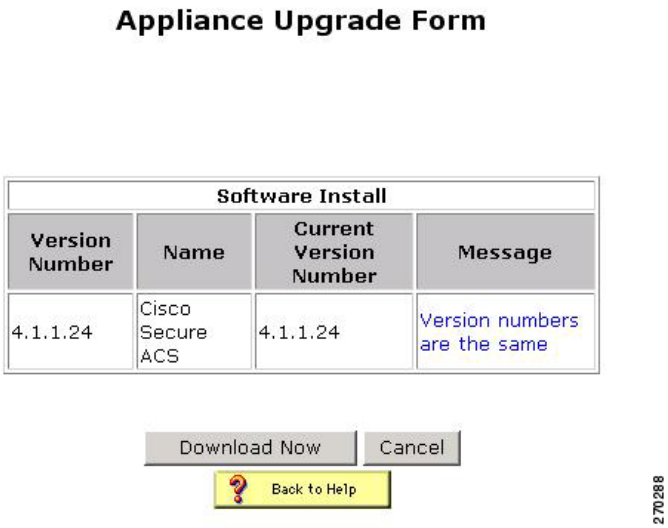
Figure 5-3 Appliance Upgrade Form with Text Box for the Distribution Server



h. Enter the IP address of the distribution server and click **Connect**.

The Appliance Upgrade Form page opens, as shown in Figure 5-4. This page lists the current version number of the appliance-management software.

Figure 5-4 Appliance Upgrade Form

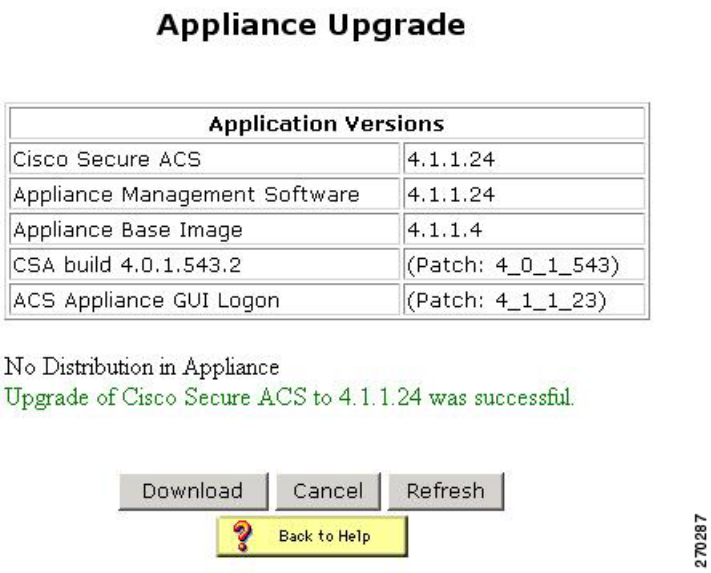


i. Click **Download Now**.

The upgrade utility downloads the upgrade image.

The Appliance Upgrade page opens, as shown in Figure 5-5. The Appliance Versions table provides information about the software version.

Figure 5-5 Appliance Upgrade Page



j. Click **Apply Upgrade**.

The upgrade utility applies the management software upgrade.

Note This process takes several minutes. The system reboots several times.

Step 6 Download and apply the ACS Software Upgrade package.

a. Go to the */Upgrade package software for appliance ACS 4.1* folder on the upgrade CD.

b. Double-click the *autorun.bat* icon.

The download utility starts. You are prompted to enter the hostname or IP address of the appliance, as shown in Figure 5-1.

c. Enter the hostname or the IP address of the distribution server and click **Install**.

The ACS web interface starts.

d. Log in to the web interface.

e. Choose **System Configuration** > **Appliance Upgrade Status**.

The Appliance Upgrade page opens, as shown in Figure 5-2.

f. Download and install the software upgrade.

The steps for downloading and installing the software upgrade package are the same as the steps for installing the management software as described in Step 5.

Note If you complete the upgrade and the ACS console displays the message `Appliance upgrade in progress`, this indicates that the upgrade progress is hanging.

If this condition occurs, start an ACS console session and enter the command **`download`** `[hostAddress]`, where `hostAddress` can be any IP address. This action releases the ACS console from the upgrade process.

Step 7 Back up the upgraded ACS SE data and configuration.

To upgrade the ACS SE appliance to the latest Microsoft hotfixes, you must re-image the ACS SE device. Because reimaging destroys all of the existing data on the device, you must first back up your existing data and then restore it 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 latest version of the *User Guide for Cisco Secure ACS 4.2*.
- The CLI **backup** command, which you enter from the serial console. For more information, see Backing Up ACS Data from the Serial Console.

Note Use this backup to restore the data after you recover the ACS SE 4.1 base image.

Step 8 Use the Recovery DVD for your CSACS 1120 hardware version. If your CSACS 1120 is a:

Step 9 Perform an initial configuration of the CSACS 1120. For more information, see Configuring CSACS 1120.

Step 10 Restore the data that you previously backed up in Step 7 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 latest version of the *User Guide for Cisco Secure ACS 4.2*.
- **The restore** command, which you enter from the serial console. For more information, see Restoring ACS Data from the Serial Console.

Step 11 Verify that CSAgent 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, check it and click **Submit**.

Reimaging the CSACS 1120 with the ACS 4.2 Recovery DVD

This section describes the procedure of reimaging the appliance using the ACS 4.2 Recovery DVD.

To re-image the appliance:

Step 1 Obtain the ACS 4.2 Recovery DVD.

Step 2 Insert the ACS 4.2 Recovery DVD into the DVD drive and reboot the CSACS 1120.

Result: The console displays:

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

Step 3 From the list of options on the screen, enter **`two`** in the `Enter menu item number: [ ]`: prompt.

The re-image process begins automatically.

Step 4 This process may take a few minutes. Once the re-image process is complete, the console displays:

```
Remove disk and press enter.
```

Step 5 Remove the ACS 4.2 Recovery DVD and press **Enter**.

The CSACS 1120 reboots and the initial configuration screen appears.

Step 6 Configure the CSACS 1120 by following the steps provided in the section, Chapter 3, "Configuring CSACS 1120".

Restoring the ACS SE 4.1.1.24 Configuration

This section describes the procedure for restoring the ACS SE 4.1.1.24 configuration in the appliance after installing ACS SE 4.2.

To restore the ACS SE 4.1.1.24 configuration:

Step 1 Log in as the GUI administrator.

Step 2 In the navigation bar, click **System Configuration**.

The **System Configuration** page opens.

Step 3 Click **ACS Restore**.

The **ACS System Restore Setup** page opens.

Step 4 Enter the name of the directory where you have backed up the file and click **Ok**.

A list backed up files will appear.

Step 5 From the list, select the ACS SE 4.1.1.24 file to be restored.

Step 6 In the **Select Components To Restore** dialog box, check the components you want to restore.

Step 7 In the **Restore Settings** dialog box, check the **Restore from 4.1 backup file to ACS 4.2** option.

Click **Restore Now**.

The restore process begins.

Appliance Upgrade and Patches Procedure

This section contains:

- About Appliance Upgrades and Patches
- Distribution Server Requirements
- Upgrading an Appliance
- Transferring an Upgrade Package to an Appliance
- Applying an Upgrade to an Appliance

About Appliance Upgrades and Patches

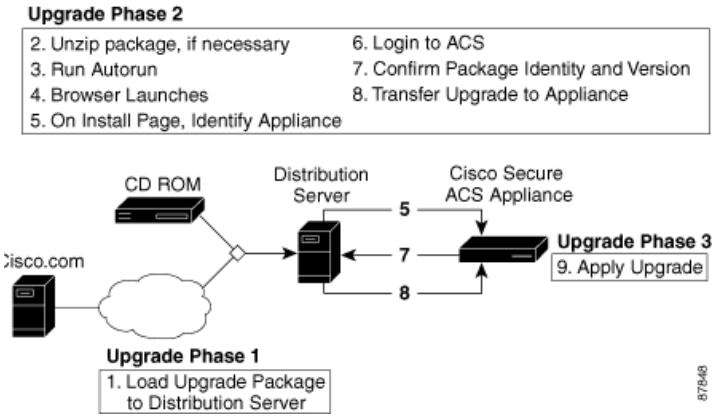
All upgrades and patches for ACS are packaged by using the upgrade mechanism. Use the following three-phase process to upgrade or patch your existing ACS.

Note To upgrade to ACS 4.2, you must re-image the appliance. You do not need to use the upgrade package mechanism.

- **Phase One**—Obtain an upgrade package and load it onto a computer designated as a distribution server for ACS upgrade distribution. The upgrade is available as a CD-ROM or a file that you download from Cisco.com.
- **Phase Two**—Transfer installation package files from the distribution server to the appliance. The HTTP server that is part of the installation package performs the file transfer. The upgrade files are signed and the signature is verified after uploading to ensure that the files have not been corrupted.
- **Phase Three**—Apply the upgrade to the appliance. Before the upgrade files are applied to the appliance, ACS verifies the digital signature on the files to ensure their authenticity and to verify that they are not corrupt.

Note While you apply the upgrade, ACS cannot provide AAA services. If it is not critical to immediately apply an upgrade package, you should consider performing this phase when ACS downtime will have the least impact on users. For example, when you apply the upgrade, it will stop the AAA servers, apply the new patch, and then restart the AAA servers again.

Figure 5-6 Appliance Upgrade Process



Distribution Server Requirements

The distribution server must meet the following requirements:

- For support, the distribution server must use an English-language version of one of the following operating systems:
  - Windows Server 2003 R2, Enterprise Edition
  - Windows 2000 Server with Service Pack 3 installed
  - Windows XP Professional with Service Pack 1 installed
  - Solaris 2.8

Note While the upgrade process may succeed by using an unsupported operating system, the list reflects the operating systems that we used to test the upgrade process. We do not support upgrades from distribution servers that use untested operating systems.

- If you acquire the upgrade package on CD, the distribution server must have a CD-ROM drive or must be able to use the CD-ROM drive on another computer that you can access.
- TCP port 8080 should not be in use on the distribution server. The upgrade process requires exclusive control of port 8080.

Tip We recommend that no other web server runs on the distribution server.

- A supported web browser should be available on the distribution server. If necessary, you can use a web browser on a different computer than the distribution server. For a list of supported browsers, see the latest version of the *Release Notes for Cisco Secure ACS Release 4.2*. The most recent revision to the Release Notes is posted on Cisco.com.

Gateway devices between the distribution server and any appliance that you want to upgrade must permit HTTP traffic to the distribution server on port 8080. They must also permit an ACS remote administrative session; therefore, they must permit HTTP traffic to the appliance on port 2002 and the range of ports allowed for administrative sessions. For more information, see the latest version the *User Guide for Cisco Secure Access Control Server 4.2*.

Upgrading an Appliance

Use the information in this section to upgrade the appliance software.

Before You Begin

Always back up ACS before upgrading. For information on backing up ACS, see the latest version of the *User Guide for Cisco Secure Access Control Server 4.2*.

To upgrade an appliance:

Step 1 Acquire the upgrade package. Acquisition of an upgrade package differs depending on the type of upgrade package and service agreement. For:

- **Commercial upgrade packages**—Contact your Cisco sales representative.
- **Maintenance contracts**—You may be able to download upgrade packages from Cisco.com. Contact your Cisco sales representative.
- **Upgrade packages that apply patches for specific issues**—Contact your TAC representative.

Step 2 Choose a computer to use as the distribution server. The distribution server must meet the requirements discussed in Distribution Server Requirements

Step 3 If you have acquired the upgrade package in a compressed file format, such as a *.zip* or *.gz*:

a. If you have not already done so, copy the upgrade package file to a directory on the distribution server.

b. Use the appropriate file decompression utility to extract the upgrade package.

Tip Consider extracting the upgrade package in a new directory that you create for the contents of the upgrade package.

Step 4 If you have acquired the upgrade package on CD, do not insert the CD in a CD-ROM drive until instructed to do so. The CD contains *autorun* files, and if the distribution server uses Microsoft Windows, the CD-ROM drive can prematurely start the *autorun* process.

Step 5 Transfer the upgrade package to an appliance. For detailed steps, see Transferring an Upgrade Package to an Appliance

The upgrade package is now on the appliance and ready to be installed.

Step 6 If the Cisco Security Agent is running on the appliance, disable the Cisco Security Agent. For detailed steps, see the latest version of the *User Guide for Cisco Secure Access Control Server 4.2*.

Step 7 Apply the upgrade package to the appliance. For detailed steps, see Applying an Upgrade to an Appliance.

ACS applies the upgrade and runs using the upgraded software.

Step 8 If you want the Cisco Security Agent to protect the appliance, enable it. For detailed steps, see the latest version of the *User Guide for Cisco Secure Access Control Server 4.2*.

Note System restarts performed during the upgrade do not re enable **CSAgent**.

Transferring an Upgrade Package to an Appliance

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

Note After you have performed this procedure, you must still apply the upgrade for it to become effective. For information on applying the upgrade, see Applying an Upgrade to an Appliance. For more general information about the upgrade process, see About Appliance Upgrades and Patches.

Before You Begin

You must have the upgrade package and a distribution server. For more information, see Upgrading an Appliance .

To transfer an upgrade to your appliance:

Step 1 If the distribution server uses Solaris, go to Step 2. If the distribution server uses Microsoft Windows:

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 this and *autorun* is enabled on the shared CD drive, the HTTP server included in the upgrade package starts on the other computer. For example, if computer A and computer B share a CD drive, and you use the CD drive on computer B where *autorun* is also enabled, the HTTP server starts on computer B.

b. If either of the following conditions are true:

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

Locate the *autorun.bat* file on the CD or in the directory to which you extracted the compressed upgrade package, and start the *autorun*.

c. The HTTP server starts, messages from *autorun.bat* appear in a console window, and ACS displays the following two browser windows:

- Use **Appliance Upgrade** to enter the appliance hostname or IP address.
- Use **New Desktop** to start transfers to other appliances.

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 to which you extracted the compressed upgrade package.

c. Run *autorun.sh*.

Tip If *autorun.sh* has insufficient permissions, enter `chmod +x autorun.sh` and repeat step c.

d. The HTTP server starts, messages from *autorun.bat* appear in a console window, and the following two browser windows appear:

- Use **Appliance Upgrade** to enter the appliance hostname or IP address.
- Use **New Desktop** to start transfers to other appliances.

Step 3 If no web browser opens after you have run the *autorun* file, start a web browser on the distribution server and open the following URL:

http://127.0.0.1:8080/install/index.html

Tip You can access the HTTP server on the distribution server from a web browser on a different computer using the following URL: *http://IP address:8080/install/index.html*, where *IP address* is the IP address of the distribution server.

Step 4 In the Appliance Upgrade browser window, enter the appliance IP address or hostname in the **Enter appliance hostname or IP address** box, and click **Install**.

The ACS login page for the specified appliance appears.

Step 5 Log in to the ACS web interface:

a. Enter a valid ACS administrator user name.

b. Enter the administrator password.

c. Click **Log in**.

Step 6 In the navigation bar, click **System Configuration**.

Step 7 Click **Appliance Upgrade Status**.

ACS displays the Appliance Upgrade page.

Step 8 Click **Download**.

ACS displays the Appliance Upgrade Form page. This page contains the Transfer Setup table, which enables you to identify the distribution server.

Step 9 In the **Install Server** box, enter the hostname or IP address of the distribution server.

Step 10 Click **Connect**.

The Appliance Upgrade Form page displays the Software Install table, which details the version and name of the upgrade available from the distribution server.

Step 11 Examine the Software Install table to confirm that the version, name, and condition of the upgrade is satisfactory, and click **Download Now**.

ACS displays the Appliance Upgrade page and the upgrade file is downloaded from the distribution server to the appliance. ACS displays the status of the download below the Appliance Versions table.

Tip On the Appliance Upgrade page, the system displays the message `Distribution Download in Progress`, followed by the number of downloaded kilobytes.

Step 12 If you want to update the transfer status message, click **Refresh**. **Refresh** exhibits the following behavior:

Tip During the transfer, you can click **Refresh** as often as necessary to update the status message.

- If you click **Refresh** while the transfer is in progress, ACS displays the number of downloaded kilobytes.
- If you click **Refresh** after the transfer is complete, ACS displays the Apply Upgrade button and the transfer progress text is replaced with a message indicating that an upgrade package is available on the appliance.

Step 13 To ensure that the download was successful and the upgrade is ready to be applied, confirm that the following message appears on the Appliance Upgrade page: `Ready to Upgrade to` *version*, where *version* is the version of the upgrade package you have transferred to the appliance.

The upgrade package is now successfully transferred to the appliance.

Step 14 If you want to transfer the upgrade package to another appliance, access the browser window titled **New Desktop**, click **Install Next**, and return to Step 4.

Tip If you know the URL for the web interface of another appliance, you can enter it in the browser location box and return to Step 5 to transfer the upgrade package to that appliance.

Step 15 If you are finished transferring upgrade packages to appliances, access the browser window titled **New Desktop** and click **Stop Distribution Server**.

The HTTP server stops and the distribution server releases the resources used by the HTTP server.

Step 16 If you want to apply the upgrade, perform the steps in Applying an Upgrade to an Appliance. Alternatively, you can use the **upgrade** command by using the serial console.

Applying an Upgrade to an Appliance

You use this procedure to apply an upgrade package to an ACS.

Note As as alternative, you can apply an upgrade package by using the **upgrade** command on the serial console.

Before You Begin

Before you apply the upgrade, be sure to:

- Transfer the upgrade package to the appliance. For detailed steps, see Transferring an Upgrade Package to an Appliance. For the steps required to upgrade an appliance, see Upgrading an Appliance.
- Back up ACS. For information about backing up ACS, see the latest version of the *User Guide for Cisco Secure Access Control Server 4.2*.
- Disable the **CSAgent** service. Application of the upgrade will fail if **CSAgent** is running. For detailed steps, see the latest version of the *User Guide for Cisco Secure Access Control Server 4.2*.

Note During the upgrade, ACS cannot provide AAA services. If it is not critical to immediately apply an upgrade package, consider performing this procedure when ACS downtime will have the least impact on users.

To apply an upgrade to an ACS:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Appliance Upgrade Status**.

ACS displays the Appliance Upgrade page.

Step 3 Verify that the message `Ready to Upgrade to` *version* appears, where *version* is the version of the upgrade package that is available on the appliance.

Step 4 Click **Apply Upgrade**.

ACS displays the Apply Upgrade Message table. This table displays messages about the upgrade process.

Step 5 For each message that ACS displays, you should carefully read the message and click the appropriate button.

Caution You might receive a warning message that an upgrade package is not verified. Before applying an upgrade or patch, ACS attempts to verify that the upgrade or patch is certified by Cisco. Some valid upgrade packages might not pass this verification, such as patches distributed for an urgent fix. Do not apply an upgrade package if you have unresolved concerns about the validity of the upgrade package.

After you have answered all confirmation prompts, ACS applies the upgrade. You should be aware of the following important points:

- During an upgrade, ACS services and the web interface are not available. When the upgrade is complete, the ACS services and the web interface become available.
- Application of an upgrade can take several minutes. A full upgrade of ACS takes longer if the ACS internal database contains a large number of user profiles.
- Upgrade of ACS usually requires the appliance to restart itself once or twice. Smaller patches might not require restarts.
- If the browser window is open and the web interface is not available, wait for the appliance to resume normal operation. Then close the original browser window, open a new browser window, and log in to ACS.

Caution Do not reset the appliance during application of an upgrade unless the TAC directs you to do so.

Step 6 After application of the upgrade, go to the Appliance Upgrade page and verify the versions of the software on the appliance. The Appliance Versions table lists the versions of software running on the appliance. Table entries should reflect the upgrade package that you applied.

Note If the browser window is open and the web interface is not available, wait for the appliance to resume normal operation. Then close the original browser window, open a new browser window, and log in to ACS.

Migrating from ACS for Windows 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. Whereas with ACS SW 4.1 and 4.2, you can restore the ACS SW 4.1 configuration in the ACS SE 4.2 appliance after migrating from ACS for Windows 4.1 to ACS SE 4.2.

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 If ACS runs on Windows NT 4.0, the following procedure will advise you when it is necessary to upgrade to Windows 2000 Server. The use of the backup and restore features is only supported between ACSs of the same version, to transfer data from ACS for Windows to ACS SE. But, in ACS 4.2 you can migrate from ACS SW 4.1 to ACS SE 4.2, by backing up the ACS SW 4.1 and restoring it in ACS SE 4.2. ACS for Windows 4.2 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 the Cisco 1120 Secure Access Control Server 4.2".

Note If you migrate from ACS SW 4.1 or if you already have ACS SW 4.2 installed, you do not need to install ACS SW 4.2. You only have to back up and restore the ACS SW 4.1 configuration in ACS SW 4.2.

Step 2 On the ACS server, upgrade ACS for Windows to version 4.2. If you do not have a license for version 4.2, you can use the trial version, available at http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des.

Note If you are running ACS 2.0 on Windows NT 4.0, upgrade to ACS 3.0, and then migrate to Windows 2000 Server before upgrading to ACS 4.2. Only ACS 3.0 and previous releases can run on Windows NT. For information about upgrading to ACS 3.0 or about migrating to Windows 2000 Server, see the latest version of the *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 4.2, use the ACS Backup feature to back up the database. For more information about the ACS Backup feature, see the latest version of 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 4.2 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 for ACS 4.2, use the ACS Restore feature to restore the database. For more information about restoring databases, see the latest version of the *User Guide for Cisco Secure ACS 4.2*.

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

Step 6 Continuing in the web interface, 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 CSACS 1120 IP Address.

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.

Migrating ACS SE on the ACS 1111 or ACS 1112 or ACS 1113 Platform to CSACS 1120

Table 5-2 indicates the Cisco Secure ACS software versions that each Cisco Secure ACS SE platform supports.

Table 5-2 Supported Versions

Cisco Secure ACS Solution Engine Platform	Cisco Secure ACS version 4.2	Cisco Secure ACS version 4.0.1 and 4.1	Cisco Secure ACS version 3.3.4	Cisco Secure ACS version 3.2
Cisco 1111	No	Yes	Yes	Yes
Cisco 1112	Yes	Yes	Yes	No
Cisco 1113	Yes	Yes	Yes	No
CSACS 1120	Yes	No	No	No

To migrate the ACS software running on a previous SE appliance platform (the Cisco 1111, the Cisco 1112 or the Cisco 1113) to run on the ACS 4.2 CSACS 1120:

Step 1 Upgrade the software on a previous SE hardware platform (the Cisco 1111 or the Cisco 1112) to ACS version 4.1 by using the full upgrade method. For information on this method, see Upgrade Procedure.

Step 2 Back up the 4.1 software on the previous SE hardware platform.

Step 3 Use the ACS 4.2 Recovery DVD to re-image the appliance with ACS 4.2 and then restore the 4.1 configuration.

For information on Steps 2 and 3, see Migrating from ACS for Windows to ACS SE.

APPENDIX A

Site Log

The site log provides a record of all actions related to installing and maintaining the CSACS 120 Series appliance. Keep the log in an accessible place near the appliance chassis so that anyone who performs tasks has access to it. Use the installation checklist (see the Installation Checklist, page 2-13) to verify the steps for the installation and maintenance process of your appliance.

Site Log entries might include the following:

- Installation progress—Make a copy of the appliance installation checklist, and insert it into the site log. Make entries as you complete each task.
- Upgrade, removal, and maintenance procedures—Use the site log as a record of ongoing appliance maintenance and expansion history. Each time a task is performed on the appliance, update the site log to reflect the following information:
  - Configuration changes
  - Maintenance schedules and requirements
  - Maintenance procedures performed
  - Intermittent problems
  - Comments and notes

Table A-1 shows a sample site log. Make copies of the sample, or design your own site log to meet the needs of your site and equipment.

Table A-1 Site Log

Date	Description of Action Performed or Symptom Observed	Initials

Table A-1 Site Log

Date	Description of Action Performed or Symptom Observed	Initials

APPENDIX **B**

Windows Service Advisement

The operating system for the CSACS 1120 is a customized and minimized version of the Windows 2003 operating system. The CSACS 1120 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
- Services that are Not Run, page B-2

Services That are Run

Table B-1 lists the services that are run on the CSACS 1120.

Table B-1 Operating System Services Automatically Run by CSACS 1120

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 the 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 B-1 Operating System Services Automatically Run by CSACS 1120 (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.
Run as 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 login, network, and power events. Notifies COM+ Event System subscribers of these events.
Telnet	Allows a remote user to log on to the system and run console programs using the command line.
Windows Management Instrumentation	Provides system management information.
Windows Management Instrumentation Driver Extensions	Provides systems management information to and from drivers.

Services that are Not Run

Table B-2 lists the operating system services that are not run on the CSACS 1120.

Table B-2 Disabled Operating System Services in CSACS 1120

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 website.
Background Intelligent Transfer Service	Transfers files in the background using idle network bandwidth. If the service is stopped, features such as Windows Update and MSN Explorer will be unable to automatically download programs and other information. If this service is disabled, any services
ClipBook	Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.
Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.
Distributed File System	Manages logical volumes distributed across a local or wide area network.

Table B-2 Disabled Operating System Services in CSACS 1120 (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 of 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 Login	Supports pass-through authentication of account login events for computers in a domain.
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop using NetMeeting.
Network DDE	Provides network transport and security for dynamic data exchange (DDE).
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE.
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 B-2 Disabled Operating System Services in CSACS 1120 (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 the *.msi* files.
Windows Time	Sets the computer clock.

APPENDIX C

Command Reference

This appendix summarizes the CLI commands of the CSACS 1120.

This appendix contains:

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 non-quoted set of characters.

Note Do not confuse the CSACS 1120 CLI with the IOS CLI. Though they are similar, they are not identical.

Command Privileges

Access to CLI commands on the CSACS 1120 is limited to those who physically connect via the console port and who possess the proper administrative credentials.

Note The CLI administrator does not have access to the ACS web GUI. To create an initial GUI administrator account that allows web access to the ACS GUI, use the **add guiadmin** command to create a GUI account. For more information about creating a GUI administrator account, see Setting Up a GUI Administrator Account.

For more information about establishing the console connection, see Configuring CSACS 1120.

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 of a valid command that 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, enter 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 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 CSACS 1120 commands.

Note Command names are case insensitive.

add guiadmin

To add a GUI account that a remote user can use to access the ACS web GUI, use the **add guiadmin** command:

`add guiadmin` [*admin*] [*password*]

Syntax Description

*admin*Username for the GUI account.

*password*Password for the GUI account.

Usage Guidelines

During initial installation, you are prompted to set up a GUI administration account that remote users can use to access and configure the CSACS 1120. The **add guiadmin** command is provided to set up additional web GUI accounts, and also to set up a new web GUI account if the initial web GUI account that you set up, does not work.

Example

The following command adds a GUI account *joeadmin* with the password *joltinjoe*:

```
add guiadmin joeadmin joltinjoe
```

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.

Example

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

Recommended Action `backup onyx joeadmin backupdata`

download

To download an upgrade image to the CSACS 1120 use the **download** command. Executing the **download** command establishes contact with the specified system, retrieves the manifest file from that system, and automatically downloads the upgrade image to the CSACS 1120. 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.

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 to 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 you can download 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(s) 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 to 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
```

lock guiadmin

To lock a GUI administrator account so that it cannot be used, use the **lock guiadmin** command:

lock guiadmin [*admin*] [*password*]

Syntax Description

*admin*Username for the GUI account.

*password*Password for the GUI account.

Usage Guidelines

During initial installation, the *setup* script prompts the installer to set up a GUI administration account that remote users can use to access and configure the ACS solution engine. A GUI administrator account can also be added by using the **add guiadmin** command.

GUI administrator accounts are not usable until they have been unlocked using the **unlock guiadmin** command. The **lock guiadmin** command is provided to lock web GUI accounts that have been unlocked.

Example

The following command locks a GUI administrator account *joeadmin* with the password *joltinjoe*:

lock guiadmin joeadmin joltinjoe

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 C-12.

ntpsync

Syntax Description

This command has no arguments or keywords.

Example

The following command uses the predefined NTP synchronization server to synchronize CSACS 1120 time to the NTP server time:

ntpsync

ping

To send ICMP echo_request packets for diagnosing basic network connectivity, uses 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 C-1 Syntax for the Ping Command

Argument	Description
-t	**Ping** the specified host until stopped.To see statistics and continue, enter Ctl-Break. To stop, enter Ctl-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 CSACS 1120, 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 CSACS 1120:

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 ACS Services from a Serial Console.

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, 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 it existed before the patch program was applied:

```
rollback remvptch4
```

set admin

To set the name of the CSACS 1120 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 CSACS 1120 administrator. For more information, see Resetting the CSACS 1120 Administrator Password.

Example

This command sets the administrator name to john:

```
set admin john
```

set dbpassword

To set the CSACS 1120 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 CSACS 1120 Database Password.

Example

The following command initiates the database password setting procedure:

```
set dbpassword
```

set domain

To set the DNS domain of the CSACS 1120, 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 CSACS 1120, use the **set hostname** command:

set hostname [*hostname*]

Syntax Description

*hostname*Name of the CSACS 1120.

Example

This command sets the CSACS 1120 name to *acs1*:

```
set hostname acs1
```

set ip

To set the CSACS 1120 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 CSACS 1120 IP Address.

Example

The following command begins the system IP address configuration.

```
set ip
```

set password

To set the CSACS 1120 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 CSACS 1120 Administrator Password.

Example

The following command initiates the password setting procedure:

```
set password
```

set time

To set the CSACS 1120 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 set 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.

You can also use the **set time** command to enable an NTP server to synchronize the CSACS 1120. 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 and the command reference ntpsync, page C-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 CSACS 1120, system load status, ACS service status, IP configuration, system time, and NTP settings, CSACS 1120 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 CSACS 1120 information:

```
show
```

shutdown

To shut down the CSACS 1120 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 ACS Services from a Serial Console.

Example

The following command restarts 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 they are restarted again, which may interfere with AAA services.

Note When you stop the **CSAgent** service, not only does the CSACS 1120 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 ACS Services from a Serial Console.

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 filepat**h [*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.
```

unlock guiadmin

To unlock a GUI administrator account that a remote user can use to access the ACS web GUI, use the **unlock guiadmin** command:

unlock guiadmin [*admin*] [*password*]

Syntax Description

*admin*Username for the GUI account.

*password*Password for the GUI account.

Usage Guidelines

During initial installation, the *setup* script prompts the installer to set up a GUI administrator account that remote users can use to access and configure the CSACS 1120. This account cannot be used until you unlock it by issuing the **unlock guiadmin** command.

In addition, you can add additional GUI administrator accounts by using the **add guiadmin** command. These accounts are not usable until they are unlocked by using the **unlock guidamin** command. And, if a GUI administrator account has been locked using the **lock guiadmin** command, you can use the **unlock guiadmin** command to unlock the account.

Example

The following command unlocks a GUI administrator account *joeadmin* with the password *joltinjoe*:

```
unlock guiadmin joeadmin joltinjoe
```

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 CSACS 1120.

Note Ensure that you have stopped the **CSAgent** prior to executing the **upgrade** command.

Example

The following initiates the second stage of an upgrade:

```
upgrade
```

APPENDIX D

Troubleshooting

The CSACS 1120 Series appliance undergoes extensive testing before it leaves the factory. If you encounter problems, use the information in this appendix to help isolate problems or to eliminate the appliance as the source of the problem.

Although an overtemperature or overvoltage condition is unlikely at initial startup, a discussion of environmental temperature and voltage monitoring functions is provided in Environmental Monitoring, page 1-9 section.

Note The procedures in this chapter assume that you are troubleshooting the initial CSACS 1120 Series appliance startup, and that the appliance is in the original factory configuration. If you have removed or replaced components, or changed any default settings, the recommendations in this chapter might not apply.

This appendix does not cover every possible issue that might occur on an appliance but instead focuses on those events that are frequently seen by the customer.

This appendix contains:

Troubleshooting Overview

At the initial system boot, you should verify the following:

- The external power cable is connected, and the proper power source is being applied. For more information, see Power Considerations, page 2-9, Powering Up the CSACS 1120 Series Appliance, page 3-12, and Troubleshooting the Power and Cooling Systems, page D-3.
- The appliance fan and blower are operating. See Airflow Guidelines, page 2-8 and Troubleshooting the Power and Cooling Systems, page D-3.
- The appliance software boots successfully.
- The adapter cards (if installed) are properly installed in their slots, and each initializes (is enabled by the appliance software) without problems.

When each of these conditions is met, the hardware installation is complete, and you should proceed to perform a basic configuration. For proper configuration features, see Chapter 3, "Installing and Configuring the Cisco 1120 Secure Access Control Server 4.2".

If you cannot locate the source of the problem, contact a customer service representative for information on how to proceed. For technical support information, see the *Cisco Information Packet* publication that is shipped with your appliance. Before you call, ensure that you have the following information ready:

- Appliance chassis type and serial number. For more information, see Cisco Product Identification Tool, page 1-3.
- Maintenance agreement or warranty information (see the *Cisco Information Packet*).
- Type of software and version number (if applicable).
- Date you received the new appliance.
- Brief description of the problem you are facing and the steps you have taken to isolate and resolve the problem.

Note Be sure to provide the customer service representative with any upgrade or maintenance information that was performed on the CSACS 1120 Series appliance after your initial installation. For site log information, see Creating a Site Log, page 2-14 and Site Log, page B-1

Problem Solving

The key to problem solving is to isolate the problem to a specific location by comparing what the CSACS 1120 Series appliance is doing with what it should be doing. In other words, when troubleshooting, define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

The following steps provide guidelines you can use during the troubleshooting process.

Step 1 Analyze the problem and create a clear problem statement. Define symptoms and potential causes.

Step 2 Gather the facts that you need to help isolate possible causes.

Step 3 Consider possible causes based on the facts that you gathered.

Step 4 Create an action plan based on those causes. Begin with the most likely problem and devise a plan in which you manipulate only one variable.

Step 5 Implement the action plan. Perform each step carefully while testing to see whether the symptom disappears.

Step 6 Analyze the results to determine whether the problem has been resolved. If the problem is resolved, consider the process complete.

Step 7 If the problem has not been resolved, create an action plan based on the next most probable cause on your list. Return to Step 4 and repeat the process until the problem is solved.

Step 8 Be sure to undo anything that you changed while implementing your action plan. Remember to change only one variable at a time.

Note The LEDs on the front-panel of the appliance enable you to determine the performance and operation of the appliance. For a description of these LEDs, see Reading the LEDs, page D-5.

When troubleshooting, check the following appliance subsystems first:

- Power and cooling systems (external power source, power cable, and appliance fans). Also, check for inadequate ventilation, air circulation, or environmental conditions.
- Adapter card—Checking the LEDs on the adapter card can help you to identify a failure.
- Cables—Verify that the external cables connecting the appliance to the network are all secure.

Troubleshooting the Power and Cooling Systems

Both the power LED and the fans can help you troubleshoot a power problem. Check the following items to help isolate the problem:

- When the CSACS 1120 Series appliance is connected to the power source, is the appliance power LED on the front-panel on? If not, check the AC power cord connection; if the power LED is still off, the problem might be due to a power supply failure.
- Does the appliance shut down after being on for only a short time?
  - Check for an environmentally induced shutdown. For more information, see Environmental Reporting Features, page D-3 section.
  - Check the fans. If the fans are not working, the appliance will overheat and shut itself down.
  - If the fans are not working, you might need to check the power supply connection to the fans.

    Checking this connection will require you to shut down the appliance, remove any external cables, and open up the appliance.
  - Ensure that the appliance intake and exhaust vents are clear.
  - Check the environmental site requirements in Temperature and Humidity Guidelines, page 2-9.
- Does the appliance partially boot, but the LEDs do not light? Check for a power supply failure by inspecting the power LED on the front-panel of the appliance:
  - If the LED is on, the power supply is functional.
  - If the LED is off, refer to the *Cisco Information Packet* for warranty information, or contact your customer service representative.

Environmental Reporting Features

The CSACS 1120 Series appliance has protection circuits that monitor and detect overcurrent, overvoltage, and overtemperature conditions inside the appliance. If the power supply shuts down or latches off, an AC cycle switches off for 15 seconds and switches on for 1 second to reset the power supply. For more information, see Environmental Monitoring, page 1-9.

The following conditions can cause an abnormally high appliance temperature:

- Fan failure
- Air conditioner failure in the room
- Airflow blocked to cooling vents

Take steps to correct the problem. For information about environmental operating conditions, see Temperature and Humidity Guidelines, page 2-9.

Troubleshooting Adapter Cards, Cables, and Connections

Network problems can be caused by an adapter card, cables or cable connections, or external devices such as a hub, wall jack, WAN interface, or terminal. Check for the following symptoms to help isolate a problem:

- Adapter card is not recognized by the CSACS 1120 Series appliance:
  - Ensure that the adapter card is firmly seated in its slot. For more information on adapter card installation and removal, see Installing and Removing a PCI Adapter Card, page 5-22.
  - Check the LEDs on the adapter card. Each adapter card has its own set of LEDs.
  - Verify that your software release supports the adapter card. Refer to the documentation that was included with your adapter card.
- Adapter card is recognized, but interface ports do not initialize:
  - Ensure that the adapter card is firmly seated in its slot.
  - Check external cable connections.
  - Verify that your software release supports the adapter card. Refer to the documentation that was included with your adapter card.
- The CSACS 1120 Series appliance does not boot properly, or it constantly or intermittently reboots:
  - Ensure that the adapter card is firmly seated in its slot.
  - Check the appliance chassis or the application software. For warranty information, refer to the *Cisco Information Packet* publication that is shipped with your appliance or contact your customer service representative.
- If you are using the console port with a terminal, and the CSACS 1120 Series appliance boots but the console screen is frozen:
  - Check the external console connection.
  - Verify that the parameters for your terminal are set as follows:

    (a) The terminal should have the same data rate that the appliance has (9600 bps is the default).

    (b) 8 data bits.

    (c) No parity generated or checked.

    (d) 1 stop bit.

- The CSACS 1120 Series appliance powers on and boots only when an adapter card is removed. Check the adapter card. For warranty information, refer to the *Cisco Information Packet* publication that is shipped with your appliance or contact your customer service representative.
- The CSACS 1120 Series appliance powers on and boots only when a particular cable is disconnected. There might be a problem with the cable. For warranty information, refer to the *Cisco Information Packet* publication that is shipped with your appliance or contact your customer service representative.

Reading the LEDs

There are several LEDs on the CSACS 1120 Series appliance. LEDs serve the following purposes:

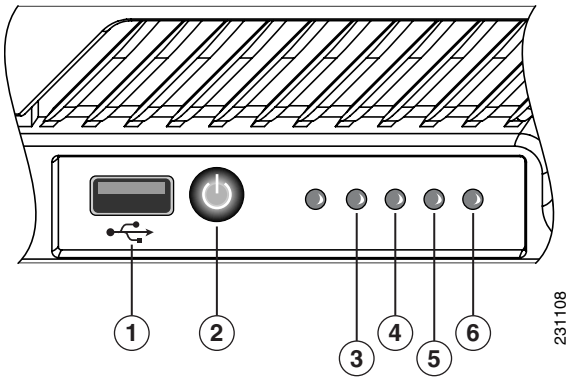
- Indicate that basic power is available to the appliance.
- Guide you to a broken adapter card, or to one that has failed its diagnostics.
- Indicate that traffic is flowing through the adapter card to the appliance.

The LEDs on the front-panel of the CSACS 1120 Series appliance and corresponding adapter card are aids for determining appliance and adapter performance and operation.

Front-Panel LEDs

Figure D-1 shows the locations of the appliance's front-panel LEDs.

Figure D-1 Front-Panel LEDs



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

1	USB port	**4**	Hard disk drive activity LED
2	Power button	**5**	NIC 1 LED
3	Appliance power LED	**6**	NIC 2 LED

Table D-1 describes the front-panel LEDs.

Table D-1 Front-Panel LED Descriptions

LED	Color	State	Description
Appliance power	Green	On	Power on
	Green	Blinking	Sleep (standby)
	Off	Off	Power off
Hard disk drive activity	Green	Random blinking	Hard disk drive activity
	Off	Off	No hard disk drive activity
NIC 1 and NIC 2	Green	On	NIC link, no access
	Green	Blinking	LAN access

Note Since ACS does not support Sleep (standby) mode, LED for Sleep (standby) is not applicable.

NIC LEDs

Figure D-2 shows the NIC 1 and NIC 2 LEDs located at the rear of the appliance. These LEDs indicate the connection activity and speed of the NIC ports.

Figure D-2 NIC 1 and NIC 2 LEDs

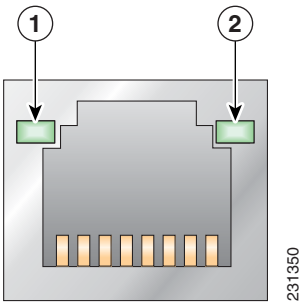


Table D-2 describes the activity and connection speed associated with each LED state.

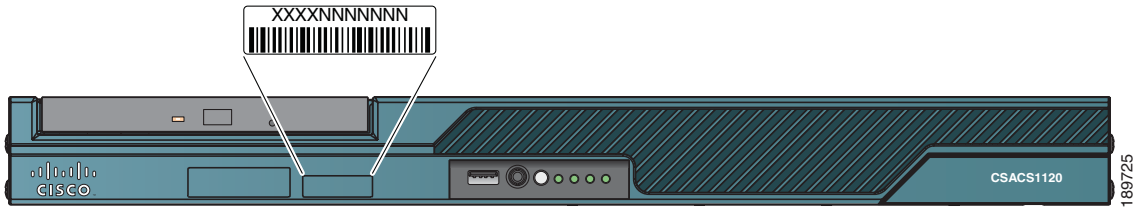
Table D-2 NIC 1 and NIC 2 LED Descriptions

LED	Color	State	Description
Left (1)	—	Off	No network connection
	Amber	Solid	Network connection
	Amber	Blinking	Transmit/receive activity
Right (2)	—	Off	10-Mb/s connection (if left LED is on or blinking)
	Amber	Solid	1000-Mb/s connection
	Green	Solid	100-Mb/s (or 1-Gb/s) connection

Product Serial Number Location

On the CSACS 1120 Series appliance, the serial number label is located on the front-panel of the appliance, at the lower-left. Figure D-3 shows the location of the serial number label.

Figure D-3 Serial Number Location for the CSACS 1120 Series Appliance



Note The serial number for the CSACS 1120 Series appliance is 11 characters long.

Cisco Product Identification Tool

The Cisco Product Identification (CPI) tool helps you retrieve the serial number of your Cisco products.

Before you submit a request for service online or by phone, use the CPI tool to locate your product serial number. You can access this tool from the Cisco Support website.

To access the CPI tool:

Step 1 Click the **Get Tools & Resources** link.

Step 2 Click the **All Tools (A-Z)** tab

Step 3 Choose **Cisco Product Identification Tool** from the alphabetical list.

This tool offers three search options:

- Search by product ID or model name.
- Browse for Cisco model.
- Copy and paste the output of the **show** command to identify the product.

Search results show an illustration of your product with the location of the serial number label highlighted. Locate the serial number label on your product and record the information before you place a service call.

You can access the CPI tool from Cisco.com at:

http://tools.cisco.com/Support/CPI/index.do

Access to the CPI tool on the Cisco Support 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:

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

APPENDIX **E**

Maintaining the Cisco 1120 Secure Access Control Server

The CSACS 1120 Series appliance is configured to order and is ready for installation when it leaves the factory. After you install and configure your appliance, you may have to perform specific maintenance procedures and operations to ensure that the appliance is operating properly.

These preventive procedures will maintain your appliance in good operating condition and minimize the need for costly, time-consuming service procedures.

Caution To help prevent problems, before performing any procedures in this chapter, review Safety Warnings and the Safety Guidelines sections.

The following sections discuss various environmental factors that can adversely affect appliance performance and longevity.

Maintaining Your Site Environment

Good preventive maintenance includes regular visual inspections of the appliance, including exterior cleaning and inspection.

This chapter contains:

- Cooling
- Temperature
- Humidity
- Altitude
- Electrostatic Discharge
- Electromagnetic and Radio Frequency Interference
- Magnetism
- Power Source Interruptions

General Exterior Cleaning and Inspection

This section details the cleaning requirements for exterior surfaces of the appliance. It also provides information on inspecting cables and adapter cards.

Caution Never spray cleaning solution on the surfaces of the appliance. Over spray can penetrate into the appliance and cause electrical problems and corrosion.

Appliance

Use a lint-free, nonabrasive cloth to perform cleaning. *Do not* use a solvent, abrasive cleaning agents, or tissue paper. If the appliance is dirty (for example, with thick dust), use a soft damp cloth and gently wipe the surface of the appliance.

Immediately wipe any water or liquid off from the appliance.

Dust and Particles

A clean operating environment can greatly reduce the negative effects of dust and other particles, which act as insulators and interfere with the operation of an appliance's mechanical components. In addition to regular cleaning, you should follow these guidelines to deter contamination of the appliance:

- Do not permit smoking anywhere near the appliance.
- Do not permit food or drink near the appliance.

Cables and Connectors

Periodically inspect cables and connectors to and from your appliance periodically to see if they are worn out or loose.

Adapter Cards

Check the connections on the adapter cards. Ensure that they are secured to the appliance and have not been jarred loose or mechanically damaged.

Corrosion

The oil from a person's fingers, or prolonged exposure to high temperature or humidity, can corrode the gold-plated edge connectors and pin connectors on adapter cards in the appliance. This corrosion on adapter card connectors is a gradual process that can eventually lead to intermittent failure of electrical circuits.

To prevent corrosion, you should avoid touching contacts on adapter cards. Protecting the appliance from corrosive elements is especially important in moist and salty environments, which tend to promote corrosion. Also, as a further deterrent to corrosion, the appliance should not be used in extreme temperatures, as explained in the Temperature, page E-3 section.

Cooling

Exhaust fans in the power supply and in the appliance cool the power supply and the appliance by drawing air in through various openings in the front of the appliance and blowing it out the back. However, the fans also draw dust and other particles into the appliance, causing contaminant buildup, which results in an increase in the appliance's internal temperature and interferes with the operation of various appliance components.

To avoid these conditions, we recommend keeping your work environment clean to reduce the amount of dust and dirt around the appliance, thereby reducing the amount of contaminants drawn into the appliance by the fans.

Temperature

Temperature extremes can cause a variety of problems, including premature aging and failure of integrated circuits (ICs) or mechanical failure of devices. Extreme temperature fluctuations can cause ICs to become loose in their sockets, causing expansion and contraction of disk drive platters, resulting in read or write data errors.

To minimize the negative effects of temperature on appliance performance, follow these guidelines:

- Ensure that the appliance is operated in an environment no colder than 50°F (10°C) and no hotter than 95°F (35°C).
- Ensure that the appliance has adequate ventilation. Do not place it within a closed-in wall unit or on top of cloth, which can act as insulation. Do not place it where it will receive direct sunlight, particularly in the afternoon. Do not place it next to a heat source of any kind, including heating vents during winter.

Adequate ventilation is particularly important at high altitudes. Appliance performance may not be optimum when the appliance is operating at high temperatures as well as high altitudes. Do the following:

- Ensure that all slots and openings on the appliance remain unobstructed, especially the fan vents on the back of the appliance.
- Clean the appliance at regular intervals to avoid any buildup of dust and debris, which can cause the appliance to overheat.
- If the appliance has been exposed to abnormally cold temperatures, allow a 2-hour warm-up period to bring it up to normal operating temperature before turning it on. Failure to do so may cause damage to internal components, particularly the hard disk drive.

Humidity

High-humidity conditions can cause moisture migration and penetration into the appliance. This moisture can cause corrosion of internal components and degradation of properties such as electrical resistance, thermal conductivity, physical strength, and size. Extreme moisture buildup inside the appliance can result in electrical shorts, which can cause serious damage to the appliance.

Each appliance is rated to operate at 8 to 80 percent relative humidity, with a humidity gradation of 10 percent per hour. Buildings in which climate is controlled by air conditioning in the warmer months and by heat during the colder months usually maintain an acceptable level of humidity for appliances. However, if an appliance is located in an unusually humid location, a dehumidifier can be used to maintain the humidity within an acceptable range.

Altitude

Operating an appliance at high altitudes (low atmospheric pressure) reduces the efficiency of forced and convection cooling which can result in electrical problems related to arcing and corona effects. This condition can also cause sealed components with internal pressure, such as electrolytic capacitors, to fail or perform at reduced efficiency.

Electrostatic Discharge

Electrostatic discharge (ESD) results from the buildup of static electricity on the human body and certain other objects. This static electricity is often produced by simple movements, such as walking across a carpet. ESD is a discharge of a static electrical charge that occurs when a person whose body contains such a charge touches a component in the appliance. This static discharge can cause components, especially ICs, to fail. ESD is a problem particularly in dry environments where the relative humidity is below 50 percent.

To reduce the effects of ESD, you should observe the following guidelines:

- Wear a grounding wrist strap. If a grounding wrist strap is unavailable, touch an unpainted metal surface on the appliance chassis periodically to neutralize any static charge.
- Keep components in their antistatic packaging until they are installed.
- Avoid wearing clothing made of wool or synthetic materials.

Electromagnetic and Radio Frequency Interference

Electromagnetic interference (EMI) and radio frequency interference (RFI) from an appliance can adversely affect devices such as radio and television receivers operating near the appliance. Radio frequencies emanating from an appliance can also interfere with cordless and low-power telephones.

RFI is defined as any EMI with a frequency above 10 kHz. This type of interference can travel from the appliance to other devices through the power cable and power source, or through the air, like transmitted radio waves. The Federal Communications Commission (FCC) publishes specific regulations to limit the amount of EMI and RFI emitted by computing equipment. Each appliance meets these FCC regulations.

To reduce the possibility of EMI and RFI, follow these guidelines:

- Operate the appliance only with the appliance cover installed.
- Ensure that the screws on all peripheral cable connectors are securely fastened to their corresponding connectors on the back of the appliance.
- Always use shielded cables with metal connector shells for attaching peripherals to the appliance.

Magnetism

Hard disk drives are susceptible to the effects of magnetism as they store data magnetically. Hard disk drives should never be stored near magnetic sources such as:

- Monitors
- Printers
- Telephones with real bells
- Fluorescent lights

Power Source Interruptions

Appliances are especially sensitive to variations in voltage supplied by the AC power source. Overvoltage, undervoltage, and transients (or spikes) can erase data from the memory or even cause components to fail. To protect against these types of problems, power cables should always be properly grounded and one, or both, of the following methods should be used:

- Place the appliance on a dedicated power circuit (rather than sharing a circuit with other electrical equipment). In general, do not allow the appliance to share a circuit with any of the following:
  - Copier machines
  - Teletype machines
  - Laser printers
  - Fax machines
  - Any other motorized equipment

Besides the above equipment, the greatest threats to an appliance's power supply are surges or blackouts caused by electrical storms.

If a blackout occurs—even a temporary one—while the appliance is turned on, turn off the appliance immediately and disconnect it from the electrical outlet. Leaving the appliance on may cause problems when the power is restored.

INDEX

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

T

U

W