

You'll be entered into a quarterly drawing for **free** Cisco Press books by returning this survey! Cisco is dedicated to customer satisfaction and would like to hear your thoughts on these printed manuals. Please visit the Cisco Product Comments on-line survey at www.cisco.com/go/crc to submit your comments about accessing Cisco technical manuals. Thank you for your tin

General Information

- 1 Years of networking experience: _____ Years of experience with Cisco products: _____
- 2 I have these network types: _____ LAN _____ Backbone _____ WAN
_____ Other: _____
- 3 I have these Cisco products: _____ Switches _____ Routers
_____ Other (specify models): _____
- 4 I perform these types of tasks: _____ H/W installation and/or maintenance _____ S/W configuration
_____ Network management _____ Other: _____
- 5 I use these types of documentation: _____ H/W installation _____ H/W configuration _____ S/W configuration
_____ Command reference _____ Quick reference _____ Release notes _____ Online help
_____ Other: _____
- 6 I access this information through: _____ % Cisco.com _____ % CD-ROM _____ % Printed manuals
_____ % Other: _____
- 7 I prefer this access method: _____ Cisco.com _____ CD-ROM _____ Printed manuals
_____ Other: _____
- 8 I use the following three product features the most: _____

Document Information

Document Title: Cisco ASA 5500 Series Hardware Installation Guide

Part Number: OL-10089-01 S/W Release (if applicable): _____

On a scale of 1–5 (5 being the best), please let us know how we rate in the following areas:

- _____ The document is complete. _____ The information is accurate.
_____ The information is well organized. _____ The information I wanted was easy to find.
_____ The document is written at my _____ The information I found was useful to my job.
_____ technical level of understanding.

Please comment on our lowest scores: _____

Mailing Information

Organization _____ Date _____

Contact Name _____

Mailing Address _____

City _____ State/Province _____ Zip/Postal Code _____

Country _____ Phone () _____ Extension _____

E-mail _____ Fax () _____

May we contact you further concerning our documentation? _____ Yes _____ No

You can also send us your comments by e-mail to bug-doc@cisco.com, or by fax to **408-527-8089**.

When mailing this card from outside of the United States, please enclose in an envelope addressed to the location on the back of this card with the required postage or fax to 1-408-527-8089.

BUSINESS REPLY MAIL

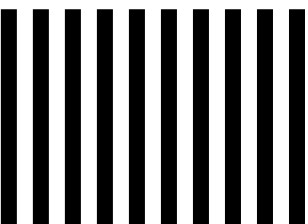
FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

DOCUMENT RESOURCE CONNECTION
CISCO SYSTEMS INC
170 WEST TASMAN DR
SAN JOSE CA 95134-9916



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES





Cisco ASA 5500 Series Hardware Installation Guide

Corporate Headquarters

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

Customer Order Number:
Text Part Number: OL-10089-01



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.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0601R)

Cisco ASA 5500 Series Hardware Installation Guide
© 2006 Cisco Systems, Inc. All rights reserved.



About This Guide	v
Document Objectives	v
Audience	v
Document Organization	vi
Document Conventions	vi
Safety Warning	vii
Installation Warnings	x
Where to Find Safety and Warning Information	xiii
Obtaining Documentation	xiv
Cisco.com	xiv
Documentation DVD	xiv
Ordering Documentation	xiv
Documentation Feedback	xv
Cisco Product Security Overview	xv
Reporting Security Problems in Cisco Products	xv
Obtaining Technical Assistance	xvi
Cisco Technical Support Website	xvi
Submitting a Service Request	xvi
Definitions of Service Request Severity	xvii
Obtaining Additional Publications and Information	xvii

CHAPTER 1

Preparing for Installation	1-1
Overview	1-1
Installation Overview	1-2
Safety Recommendations	1-2
Maintaining Safety with Electricity	1-3
Preventing Electrostatic Discharge Damage	1-4
General Site Requirements	1-4
Site Environment	1-4
Preventive Site Configuration	1-4
Power Supply Considerations	1-5
Configuring Equipment Racks	1-5

CHAPTER 2

ASA 5505 2-1

- Product Overview 2-2
- Memory Requirements 2-3
- Installing the Chassis 2-3
 - Connecting the Interface Cables 2-3
 - Powering on the ASA 5505 2-5
 - Installing a Cable Lock 2-6

CHAPTER 3

ASA 5510, ASA 5520, ASA 5540, and ASA 5550 3-1

- Product Overview 3-2
- Memory Requirements 3-5
- Installing the Chassis 3-5
 - Rack-Mounting the Chassis 3-6
 - Setting the Chassis on a Desktop 3-7
 - Connecting the Interface Cables 3-8

APPENDIX A

Installing and Replacing the SSM A-1

- Installing and Replacing the 4GE SSM A-1
 - Overview A-2
 - Installing the 4GE SSM A-3
 - Replacing the 4GE SSM A-4
 - Installing and Removing the SFP Modules A-4
 - SFP Module A-5
 - Installing the SFP Module A-6
 - Removing the SFP Module A-7
- Installing and Replacing the SSM A-8
 - Installing an SSM A-9
 - Replacing an SSM A-10

APPENDIX B

Maintenance and Upgrade Procedures B-1

- Removing and Replacing the Chassis Cover B-1
 - Removing the Chassis Cover B-1
 - Replacing the Chassis Cover B-3
- Working in an ESD Environment B-4
- Removing and Replacing the Power Supply B-4
 - Removing the AC Power Supply B-4
 - Replacing the AC Power Supply B-7
- Installing the DC Model B-8

Removing and Replacing the CompactFlash	B-10
Removing the System CompactFlash	B-10
Replacing the System CompactFlash	B-12
Removing the User CompactFlash	B-13
Replacing the User CompactFlash	B-14

APPENDIX C**Cable Pinouts C-1**

10/100/1000BaseT Connectors	C-1
Console Port (RJ-45)	C-2
RJ-45 to DB-9	C-3
MGMT 10/100/1000 Ethernet Port	C-3
Gigabit and Fibre Channel Ports	C-4

INDEX



About This Guide

This preface includes the following sections:

- [Document Objectives, page v](#)
- [Audience, page v](#)
- [Document Organization, page vi](#)
- [Document Conventions, page vi](#)
- [Safety Warning, page vii](#)
- [Installation Warnings, page x](#)
- [Obtaining Documentation, page xiv](#)
- [Documentation Feedback, page xv](#)
- [Cisco Product Security Overview, page xv](#)
- [Obtaining Technical Assistance, page xvi](#)
- [Obtaining Additional Publications and Information, page xvii](#)

Document Objectives

This guide describes how to install hardware components in the following Cisco ASA 5500 series adaptive security appliances.

Audience

This guide is for network administrators who perform any of the following tasks:

- Managing network security
- Installing and configuring firewalls
- Managing default and static routes, and TCP and UDP services

Document Organization

This guide includes the following chapters:

- [Chapter 1, “Preparing for Installation”](#) describes the installation overview, safety recommendations, and general site requirements.
- [Chapter 2, “ASA 5505”](#) describes the ASA 5505 product overview, and the installation procedures.
- [Chapter 3, “ASA 5510, ASA 5520, ASA 5540, and ASA 5550”](#) describes the ASA 5510, ASA 5520, ASA 5540, ASA 5550 product overview, and the installation procedures.
- [Appendix A, “Installing and Replacing the SSM,”](#) describes how to install and replace the SSM.
- [Appendix B, “Maintenance and Upgrade Procedures,”](#) describes the adaptive security appliance maintenance and upgrade procedures.
- [Appendix C, “Cable Pinouts,”](#) describes the cable pinouts.

Document Conventions

Command descriptions use these conventions:

- Braces ({ }) indicate a required choice.
- Square brackets ([]) indicate optional elements.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- **Boldface** indicates commands and keywords that are entered literally as shown.
- *Italics* indicate arguments for which you supply values.

Examples use these conventions:

- Examples depict screen displays and the command line in `screen` font.
- Information you need to enter in examples is shown in **boldface screen** font.
- Variables for which you must supply a value are shown in *italic screen* font.

Graphical user interface examples uses these conventions:

- **Boldface** indicates buttons and menu items.
- Selecting a menu item (or screen) is indicated by the following convention:
Click **Start > Settings > Control Panel**.



Note

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

Safety Warning



Warning

IMPORTANT SAFETY INSTRUCTIONS

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

Note: SAVE THESE INSTRUCTIONS

Waarschuwing

BELANGRIJKE VEILIGHEIDSINSTRUCTIES

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

Opmerking BEWAAR DEZE INSTRUCTIES.

Varoitus

TÄRKEITÄ TURVALLISUUTEEN LIITTYVIÄ OHJEITA

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

Huomautus SÄILYTÄ NÄMÄ OHJEET

Attention

IMPORTANTES INFORMATIONS DE SÉCURITÉ

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

Remarque CONSERVEZ CES INFORMATIONS

Warnung

WICHTIGE SICHERHEITSANWEISUNGEN

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

Hinweis BEWAHREN SIE DIESE SICHERHEITSANWEISUNGEN AUF

Figyelem FONTOS BIZTONSÁGI ELOÍRÁSOK

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

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Avvertenza IMPORTANTI ISTRUZIONI SULLA SICUREZZA

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

Nota CONSERVARE QUESTE ISTRUZIONI

Advarsel VIKTIGE SIKKERHETSINSTRUKSJONER

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

Merk TA VARE PÅ DISSE INSTRUKSJONENE

Aviso INSTRUÇÕES IMPORTANTES DE SEGURANÇA

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

Nota GUARDE ESTAS INSTRUÇÕES

¡Advertencia! INSTRUCCIONES IMPORTANTES DE SEGURIDAD

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

Nota GUARDE ESTAS INSTRUCCIONES

Varning! VIKTIGA SÄKERHETSANVISNINGAR

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

OBS! SPARA DESSA ANVISNINGAR

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。

Installation Warnings

Be sure to read the *Regulatory Compliance and Safety Information for the Cisco ASA 5500* document that accompanied this device before installing the chassis. This document contains important safety information. This section includes the following warnings:

- [Power Supply Disconnection Warning, page x](#)
- [Jewelry Removal Warning, page x](#)
- [Wrist Strap Warning, page xi](#)
- [Work During Lightning Activity Warning, page xi](#)
- [Installation Instructions Warning, page xi](#)
- [Chassis Warning for Rack-Mounting and Servicing, page xi](#)
- [Short-Circuit Protection Warning, page xi](#)
- [SELV Circuit Warning, page xi](#)
- [Ground Conductor Warning, page xi](#)
- [Blank Faceplates and Cover Panels Warning, page xii](#)
- [Product Disposal Warning, page xii](#)
- [Short-Circuit Protection Warning, page xii](#)
- [Compliance with Local and National Electrical Codes Warning, page xii](#)
- [DC Power Connection Warning, page xii](#)
- [AC Power Disconnection Warning, page xii](#)
- [TN Power Warning, page xii](#)
- [48 VDC Power System, page xiii](#)
- [Multiple Power Cord, page xiii](#)
- [Circuit Breaker \(15A\) Warning, page xiii](#)
- [Grounded Equipment Warning, page xiii](#)
- [Safety Cover Requirement, page xiii](#)
- [Faceplates and Cover Panel Requirement, page xiii](#)

Power Supply Disconnection Warning



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

Jewelry Removal Warning



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

Wrist Strap Warning



Warning

During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself. Statement 94

Work During Lightning Activity Warning



Warning

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

Installation Instructions Warning



Warning

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

Chassis Warning for Rack-Mounting and Servicing



Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety: This unit should be mounted at the bottom of the rack if it is the only unit in the rack. When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack. If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

Short-Circuit Protection Warning



Warning

This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations. Statement 1045

SELV Circuit Warning



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

Ground Conductor Warning



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

Blank Faceplates and Cover Panels Warning



Warning

Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Statement 1029

Product Disposal Warning



Warning

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

Short-Circuit Protection Warning



Warning

This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations. Statement 1045

Compliance with Local and National Electrical Codes Warning



Warning

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

DC Power Connection Warning



Warning

After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position. Statement 8

AC Power Disconnection Warning



Warning

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

TN Power Warning



Warning

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

48 VDC Power System



Warning

The customer 48 volt power system must provide reinforced insulation between the primary AC power and the 48 VDC output. Statement 128

Multiple Power Cord



Warning

This unit has more than one power cord. To reduce the risk of electric shock when servicing a unit, disconnect the power cord of the power strip that the unit is plugged into. Statement 137

Circuit Breaker (15A) Warning



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

Grounded Equipment Warning



Warning

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

Safety Cover Requirement



Warning

The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards. Statement 117

Faceplates and Cover Panel Requirement



Warning

Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Statement 142

Where to Find Safety and Warning Information

For safety and warning information, see the *Regulatory Compliance and Safety Information for the Cisco ASA 5500* document that accompanied the product. This document describes the international agency compliance and safety information for the Cisco ASA 5500 series adaptive security appliance. It also includes translations of the safety warnings.

Obtaining Documentation

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

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

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

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical 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 this URL:

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



Note

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

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

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

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

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

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

<http://www.ciscopress.com>

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

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

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

<http://www.cisco.com/ipj>

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

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



Preparing for Installation

The information in this guide applies to the following ASA 5500 series models: ASA 5505, ASA 5510, ASA 5520, ASA 5540, and ASA 5550. In this guide, references to “Cisco ASA 5500 series adaptive security appliance” and “adaptive security appliance” apply to all models unless specifically noted otherwise.

This chapter describes the steps to follow before installing new hardware or performing hardware upgrades, and includes the following topics:

- [Overview, page 1-1](#)
- [Installation Overview, page 1-2](#)
- [Safety Recommendations, page 1-2](#)
- [General Site Requirements, page 1-4](#)

Overview

The adaptive security appliance delivers unprecedented levels of defense against threats to the network with deeper web inspection and flow-specific analysis, improved secure connectivity via end-point security posture validation, and voice and video over VPN support. It also provides enhanced support for intelligent information networks through improved network integration, resiliency, and scalability.

The adaptive security appliance software combines firewall, VPN concentrator, and intrusion prevention software functionality into one software image. Previously, these functions were available in three separate devices, each with its own software and hardware. Combining the functionality into just one software image provides significant improvements in the available features.

Installation Overview

To prepare for the installation of the chassis, perform the following steps:

-
- Step 1** Review the safety precautions outlined in the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* document.
 - Step 2** Read the release notes for the respective software version.
 - Step 3** Unpack the chassis. An accessory kit ships with the chassis and includes the following items: documentation, a product CD, a power cord (AC models only), two RJ-45 Ethernet cables, one RJ-45 to DB-9 console cable, a rack-mounting kit, and four self-adhesive feet (for desktop mounting).
 - Step 4** Place the chassis on a stable work surface.
-

Safety Recommendations

Use the following guidelines and the information in the following sections to help ensure your safety and protect the adaptive security appliance. The list of guidelines may not address all potentially hazardous situations in your working environment, so be alert and exercise good judgement at all times.

**Note**

If you need to remove the chassis cover to install a hardware component, such as additional memory or an interface card, doing so does not affect your Cisco warranty. Upgrading the adaptive security appliance does not require any special tools and does not create any radio frequency leaks.

The safety guidelines are as follows:

- Keep the chassis area clear and dust-free before, during and after installation.
- Keep tools away from walk areas where you and others could fall over them.
- Do not wear loose clothing or jewelry, such as earrings, bracelets, or chains, that could get caught in the chassis.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Never attempt to lift an object that is too heavy for one person to handle.

This section includes the following topics:

- [Maintaining Safety with Electricity, page 1-3](#)
- [Preventing Electrostatic Discharge Damage, page 1-4](#)

Maintaining Safety with Electricity



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

Follow these guidelines when working on equipment powered by electricity:

- Before beginning procedures that require access to the interior of the chassis, locate the emergency power-off switch for the room in which you are working. Then, if an electrical accident occurs, you can act quickly to turn off the power.
- Do not work alone if potentially hazardous conditions exist anywhere in your work space.
- Never assume that power is disconnected from a circuit; always check the circuit.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- If an electrical accident occurs, proceed as follows:
 - Use caution; do not become a victim yourself.
 - Disconnect power from the system.
 - If possible, send another person to get medical aid. Otherwise, assess the condition of the victim and then call for help.
 - Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.
- Use the adaptive security appliance chassis within its marked electrical ratings and product usage instructions.
- Install the adaptive security appliance in compliance with local and national electrical codes as listed in the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* document.
- The adaptive security appliance models equipped with AC-input power supplies are shipped with a 3-wire electrical cord with a grounding-type plug that fits only a grounding-type power outlet. Do not circumvent this safety feature. Equipment grounding should comply with local and national electrical codes.
- The adaptive security appliance models equipped with DC-input power supplies must be terminated with the DC input wiring on a DC source capable of supplying at least 15 amps. A 15-amp circuit breaker is required at the 48 VDC facility power source. An easily accessible disconnect device should be incorporated into the facility wiring. Be sure to connect the grounding wire conduit to a solid earth ground. We recommend that you use a closed loop ring to terminate the ground conductor at the ground stud. The DC return connection to this system is to remain isolated from the system frame and chassis.

Other DC power guidelines are listed in the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* document.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. ESD damage occurs when electronic components are improperly handled and can result in complete or intermittent failures.

- Always follow ESD-prevention procedures when removing and replacing components. Ensure that the chassis is electrically connected to earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the grounding clip to an unpainted surface of the chassis frame to safely ground ESD voltages. To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.
- For safety, periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms (Mohms).

General Site Requirements

The topics in this section describe the requirements your site must meet for safe installation and operation of your system. Ensure that your site is properly prepared before beginning installation.

This section includes the following topics:

- [Site Environment, page 1-4](#)
- [Preventive Site Configuration, page 1-4](#)
- [Power Supply Considerations, page 1-5](#)
- [Configuring Equipment Racks, page 1-5](#)

Site Environment

Place the chassis on a desktop or mount it on a rack. The location of the chassis and the layout of the equipment rack or wiring room are extremely important for proper system operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause system malfunctions and shutdowns, and can make the chassis maintenance difficult.

When planning the site layout and equipment locations, keep in mind the precautions described in the next section “[Preventive Site Configuration, page 1-4](#),” to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are currently experiencing shutdowns or unusually high error rates with your existing equipment, these precautions may help you isolate the cause of failures and prevent future problems.

Preventive Site Configuration

The following precautions will help plan an acceptable operating environment for the chassis and avoid environmentally caused equipment failures:

- Electrical equipment generates heat. Ambient air temperature might not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Ensure that the room in which you operate your system has adequate air circulation.
- Always follow the ESD-prevention procedures described previously to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.

- Ensure that the chassis top panel is secure. The chassis is designed to allow cooling air to flow effectively within it. An open chassis allows air leaks, which may interrupt and redirect the flow of cooling air from the internal components.

Power Supply Considerations

The following chassis models can have either an AC or DC power supply: ASA 5505, ASA 5510, ASA 5520, ASA 5540 and ASA 5550.

Observe the following considerations:

- Check the power at the site before installing the chassis to ensure that the power is “clean” (free of spikes and noise). Install a power conditioner if necessary, to ensure proper voltages and power levels in the source voltage.
- Install proper grounding for the site to avoid damage from lightning and power surges.
- In a chassis equipped with an AC-input power supply, use the following guidelines:
 - The chassis does not have a user-selectable operating range. Refer to the label on the chassis for the correct AC-input power requirement.
 - Several styles of AC-input power supply cords are available; make sure you have the correct style for your site.
 - Install an uninterruptible power source for your site, if possible.
 - Install proper site grounding facilities to guard against damage from lightning or power surges.
- In a chassis equipped with a DC-input power supply, use the following guidelines:
 - Each DC-input power supply requires dedicated 15 amp service.
 - For DC power cables, it is recommend to use a minimum of 14 AWG wire cable.
 - The DC return connection to this system is to remain isolated from the system frame and chassis.

Configuring Equipment Racks

The following tips help you plan an acceptable equipment rack configuration:

- Enclosed racks must have adequate ventilation. Ensure that the rack is not overly congested, because each chassis generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake or exhaust ports. If the chassis is installed on slides, check the position of the chassis when it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, excessive heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Ensure that you provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack. Experiment with different arrangements to position the baffles effectively.



ASA 5505

Read through the entire guide before beginning any of the procedures in this chapter.


Warning

Only trained and qualified personnel should install, replace, or service this equipment. Statement 49


Caution

Read the safety warnings in the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* and follow proper safety procedures when performing these steps.

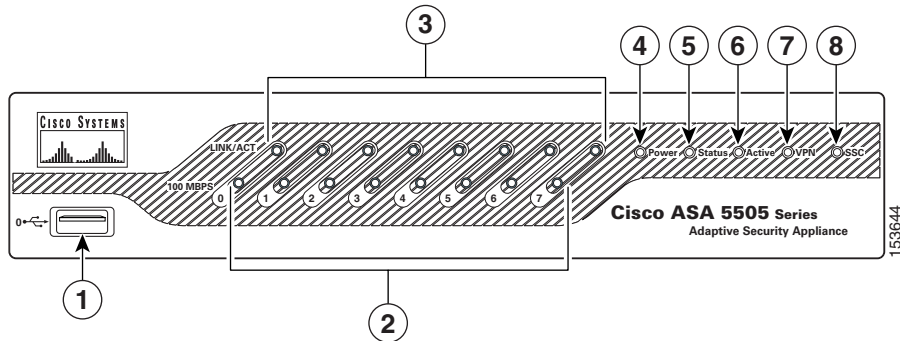
This chapter describes the product, memory requirements, and installation procedures, and includes the following topics:

- [Product Overview, page 2-2](#)
- [Memory Requirements, page 2-3](#)
- [Installing the Chassis, page 2-3](#)

Product Overview

This section describes the front and rear panels. [Figure 2-1](#) shows the front panel LEDs.

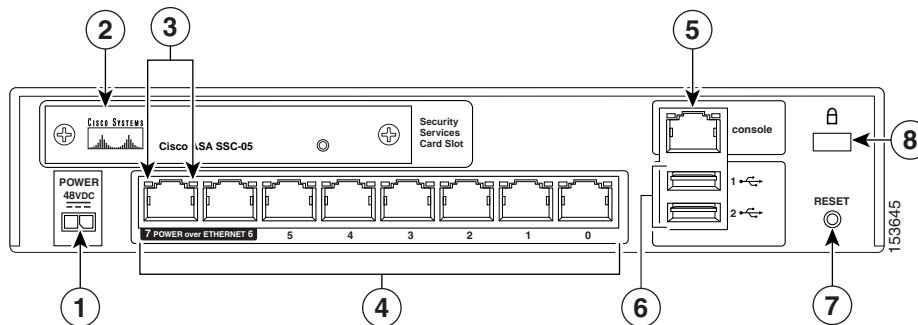
Figure 2-1 Front Panel LEDs and Ports



1	USB 2.0 interface	5	Status
2	100 Mbps	6	Active
3	LINK/ACT LEDs	7	VPN
4	Power	8	SSC

[Figure 2-2](#) shows the rear panel LEDs and Ports.

Figure 2-2 Rear Panel LEDs and Ports (AC Power Supply Model Shown)



1	Power 48VDC	5	Console port
2	SSC slot	6	USB 2.0 interface
3	Network interface LEDs	7	Reset button
4	Network interfaces ¹	8	Lock slot

1. Ports 6 and 7 are PoE ports, used for devices that can be powered by the network interface, IP phones for example. They can also be used as regular Ethernet switch ports, just like the ports numbered 0 through 5.

Memory Requirements

The memory requirement for the ASA 5505 is 256MB.

Installing the Chassis

This section contains the following topics:

- [Connecting the Interface Cables, page 2-3](#)
- [Powering on the ASA 5505, page 2-5](#)
- [Installing a Cable Lock, page 2-6](#)

Connecting the Interface Cables

This section describes how to connect the cables to the Ethernet and Console ports.



Only trained and qualified personnel should install, replace, or service this equipment. Statement 49



Read the safety warnings in the [Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series](#) and follow proper safety procedures when performing these steps.

To connect cables to the ports perform the following steps:

-
- Step 1** Place the chassis on a flat, stable surface.
- Step 2** Before connecting a computer or terminal to the ports, check to determine the baud rate of the serial port. The baud rate must match the default baud rate (9600 baud) of the Console port of the adaptive security appliance. Set up the terminal as follows: 9600 baud (default), 8 data bits, no parity, 1 stop bits, and Flow Control (FC) = Hardware.
- Step 3** Connect the cables to the ports.

a. Ethernet ports

Step 1 Connect Port 0, the outside Ethernet port, to the public network, that is, the Internet:

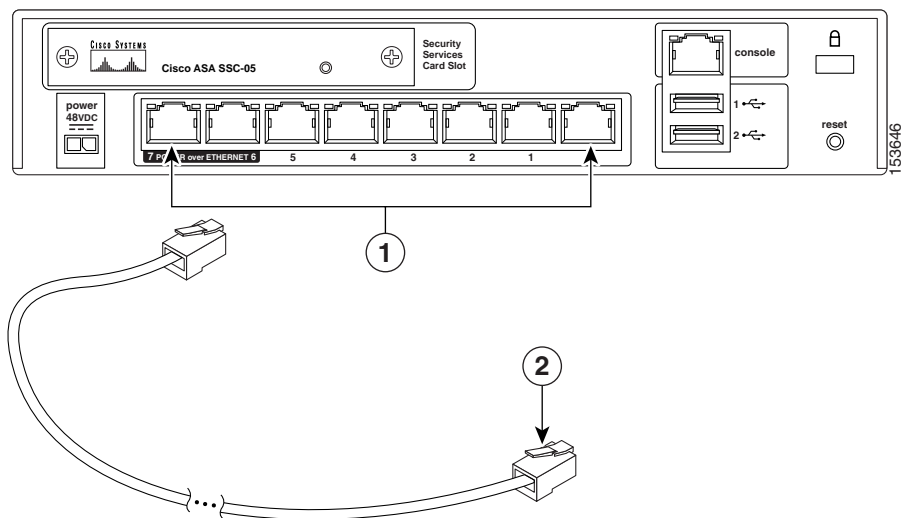


Note By default, switch port 0/0 is the outside port. If needed you can change the inside and outside ports assignments later.

Step 2 Connect your network devices with an Ethernet cable to one of the inside ports (numbered 1 through 7).
If you are connecting any PoE devices, connect them to one of the switch ports that support PoE (ports numbered 6 and 7).

Step 3 Check the LINK LED to verify that the network devices have basic connectivity to the ASA 5505 on one of the inside ports (numbered 0 through 7). When connectivity is established, the LINK LED on the front panel of the ASA 5505 lights up solid green.

Figure 2-3 Connecting Cables to Network Interfaces



1	RJ-45 Ethernet ports	2	RJ-45 connector
----------	----------------------	----------	-----------------

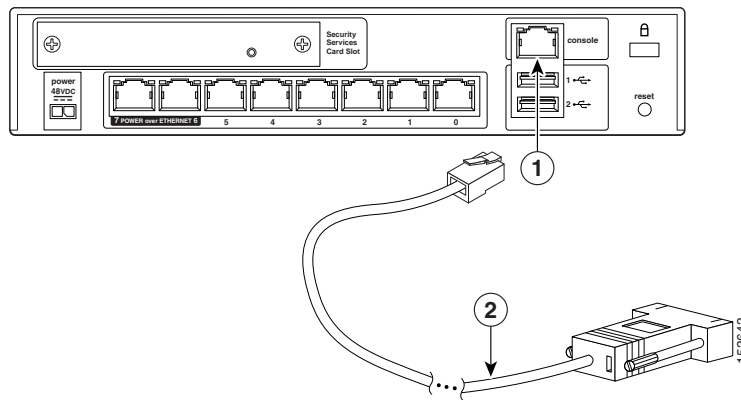
Step 4 Connect the power cord to the security appliance and plug the other end to the power source. For information on powering on the chassis, see the [“Powering on the ASA 5505”](#) section on page 2-5

b. Console port

You can access the command line for administration using the console port on the ASA 5505. To connect to the console port and run a serial terminal emulator on a PC or workstation, perform the following steps:

-
- Step 1** Plug one end of the PC terminal adapter into a standard 9-pin PC serial port on your PC.
- Step 2** Plug one end of the blue console cable into the PC terminal adapter.
- Step 3** Plug the other end of the blue console cable into the Console port.
- Step 4** Configure the PC terminal emulation software or terminal for 9600 baud, 8 data bits, no parity, and 1 stop bit.
-

Figure 2-4 Connecting to the Console Cable



1	RJ-45 Console port	2	RJ-45 to DB-9 console cable
----------	--------------------	----------	-----------------------------

Powering on the ASA 5505

To power on the ASA 5505, perform the following steps:

-
- Step 1** Connect the power supply with the power cable.
- Step 2** Connect the small, rectangular connector of the power supply cable to the power connector on the rear.
- Step 3** Connect the AC power connector of the power supply input cable to an electrical outlet.



Note The ASA 5505 does not have a power switch. Completing Step 3 powers on the device.

- Step 4** Check the power LED; if it is solid green, then the device is powered on.



Note The light will be solid green, only for 100Mbps devices.

Installing a Cable Lock

The ASA 5505 includes a slot that accepts standard desktop cable locks to provide physical security. The cable lock is not included.

To install a cable lock, perform the following steps:

-
- Step 1** Follow the directions from the manufacturer for attaching the other end of the cable for securing the ASA 5505.
 - Step 2** Attach the cable lock to the lock slot on the back panel of the ASA 5505.
-



ASA 5510, ASA 5520, ASA 5540, and ASA 5550

Read through the entire guide before beginning any of the procedures in this chapter.



Warning

Only trained and qualified personnel should install, replace, or service this equipment. Statement 49



Caution

Read the safety warnings in the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* and follow proper safety procedures when performing these steps.

This chapter describes the product, memory requirements, and rack-mount and installation procedures, and includes the following topics:

- [Product Overview, page 3-2](#)
- [Memory Requirements, page 3-5](#)
- [Installing the Chassis, page 3-5](#)



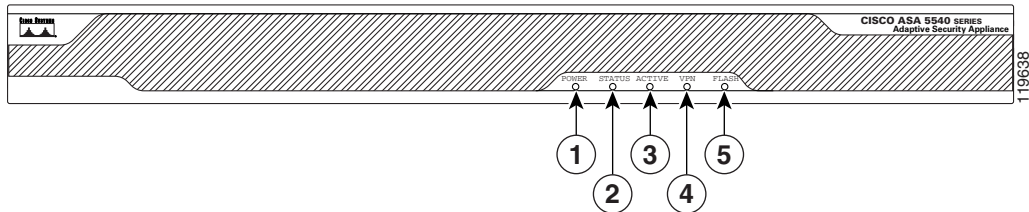
Note

The illustrations in this chapter show the Cisco ASA 5540 adaptive security appliance. The ASA 5510 and ASA 5520 adaptive security appliance look identical, containing the same back panel features and indicators. The ASA 5550 has a fixed configuration with an embedded 4GE slot as shown in [Figure 3-3](#).

Product Overview

This section describes the front and rear panels. [Figure 3-1](#) shows the front panel LEDs.

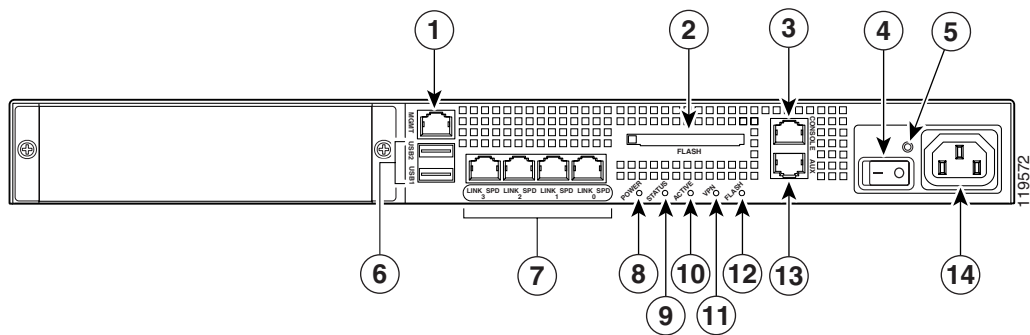
Figure 3-1 Front Panel LEDs



	LED	Color	State	Description
1	Power	Green	On	The system has power.
2	Status	Green	Flashing	The power-up diagnostics are running or the system is booting.
			Solid	The system has passed power-up diagnostics.
			Amber	Solid
3	Active	Green	Flashing	There is network activity.
4	VPN	Green	Solid	VPN tunnel is established.
5	Flash	Green	Solid	The CompactFlash is being accessed.

[Figure 3-2](#) shows the rear panel.

Figure 3-2 Rear Panel LEDs and Ports (AC Power Supply Model Shown)



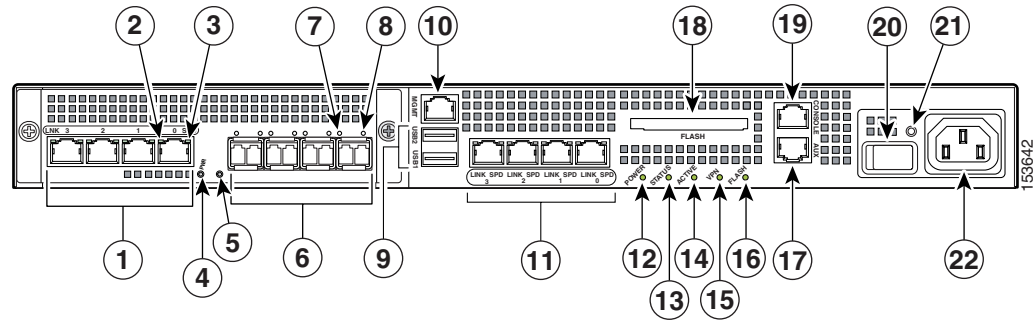
1	Management port ¹	6	USB 2.0 interfaces ²	11	VPN LED
2	External CompactFlash slot	7	Network interfaces ³	12	Flash LED
3	Serial Console port	8	Power indicator LED	13	AUX port
4	Power switch	9	Status indicator LED	14	Power connector
5	Power indicator LED	10	Active LED		

1. The management 0/0 interface is a Fast Ethernet interface designed for management traffic only.
2. Not supported at this time.
3. GigabitEthernet interfaces, from right to left, GigabitEthernet 0/0, GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3.

For more information about the Management port, see the **management only** command in the *Cisco Security Appliance Command Reference*.

The ASA 5550 has a fixed configuration with an embedded 4GE slot as shown in [Figure 3-3](#).

Figure 3-3 Rear Panel LEDs and Ports for the ASA 5550



1	RJ-45 ports ¹	9	USB 2.0 interfaces ²	17	AUX port
2	RJ-45 Link LED	10	Management port ³	18	External CompactFlash slot
3	RJ-45 Speed LED	11	Network interfaces ⁴	19	Serial Console port
4	Power LED	12	Power indicator LED	20	Power switch
5	Status LED	13	Status indicator LED	21	Power indicator LED
6	SFP ports ⁵	14	Active LED	22	Power connector
7	SFP Link LED	15	VPN LED		
8	SFP Speed LED	16	Flash LED		

1. GigabitEthernet ports, from right to left, GigabitEthernet 0/0, GigabitEthernet 1/0, GigabitEthernet 1/2, and GigabitEthernet 1/3

2. Not supported at this time.

3. The management 0/0 interface is a Fast Ethernet interface designed for management traffic only.

4. GigabitEthernet interfaces, from right to left, GigabitEthernet 0/0, GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3.

5. SFP ports, from right to left, GigabitEthernet 0/0, GigabitEthernet 1/0, GigabitEthernet 1/2, and GigabitEthernet 1/3

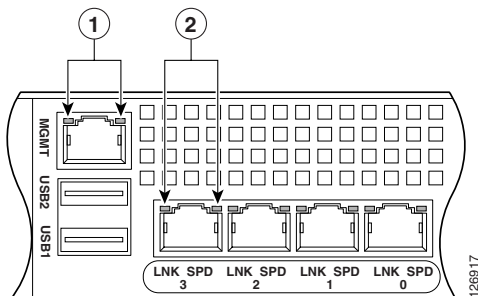
Table 3-1 describes the 4GE SSM LEDs.

Table 3-1 4GE SSM LEDs for the ASA 5550

	LED	Color	State	Description
2, 7	LINK	Green	Solid	There is an Ethernet link.
			Flashing	There is Ethernet activity.
3, 8	SPEED	Off	10 MB	There is no network activity.
		Green	100 MB	There is network activity at 100 Mbps.
		Amber	1000 MB (GigE)	There is network activity at 1000 Mbps.
4	POWER	Green	On	The system has power.
5	STATUS	Green	Flashing	The system is booting.
		Green	Solid	The system booted correctly.
		Amber	Solid	The system diagnostics failed.

Figure 3-4 shows the adaptive security appliance rear panel LEDs.

Figure 3-4 Rear Panel Link and Speed Indicator LEDs



1	MGMT indicator LEDs	2	Network interface LEDs
---	---------------------	---	------------------------

Table 3-2 lists the rear MGMT and Network interface LEDs.

Table 3-2 Link and Speed LEDs

Indicator	Color	Description
Left side	Solid green	Physical link
	Green flashing	Network activity
Right side	Not lit	10 Mbps
	Green	100 Mbps
	Amber	1000 Mbps



Note

The ASA 5510 adaptive security appliance supports only 10/100BaseTX. The ASA 5520 and the ASA 5540 support 1000BaseT.

Memory Requirements

Table 3-3 lists the CPU and the memory specifications for each model.

Table 3-3 CPU and Memory Specifications

Model	CPU	DRAM
ASA 5510	1.6 GHz Celeron	256 MB
ASA 5520	2.0 GHz Celeron	512 MB
ASA 5540	2.0 GHz Pentium 4	1024 MB
ASA 5550	2.0 GHz Pentium 4	1024 MB

Installing the Chassis

This section describes how to rack-mount and install the adaptive security appliance. You can mount the adaptive security appliance in a 19-inch rack (with a 17.5- or 17.75-inch opening).



Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety: This unit should be mounted at the bottom of the rack if it is the only unit in the rack. When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack. If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

The following information can help plan equipment rack installation:

- Allow clearance around the rack for maintenance.
- If the rack contains stabilizing devices, install the stabilizers prior to mounting or servicing the unit in the rack.
- When mounting a device in an enclosed rack, ensure adequate ventilation. Do not overcrowd an enclosed rack. Make sure that the rack is not congested, because each unit generates heat.
- When mounting a device in an open rack, make sure that the rack frame does not block the intake or exhaust ports.
- If the rack contains only one unit, mount the unit at the bottom of the rack.
- If the rack is partially filled, load the rack from the bottom to the top, with the heaviest component at the bottom of the rack.

This section contains the following topics:

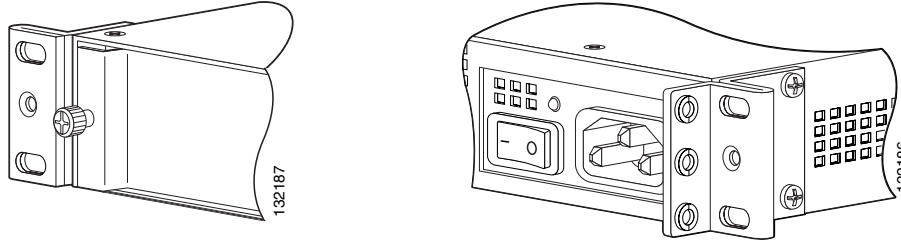
- [Rack-Mounting the Chassis, page 3-6](#)
- [Setting the Chassis on a Desktop, page 3-7](#)
- [Connecting the Interface Cables, page 3-8](#)

Rack-Mounting the Chassis

To rack-mount the chassis, perform the following steps:

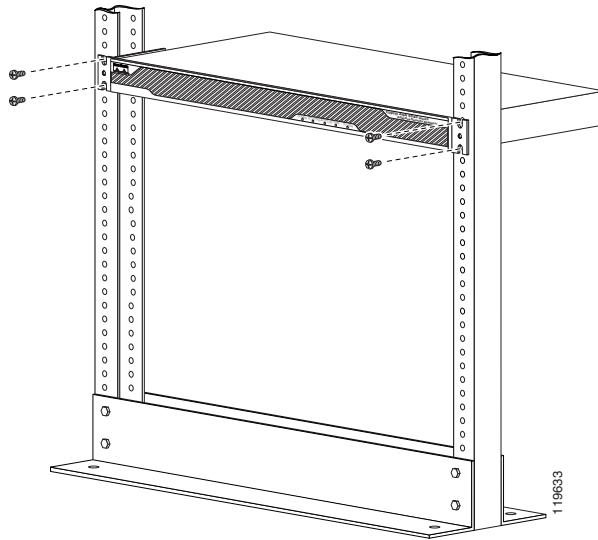
- Step 1** Attach the rack-mount brackets to the chassis using the supplied screws. Attach the brackets to the holes as shown in [Figure 3-5](#). After the brackets are secured to the chassis, you can rack-mount it.

Figure 3-5 *Installing the Right and Left Brackets*



- Step 2** Attach the chassis to the rack using the supplied screws, as shown in [Figure 3-6](#).

Figure 3-6 *Rack-Mounting the Chassis*



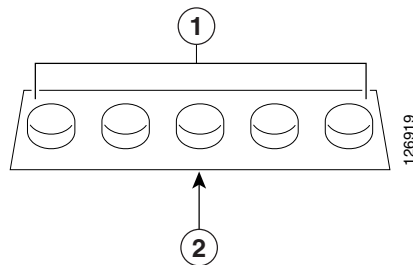
To remove the chassis from the rack, remove the screws that attach the chassis to the rack, and then remove the chassis.

Setting the Chassis on a Desktop

To set the chassis on a desktop, perform the following steps:

- Step 1** Locate the rubber feet on the black adhesive strip that shipped with the chassis.

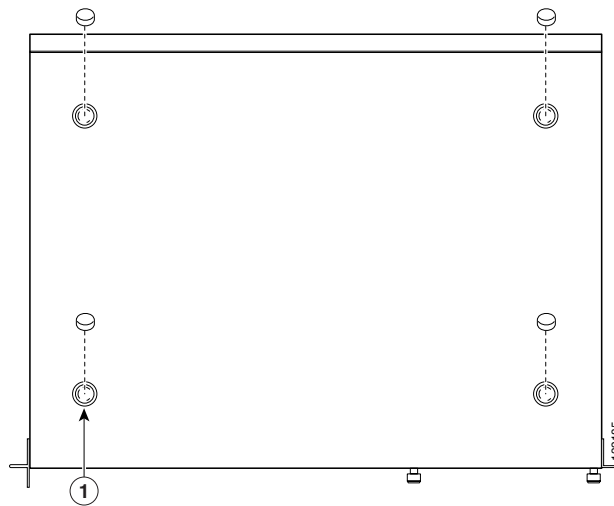
Figure 3-7 Identifying the Rubber Feet



1	Rubber feet	2	Black adhesive strip
----------	-------------	----------	----------------------

- Step 2** Place the chassis upside down, on a smooth, flat surface.
- Step 3** Peel off the rubber feet from the black adhesive strip and press them adhesive-side down onto the bottom four corners of the chassis, see [Figure 3-8](#).

Figure 3-8 Attaching the Rubber Feet



1	Rubber feet
----------	-------------

- Step 4** Place the chassis right-side up on a flat, smooth, secure surface.
- Step 5** Connect the interface cables. See the [“Connecting the Interface Cables”](#) section on page 3-8 for more information.

Connecting the Interface Cables

This section describes how to connect the cables to the Console, Auxiliary, Management, 4GE SSM, and SSM ports. In this document, SSM refers to an intelligent SSM, the AIP SSM or CSC SSM.

**Warning**

Only trained and qualified personnel should install, replace, or service this equipment. Statement 49

**Caution**

Read the safety warnings in the [Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series](#) and follow proper safety procedures when performing these steps.

To connect cables to the ports perform the following steps:

-
- Step 1** Place the chassis on a flat, stable surface, or in a rack (if you are rack-mounting it.)
 - Step 2** Before connecting a computer or terminal to the ports, check to determine the baud rate of the serial port. The baud rate must match the default baud rate (9600 baud) of the Console port of the adaptive security appliance. Set up the terminal as follows: 9600 baud (default), 8 data bits, no parity, 1 stop bits, and Flow Control (FC) = Hardware.
 - Step 3** Connect the cables to the ports.

a. Management port

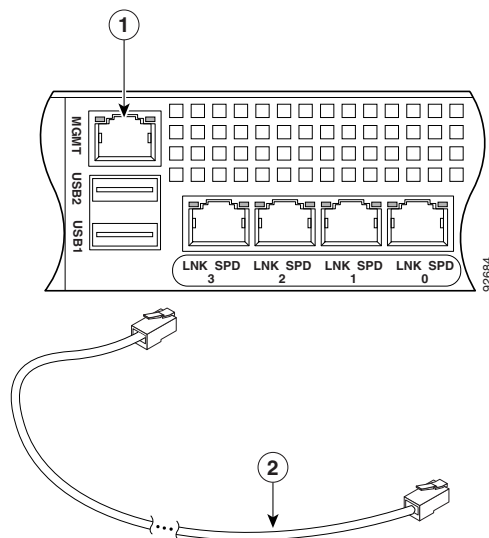
The adaptive security appliance has a dedicated management interface referred to as the Management0/0 port. The Management0/0 port is a Fast Ethernet interface with a dedicated port used only for traffic management.



Note You can configure any interface to be a management-only interface using the **management-only** command. You can also disable management-only mode on the management interface. For more information about this command, see the **management-only** command in the *Cisco Security Appliance Command Reference*.

- Connect one RJ-45 connector to the Management0/0 port, as shown in [Figure 3-9](#).
- Connect the other end of the Ethernet cable to the management port on your computer or network device.

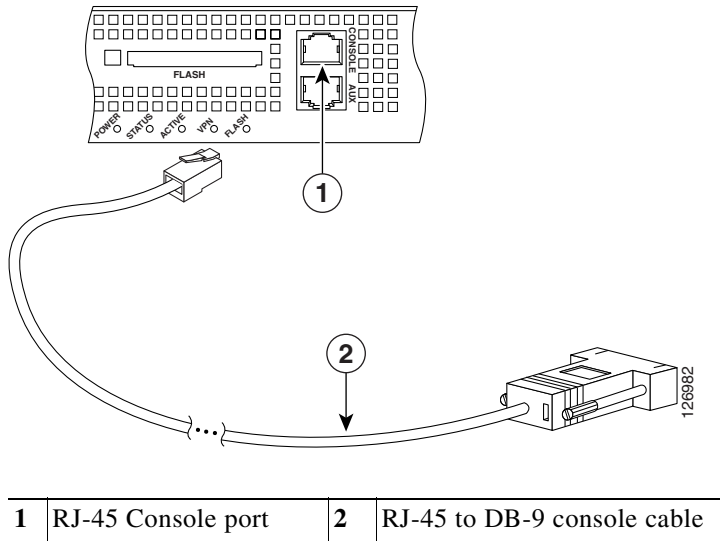
Figure 3-9 Connecting to the Management Port



1	Management port	2	RJ-45 to RJ-45 Ethernet cable
----------	-----------------	----------	-------------------------------

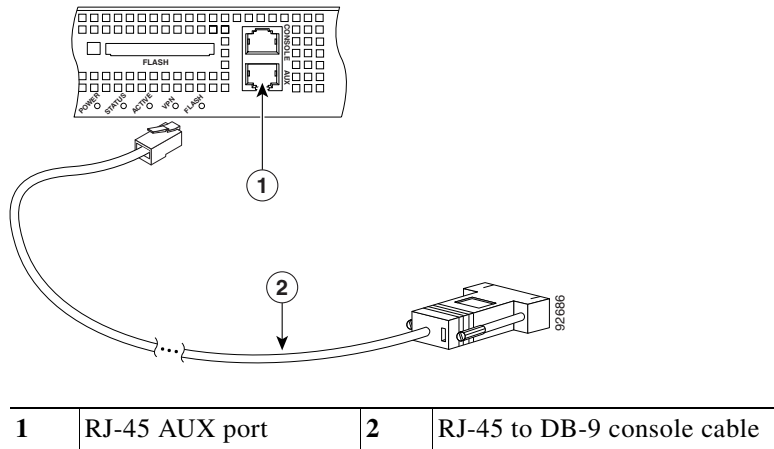
b. Console port

- Connect the serial console cable as shown in [Figure 3-10](#). The console cable has a DB-9 connector on one end for the serial port on your computer, and the other end is an RJ-45 connector.
- Connect the RJ-45 connector to the Console port on the adaptive security appliance.
- Connect the other end of the cable, the DB-9 connector, to the console port on your computer.

Figure 3-10 Connecting to the Console Cable

- c. Auxiliary port
- Connect the serial console cable as shown in [Figure 3-10](#). The console cable has a DB-9 connector on one end for the serial port on your computer, and the other end is an RJ-45 connector.
 - Connect the RJ-45 connector to the auxiliary port (labeled AUX) on the adaptive security appliance.
 - Connect the other end of the cable, the DB-9 connector, to the serial port on your computer.

Figure 3-11 Connecting to the AUX Port



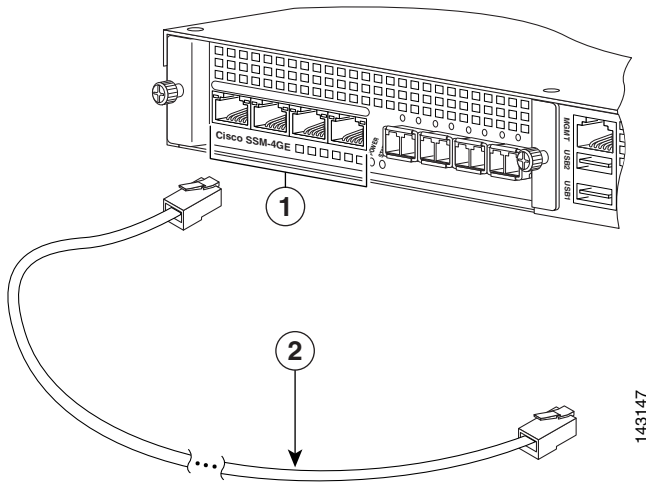
d. 4GE SSM

- Ethernet port
 - Connect one RJ-45 connector to the Ethernet port of the 4GE SSM.
 - Connect the other end of the Ethernet cable to your network device, such as a router, switch or hub.



Note The 4GE SSM is optional, this connection is necessary only if you have installed the 4GE SSM on the adaptive security appliance.

Figure 3-12 Connecting to the RJ-45 port



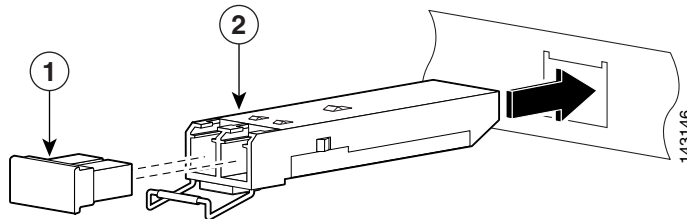
1	Ethernet ports	2	RJ-45 connector
---	----------------	---	-----------------



Note When using the 4GE SSM you can use the same numbered copper ports (RJ-45) and the SFP ports at the same time.

- SFP modules
 - Insert and slide the SFP module into the SFP port until you hear a click. The click indicates that the SFP module is locked into the port.
 - Remove the optical port plugs from the installed SFP as shown in [Figure 3-13](#).

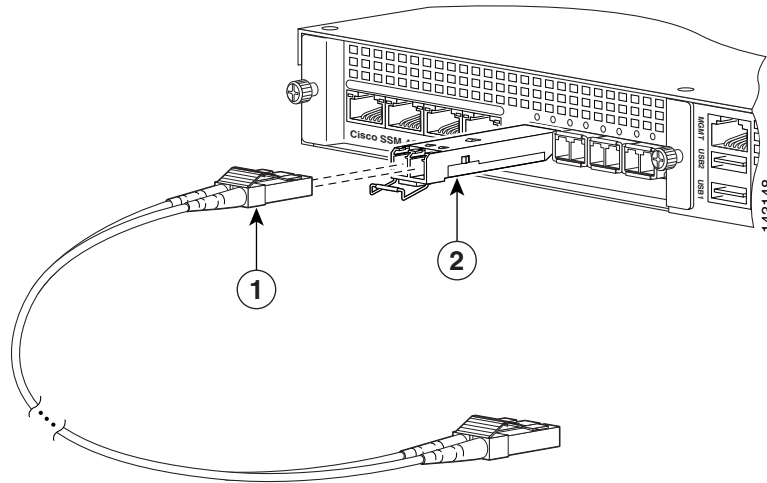
Figure 3-13 Removing the Optical Port Plug



1	Optical port plug	2	SFP module
----------	-------------------	----------	------------

- Connect the LC connector to the SFP module as shown in [Figure 3-14](#).

Figure 3-14 Connecting the LC Connector



1	LC connector	2	SFP module
----------	--------------	----------	------------

- Connect the other end to your network devices, such as routers, switches, or hubs.

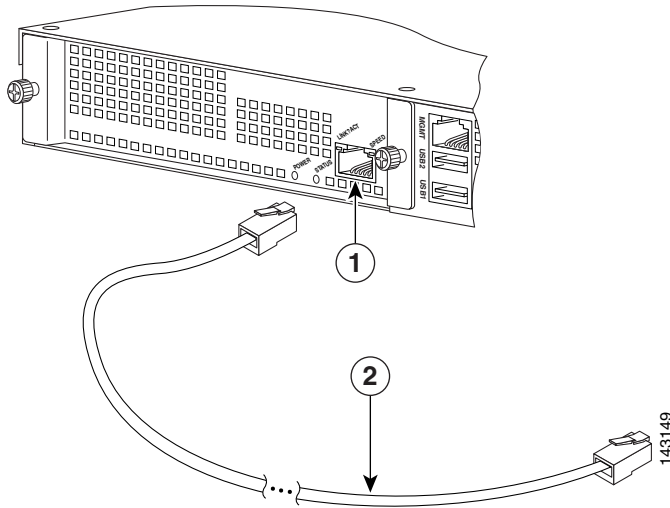
e. SSM

- Connect one RJ-45 connector to the management port on the SSM, as shown in [Figure 3-15](#).
- Connect the other end of the RJ-45 cable to your network devices.



Note SSMs are optional, this connection is necessary only if you have installed an SSM on the adaptive security appliance.

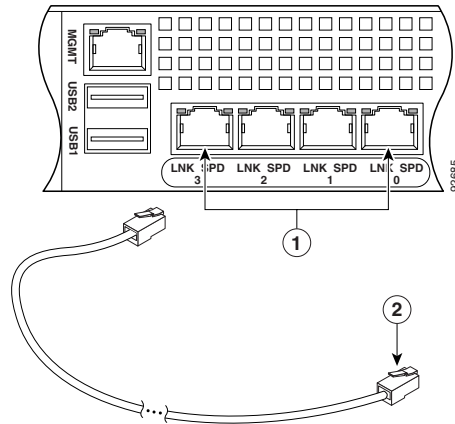
Figure 3-15 Connecting to the Management Port



1	SSM management port	2	RJ-45 to RJ-45 cable
----------	---------------------	----------	----------------------

- f. Ethernet ports
- Connect the RJ-45 connector to the Ethernet port.
 - Connect the other end of the Ethernet cable to your network device, such as a router, switch or hub.

Figure 3-16 Connecting Cables to Network Interfaces



1	RJ-45 Ethernet ports	2	RJ-45 connector
----------	----------------------	----------	-----------------

Step 4 Connect the power cord to the security appliance and plug the other end to the power source. For information on powering on a DC model, see the [“Installing the DC Model”](#) section on page B-8.

Step 5 Power on the chassis.



Installing and Replacing the SSM

This appendix describes how to install and replace the 4GE Security Services Module (SSM) and the SSM. In this document, SSM refers to the intelligent SSM, the Advanced Inspection and Prevention Security Services Module (AIP) SSM or the Content Security and Control Security Services Module (CSC) SSM. This appendix includes the following topics:

- [Installing and Replacing the 4GE SSM, page A-1](#)
- [Installing and Replacing the SSM, page A-8](#)



Note

Use either the SFP or the RJ-45 ports and not both ports at one time.

Both the SFP and the RJ-45 ports can be plugged in, but use the **media-type** command in interface configuration mode to set the media type to copper or fiber Gigabit Ethernet. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Installing and Replacing the 4GE SSM

The 4GE SSM has four 10/100/1000 Mbps, copper, RJ-45 ports and four optional 1000 Mbps, Small-Form-Factor Pluggable (SFP) fiber ports.

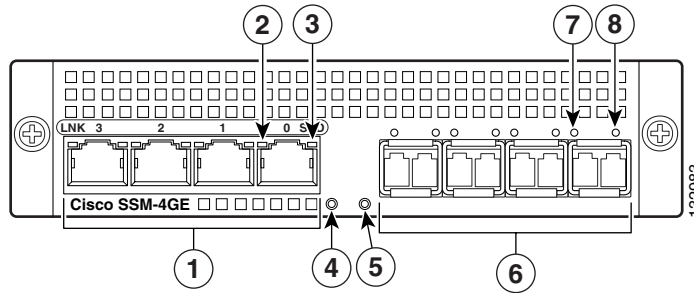
This section describes how to install and replace the 4GE SSM in the adaptive security appliance, and includes the following topics:

- [Overview, page A-2](#)
- [Installing the 4GE SSM, page A-3](#)
- [Replacing the 4GE SSM, page A-4](#)
- [Installing and Removing the SFP Modules, page A-4](#)

Overview

Figure A-1 lists the 4GE SSM ports and LEDs.

Figure A-1 4GE SSM Ports and LEDs



1	RJ-45 ports	5	Status LED
2	RJ-45 Link LED	6	SFP ports
3	RJ-45 Speed LED	7	SFP Link LED
4	Power LED	8	SFP Speed LED

Note

Figure A-1 shows SFP modules installed in the ports slots. You must order and install the SFP modules if you want to use this feature. For more information on SFP ports and modules, see the “Installing and Removing the SFP Modules” section on page A-4.

Table A-1 describes the 4GE SSM LEDs.

Table A-1 4GE SSM LEDs

	LED	Color	State	Description
2, 7	LINK	Green	Solid	There is an Ethernet link.
			Flashing	There is Ethernet activity.
3, 8	SPEED	Off	10 MB	There is no network activity.
		Green	100 MB	There is network activity at 100 Mbps.
		Amber	1000 MB (GigE)	There is network activity at 1000 Mbps.
4	POWER	Green	On	The system has power.
5	STATUS	Green	Flashing	The system is booting.
		Green	Solid	The system booted correctly.
		Amber	Solid	The system diagnostics failed.

Installing the 4GE SSM

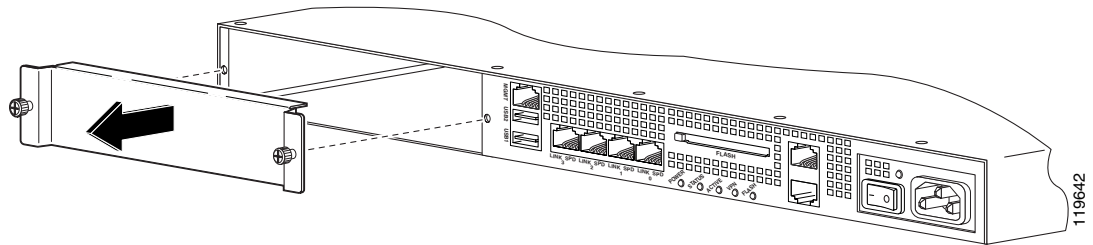


Note The following is only supported on the ASA 5510, ASA 5520, and ASA 5540.

To install a new 4GE SSM for the first time, perform the following steps:

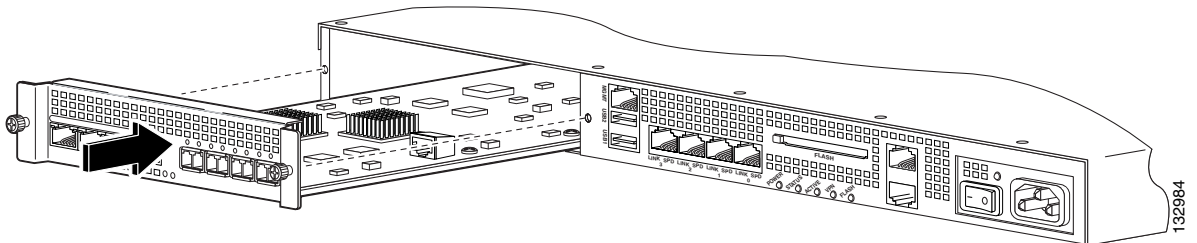
- Step 1** Power off the adaptive security appliance.
- Step 2** Locate the grounding strap from the accessory kit and fasten it to your wrist so that it contacts your bare skin. Attach the other end to the chassis.
- Step 3** Remove the two screws (as shown in [Figure A-2](#)) at the left rear end of the chassis, and remove the slot cover.

Figure A-2 Removing the Screws from the Slot Cover



- Step 4** Insert the 4GE SSM through the slot opening as shown in [Figure A-3](#).

Figure A-3 Inserting the 4GE SSM into the Slot



- Step 5** Attach the screws to secure the 4GE SSM to the chassis.
- Step 6** Power on the adaptive security appliance.
- Step 7** Check the LEDs. If the 4GE SSM is installed properly the STATUS LED flashes during boot up and is solid when operational.
- Step 8** Connect one end of the RJ-45 cable to the port and the other end of the cable to your network devices. For more information, see the [“Connecting the Interface Cables”](#) section.

Replacing the 4GE SSM

**Note**

The following is only supported on the ASA 5510, ASA 5520, and ASA 5540.

To replace an existing 4GE SSM, perform the following steps:

- Step 1** Enter the **hw-mod mod 1 shut** command in privileged EXEC mode. Verify that the module is down by making sure that the LEDs are all off.
- Step 2** Locate the grounding strap from the accessory kit and fasten it to your wrist, so that it contacts your bare skin. Attach the other end to the chassis.
- Step 3** Remove the two screws at the left rear end of the chassis.
- Step 4** Remove the 4GE SSM. Place it in a static bag and set it aside.
- Step 5** Replace the existing card by inserting the new 4GE SSM through the slot opening.
- Step 6** Attach the screws to secure the 4GE SSM to the chassis.
- Step 7** Enter the **hw-mod mod 1 reset** command in privileged EXEC mode to reset the 4GE SSM.
- Step 8** Check the LEDs. If the 4GE SSM is installed properly, the POWER LED is solid green and the STATUS LED is flashing during boot up.
- Step 9** Connect the RJ-45 cable to the port and the other end of the cable to your network devices. For more information, see the [“Connecting the Interface Cables”](#) section.

Installing and Removing the SFP Modules

**Note**

The following is supported on the ASA 5510, ASA 5520, ASA 5540, and ASA 5550.

The SFP is a hot-swappable input/output device that plugs into the SFP ports. The following SFP module types are supported:

- Long wavelength/long haul 1000BASE-LX/LH (GLC-LH-SM=)
- Short wavelength 1000BASE-SX (GLC-SX-MM=)

This section describes how to install and remove the SFP modules in the adaptive security appliance to provide optical Gigabit Ethernet connectivity. It contains the following topics:

- [SFP Module, page A-5](#)
- [Installing the SFP Module, page A-6](#)
- [Removing the SFP Module, page A-7](#)

SFP Module



Note

The following is supported on the ASA 5510, ASA 5520, ASA 5540, and ASA 5550.

The adaptive security appliance uses a field-replaceable SFP module to establish Gigabit connections.

[Table A-2](#) lists the SFP modules that are supported by the adaptive security appliance.

Table A-2 Supported SFP Modules

SFP Module	Type of Connection	Cisco Part Number
1000BASE-LX/LH	Fiber-optic	GLC-LH-SM=
1000BASE-SX	Fiber-optic	GLC-SX-MM=

The 1000BASE-LX/LH and 1000BASE-SX SFP modules are used to establish fiber-optic connections. Use fiber-optic cables with LC connectors to connect to an SFP module. The SFP modules support 850 to 1550 nm nominal wavelengths. The cables must not exceed the required cable length for reliable communications. [Table A-3](#) lists the cable length requirements.

Table A-3 Cabling Requirements for Fiber-Optic SFP Modules

SFP Module	62.5/125 micron Multimode 850 nm Fiber	50/125 micron Multimode 850 nm Fiber	62.5/125 micron Multimode 1310 nm Fiber	50/125 micron Multimode 1310 nm Fiber	9/125 micron Single-mode 1310 nm Fiber
LX/LH	—	—	550 m at 500 Mhz-km	550 m at 400 Mhz-km	10 km
SX	275 m at 200 Mhz-km	550 m at 500 Mhz-km	—	—	—

Use only Cisco certified SFP modules on the adaptive security appliance. Each SFP module has an internal serial EEPROM that is encoded with security information. This encoding provides a way for Cisco to identify and validate that the SFP module meets the requirements for the adaptive security appliance.



Note

Only SFP modules certified by Cisco are supported on the adaptive security appliance.



Caution

Protect your SFP modules by inserting clean dust plugs into the SFPs after the cables are extracted from them. Be sure to clean the optic surfaces of the fiber cables before you plug them back into the optical bores of another SFP module. Avoid getting dust and other contaminants into the optical bores of your SFP modules. The optics do not work correctly when obstructed with dust.



Warning

Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures. Statement 70

Installing the SFP Module



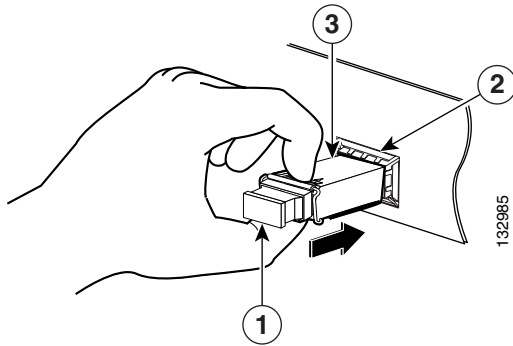
Note

The following is supported on the ASA 5510, ASA 5520, ASA 5540, and ASA 5550.

To install the SFP module in the 4GE SSM, perform the following steps:

- Step 1** Line up the SFP module with the port and slide the SFP module into the port slot until it locks into position as shown in [Figure A-4](#).

Figure A-4 Installing an SFP Module



1	Optical port plug	2	SFP port slot
3	SFP module		



Caution

Do not remove the optical port plugs from the SFP until you are ready to connect cabling.

- Step 2** Remove the Optical port plug; then connect the network cable to the SFP module.

- Step 3** Connect the other end of the cable to your network. For more information on connecting the cables, see [“Connecting the Interface Cables”](#) section on page 2-3.



Caution

The latching mechanism used on many SFPs locks them into place when cables are connected. Do not pull on the cabling in an attempt to remove the SFP.

Removing the SFP Module



Note

The following is supported on the ASA 5510, ASA 5520, ASA 5540, and ASA 5550.

The SFP modules have different types of latching devices used to detach the SFP module from a port. The following are the different types of modules:

- Mylar Tab Module
- Actuator/Button SFP Module
- Bale-Clasp SFP Module
- Plastic Collar Module

To remove the SFP module, perform the following steps:

Step 1

Disconnect all cables from the SFP.



Warning

Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures. Statement 70



Caution

The latching mechanism used on many SFPs locks the SFP into place when cables are connected. Do not pull on the cabling in an attempt to remove the SFP.

Step 2

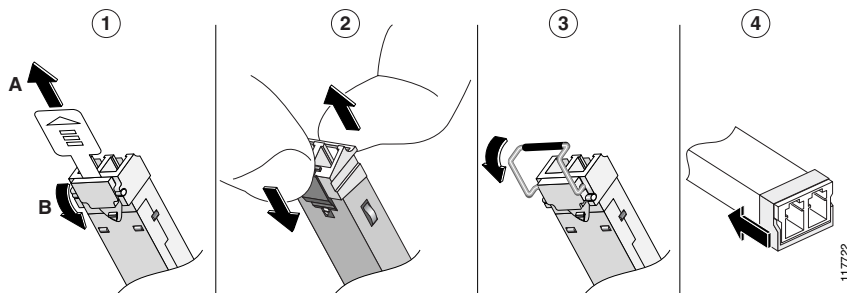
Disconnect the SFP latch as shown in [Figure A-5](#).



Note

SFP modules use various latch designs to secure the module in the SFP port. Latch designs are not linked to SFP model or technology type. For information on the SFP technology type and model, see the label on the side of the SFP.

Figure A-5 Disconnecting SFP Latch Mechanisms



1	Mylar tab	2	Actuator/Button
3	Bale-clasp	4	Plastic collar

Step 3

Grasp the SFP on both sides and remove it from the port.

Installing and Replacing the SSM

The adaptive security appliance supports the AIP SSM and the CSC SSM, also referred to as the intelligent SSM in this document.



Note

The following is only supported on the ASA 5510, ASA 5520, and ASA 5540.

The AIP SSM runs advanced IPS software that provides security inspection. There are two types of the AIP SSM: the AIP SSM 10 and the AIP SSM 20. Both types look identical, but the AIP SSM 20 has a faster processor and more memory than the AIP SSM 10. Only one module (the AIP SSM 10 or the AIP SSM 20) can populate the slot at a time.

[Table A-4](#) lists the memory specifications for the AIP SSM 10 and the AIP SSM 20.

Table A-4 SSM Memory Specifications

SSM	CPU	DRAM
AIP SSM 10	2.0 GHz Celeron	1.0 GB
AIP SSM 20	2.4 GHz Pentium 4	2.0 GB

For more information on the AIP SSM, see the [“Managing the AIP SSM”](#) section in the *Cisco Security Appliance Command Line Configuration Guide*.

The CSC SSM runs Content Security and Control software. The CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic. For more information on the CSC SSM, see the [“Managing the CSC SSM”](#) section in the *Cisco Security Appliance Command Line Configuration Guide*.

[Table A-5](#) shows the SSMs supported by each platform:

Table A-5 SSM Support

Platform	SSM Models
ASA 5510	AIP SSM 10 CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5520	AIP SSM 10 AIP SSM 20 CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5540	AIP SSM 10 AIP SSM 20 4GE SSM

This section describes how to install and replace the SSM in the adaptive security appliance. This section includes the following sections:

- [Installing an SSM, page A-9](#)
- [Replacing an SSM, page A-10](#)

Figure A-6 lists the SSM LEDs.

Figure A-6 SSM LEDs

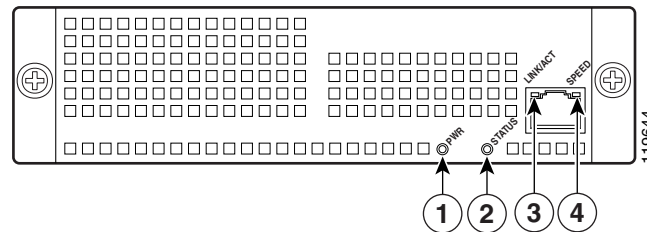


Table A-6 describes the SSM LEDs.

Table A-6 SSM LEDs

	LED	Color	State	Description
1	PWR	Green	On	The system has power.
2	STATUS	Green	Flashing	The system is booting.
			Solid	The system has passed power-up diagnostics.
3	LINK/ACT	Green	Solid	There is an Ethernet link.
			Flashing	There is Ethernet activity.
4	SPEED	Off	10 MB	There is no network activity.
		Green	100 MB	There is network activity at 100 Mbps.
		Amber	1000 MB (GigE)	There is network activity at 1000 Mbps.

Installing an SSM

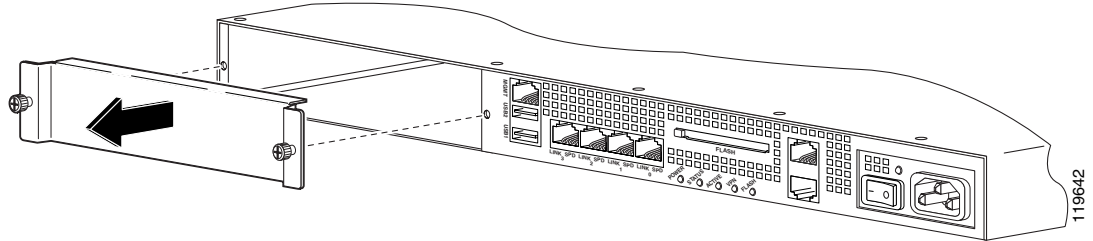


Note

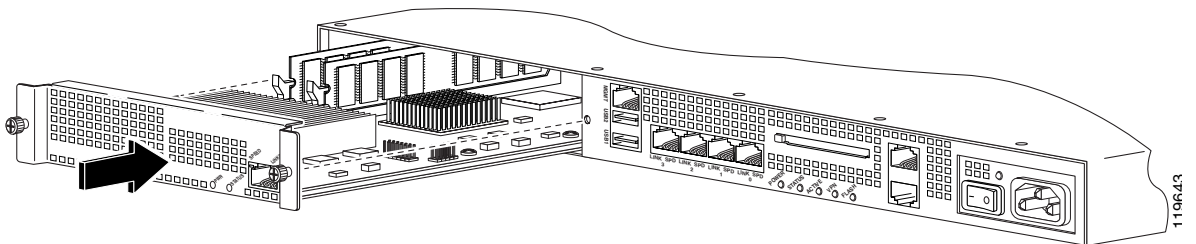
The following is only supported on the ASA 5510, ASA 5520, and ASA 5540.

To install a new SSM for the first time, perform the following steps:

- Step 1** Power off the adaptive security appliance.
- Step 2** Locate the grounding strap from the accessory kit and fasten it to your wrist so that it contacts your bare skin. Attach the other end to the chassis.
- Step 3** Remove the two screws (as shown in [Figure A-7](#)) at the left rear end of the chassis, and remove the slot cover.

Figure A-7 Removing the Screws from the Slot Cover

Step 4 Insert the SSM into the slot opening as shown in [Figure A-8](#).

Figure A-8 Inserting the SSM into the Slot

Step 5 Attach the screws to secure the SSM to the chassis.

Step 6 Power on the adaptive security appliance.

Step 7 Check the LEDs. If the SSM is installed properly the POWER LED is solid green and the STATUS LED flashes green.

Step 8 Connect one end of the RJ-45 cable to the port and the other end of the cable to your network devices. For more information, see [Figure 3-15](#).

Replacing an SSM



Note

The following is only supported on the ASA 5510, ASA 5520, and ASA 5540.

To replace an existing SSM, perform the following steps:

- Step 1** Enter the `hw-mod mod 1 shut` command in privileged EXEC mode. Verify if the module is down by checking the LEDs.
- Step 2** Locate the grounding strap from the accessory kit and fasten it to your wrist so that it contacts your bare skin. Attach the other end to the chassis.
- Step 3** Remove the two screws (as shown in [Figure A-7](#)) at the left rear end of the chassis, and remove the slot cover.
- Step 4** Remove the SSM. Set it aside.
- Step 5** Replace the existing card by inserting the new SSM through the slot opening.

- Step 6** Attach the screws to secure the SSM to the chassis.
- Step 7** Enter the **hw-mod mod 1 reset** command in privileged EXEC mode to reset the SSM.
- Step 8** Check the LEDs. If the SSM is installed properly, the POWER LED is solid green and the STATUS LED flashes green.
- Step 9** Connect one end of the RJ-45 cable to the port and the other end of the cable to your network devices. For more information, see [Figure 3-15](#).
-



Maintenance and Upgrade Procedures

This appendix describes how to install and replace the chassis cover, the power supply, and the CompactFlash. This appendix includes the following topics:

- [Removing and Replacing the Chassis Cover, page B-1](#)
- [Working in an ESD Environment, page B-4](#)
- [Removing and Replacing the Power Supply, page B-4](#)
- [Installing the DC Model, page B-8](#)
- [Removing and Replacing the CompactFlash, page B-10](#)

Removing and Replacing the Chassis Cover

This section describes how to remove and replace the chassis cover from the adaptive security appliance. This section includes the following topics:

- [Removing the Chassis Cover, page B-1](#)
- [Replacing the Chassis Cover, page B-3](#)

Removing the Chassis Cover

To remove the chassis cover, perform the following steps:



Note

Removing the chassis cover does not affect Cisco warranty. Upgrading the adaptive security appliance does not require any special tools and does not create any radio frequency leaks.

Step 1

Read the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* document.

Step 2

Power off the adaptive security appliance. Once the upgrade is complete, you can safely power on the chassis.

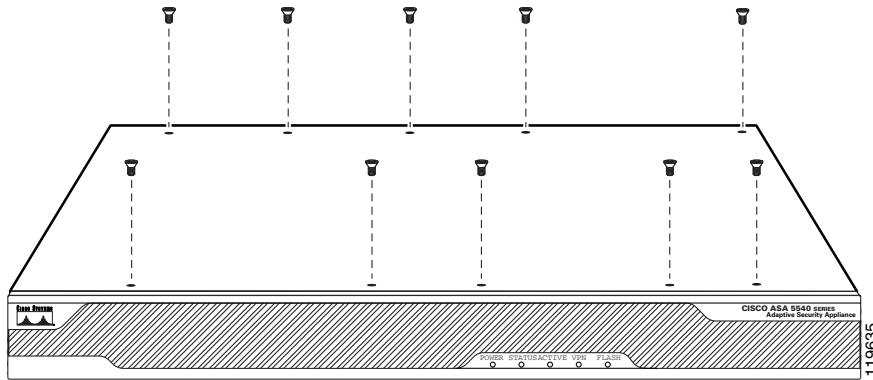


Warning

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

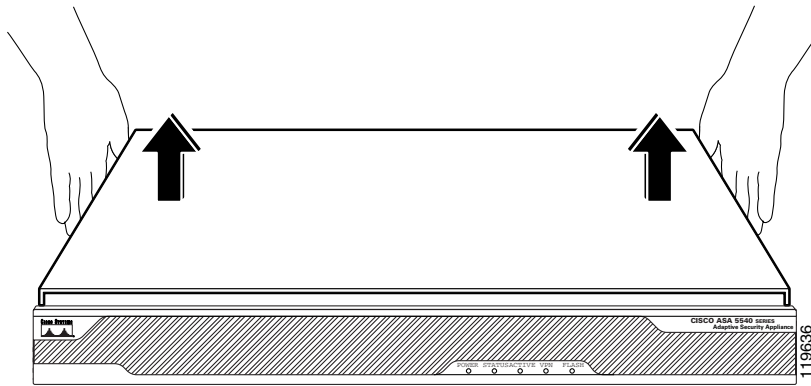
Step 3 Remove the screws from the top of the chassis (Figure B-1).

Figure B-1 Removing the Top Panel Screws



Step 4 Pull the top panel up as shown in Figure B-2. Put the panel in a safe place.

Figure B-2 Removing the Chassis Cover



Replacing the Chassis Cover



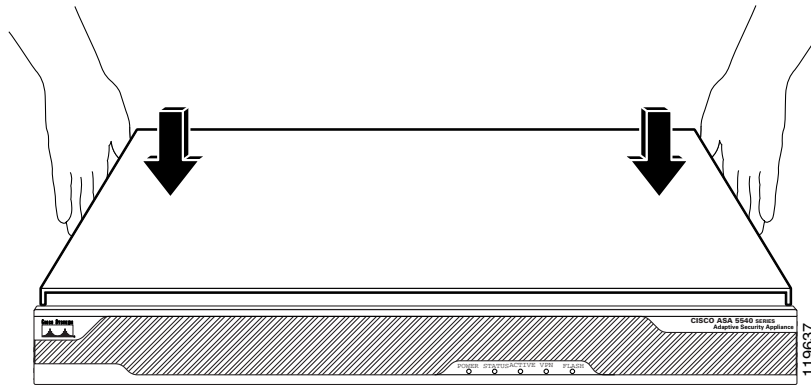
Caution

Do not operate the adaptive security appliance without the chassis cover installed. The chassis cover protects the internal components, prevents electrical shorts, and provides proper air-flow for cooling the electronic components.

To replace the chassis cover, perform the following steps:

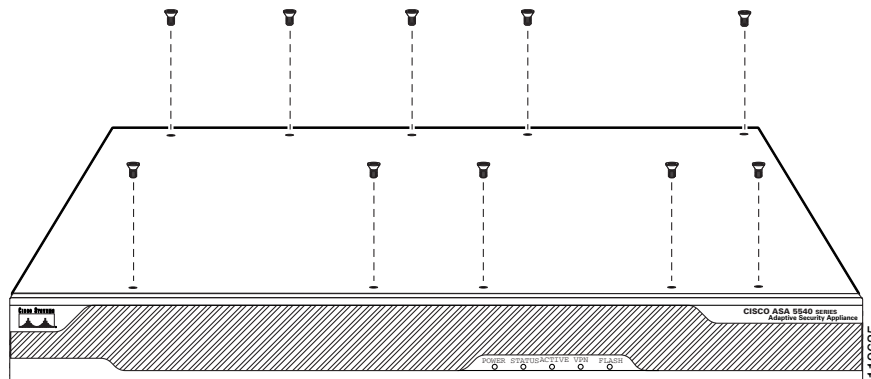
- Step 1** Place the chassis on a secure surface with the front panel facing you.
- Step 2** Hold the top panel so the tabs at the rear of the top panel are aligned with the chassis bottom.
- Step 3** Lower the front of the top panel onto the chassis as shown in [Figure B-3](#).

Figure B-3 Replacing the Chassis Cover



- Step 4** Fasten the top panel with the screws you set aside earlier as shown in [Figure B-4](#).

Figure B-4 Replacing the Screws



- Step 5** Reinstall the chassis on a rack.
- Step 6** Reinstall the network interface cables.

Working in an ESD Environment

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. ESD damage occurs when electronic components are improperly handled and can result in complete or intermittent failures. Always follow ESD-prevention procedures when you remove and replace components. Ensure that the chassis is electrically connected to earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the grounding clip to an unpainted surface of the chassis frame to safely ground unwanted ESD voltages. To guard against ESD damage and shocks, the wrist strap and cord must operate properly. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

Removing and Replacing the Power Supply

This section describes how to remove and replace the power supply, and includes the following topics:

- [Removing the AC Power Supply, page B-4](#)
- [Replacing the AC Power Supply, page B-7](#)

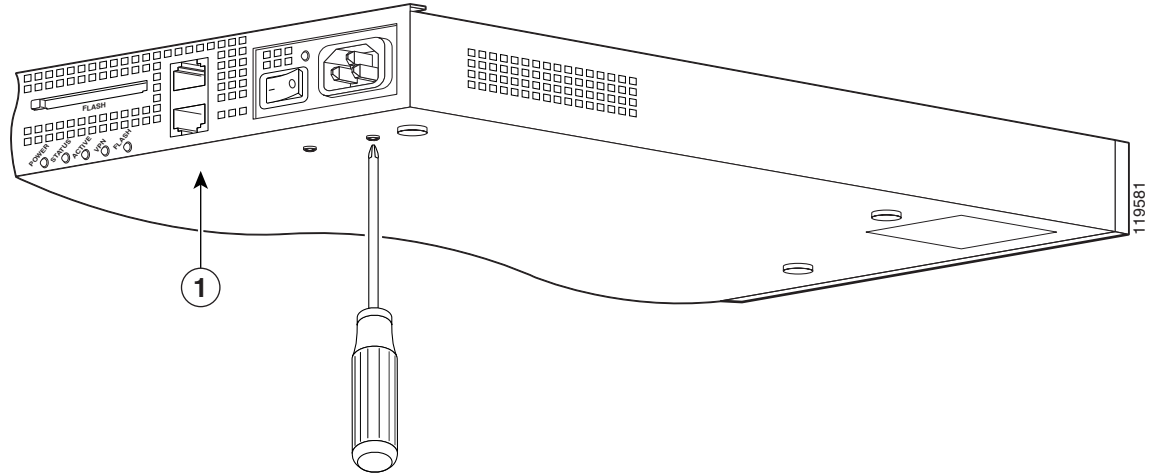
Removing the AC Power Supply

To remove the AC power supply, perform the following steps:

-
- Step 1** Power off the adaptive security appliance.
 - Step 2** Remove the power cord and all other cables from the chassis.
 - Step 3** Remove the chassis from the rack if it is rack-mounted. See the [“Rack-Mounting the Chassis” section on page 3-6](#) for more information.
 - Step 4** Remove the chassis cover. See the [“Removing and Replacing the Chassis Cover” section on page B-1](#) for more information.
 - Step 5** Place the chassis in an ESD-controlled environment. See the [“Working in an ESD Environment” section on page B-4](#) for more information.

- Step 6** Lift the rear of the chassis from the surface and unscrew both the screws that secures the power supply to the chassis, as shown in [Figure B-5](#).

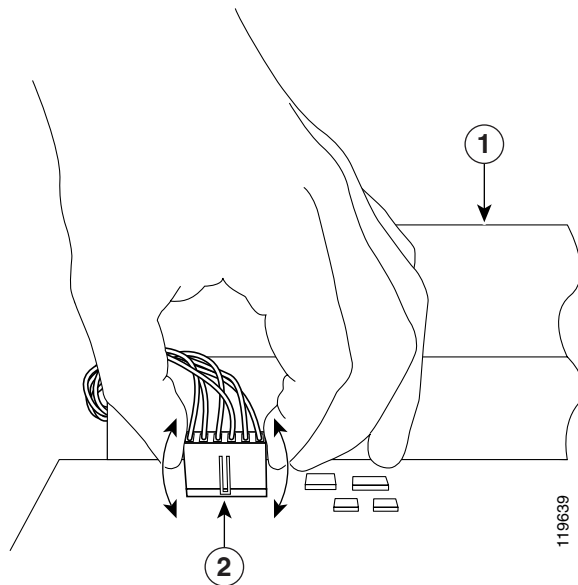
Figure B-5 Removing the Power Supply Screws



1	Chassis bottom
----------	----------------

- Step 7** Locate the power connector on the system board.
- Step 8** Unlatch the plug, then grasp the sides of the power connector and pull upward while rocking the connector from side to side. Disconnect the power connector from the system board as shown in [Figure B-6](#).

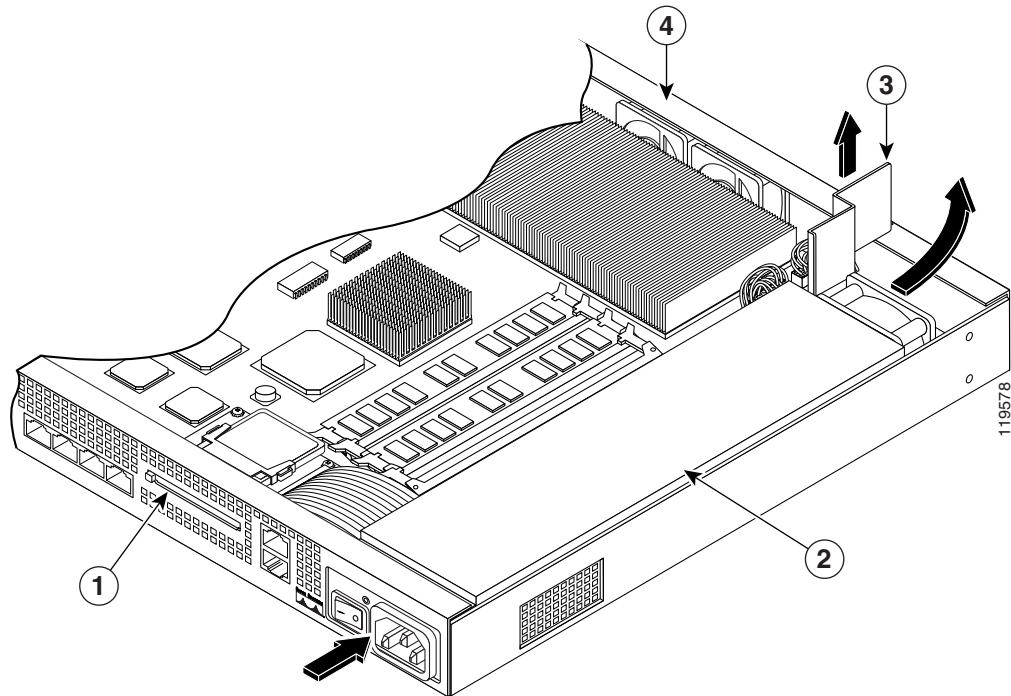
Figure B-6 Disconnecting the Power Connector



1	AC power supply	2	Power connector
----------	-----------------	----------	-----------------

Step 9 Remove the power supply brace by pulling it up and then out as shown in [Figure B-7](#).

Figure B-7 Removing the Power Supply



1	Back panel	3	Power supply brace
2	Power supply	4	Front panel

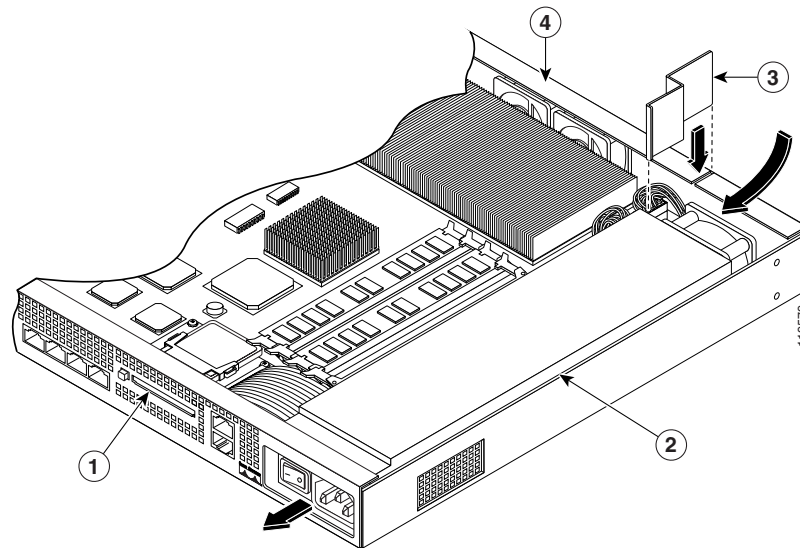
Step 10 From the back of the chassis, push the power supply forward, and then lift it up and out.

Replacing the AC Power Supply

To replace the AC power supply, perform the following steps:

- Step 1** Insert the new power supply into place and slide it towards the back of the adaptive security appliance.
- Step 2** Lift the rear of the adaptive security appliance from the surface and reinstall both screws.
- Step 3** Insert the power supply brace and press down until it fits into place, as shown in [Figure B-8](#).

Figure B-8 Replacing the Power Supply Brace and the AC Power Supply



1	Back panel	3	Power supply brace
2	Power supply	4	Front panel

- Step 4** Connect the power connector to the system board.
- Step 5** Replace the adaptive security appliance cover. See [“Replacing the Chassis Cover”](#) for more information.
- Step 6** Reinstall the network interface cables.

Installing the DC Model



Warning

Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position. Statement 7



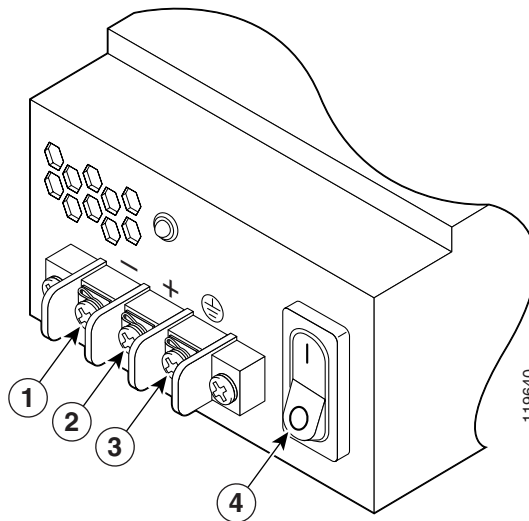
Note

The DC return connection should remain isolated from the system frame and chassis (DC-I). This equipment is suitable for connection to intra-building wiring only.

To install the DC power model, perform the following steps:

- Step 1** Read the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* document.
- Step 2** Terminate the DC input wiring on a DC source capable of supplying at least 15 amps. A 15-amp circuit breaker is required at the 48 VDC facility power source. An easily accessible disconnect device should be incorporated into the facility wiring.
- Step 3** Locate the DC-input terminal box, see [Figure B-9](#).

Figure B-9 DC-Input Terminal Box



1	Negative	3	Ground
2	Positive	4	On/Off Switch

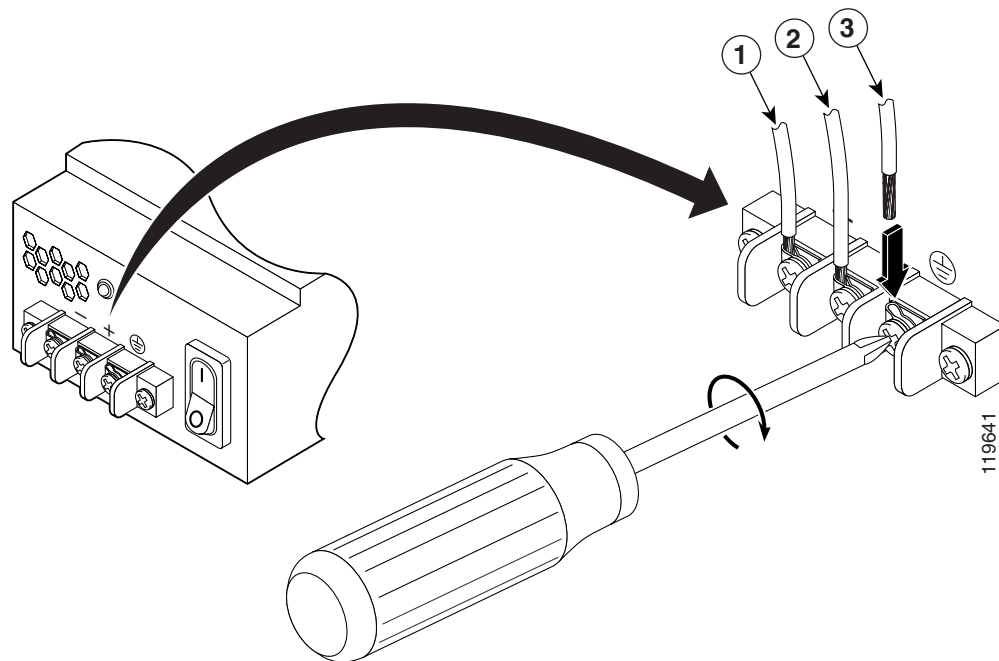
- Step 4** Power off the adaptive security appliance. Ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.
- Step 5** Remove the DC power supply plastic shield.

- Step 6** The adaptive security appliance is equipped with two grounding holes at the side of the chassis, which you can use to connect a two-hole grounding lug to the adaptive security appliance. Use 8-32 screws to connect a copper standard barrel grounding lug to the holes. The adaptive security appliance requires a lug where the distance between the center of each hole is 0.56 inches. A lug is not supplied with the adaptive security appliance.
- Step 7** Strip the ends of the wires for insertion into the power connect lugs on the adaptive security appliance.
- Step 8** Insert the ground wire into the connector for the earth ground and tighten the screw on the connector. See [Figure B-10](#), and using the same method as for the ground wire, connect the negative wire and then the positive wire.



Note The DC return connection to this system is to remain isolated from the system frame and chassis.

Figure B-10 DC-Input Power Supply Connections



1	Negative	3	Ground
2	Positive		

- Step 9** After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position.
- Step 10** Install any remaining interface boards as described in [“Installing the DC Model”](#) section on page B-8.

- Step 11** Replace the DC power supply plastic shield.
- Step 12** Power on the adaptive security appliance from the switch at the rear of the chassis.

**Note**

If you need to power cycle the DC adaptive security appliance, wait at least 5 seconds between powering off the adaptive security appliance and powering it back on.

Removing and Replacing the CompactFlash

The adaptive security appliance has two types of CompactFlash: the system CompactFlash (internal) and the user CompactFlash (external). This section includes the following topics:

- [Removing the System CompactFlash, page B-10](#)
- [Replacing the System CompactFlash, page B-12](#)
- [Removing the User CompactFlash, page B-13](#)
- [Replacing the User CompactFlash, page B-14](#)

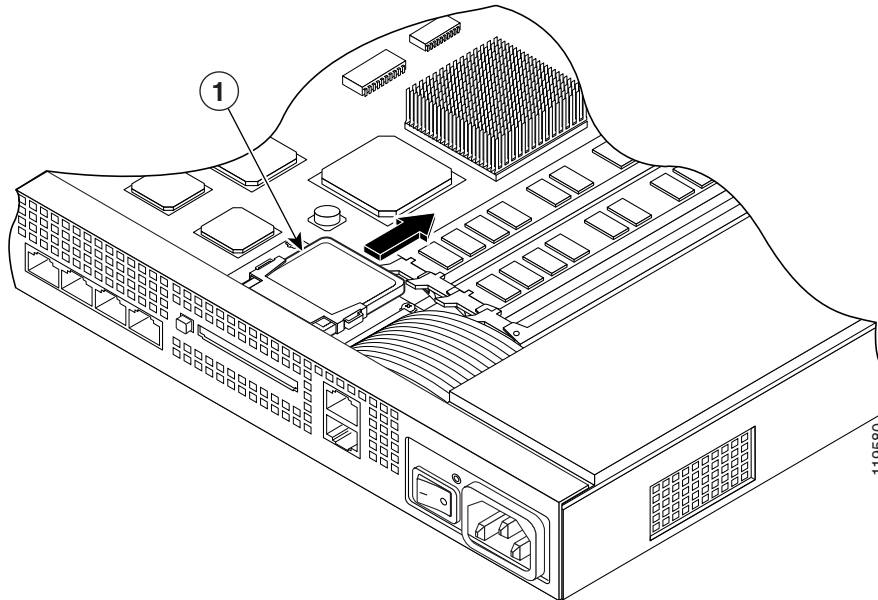
Removing the System CompactFlash

To remove the system CompactFlash, perform the following steps:

-
- Step 1** Power off the adaptive security appliance.
- Step 2** Remove the power cord and other cables from the adaptive security appliance.
- Step 3** Remove the adaptive security appliance from the rack if it is rack-mounted.
- Step 4** Place the adaptive security appliance in an ESD-controlled environment. See the “[Working in an ESD Environment](#)” section on [page B-4](#) for more information.
- Step 5** Remove the adaptive security appliance cover. See the “[Removing the Chassis Cover](#)” section on [page B-1](#) for the procedure.

- Step 6** Carefully slide the CompactFlash out of its connector as shown in [Figure B-11](#). The CompactFlash has a lip on its lower edge, which you can use to grip the CompactFlash. Otherwise, use sliding pressure with your thumb or finger to slide the CompactFlash out of its connector.

Figure B-11 Removing the System CompactFlash



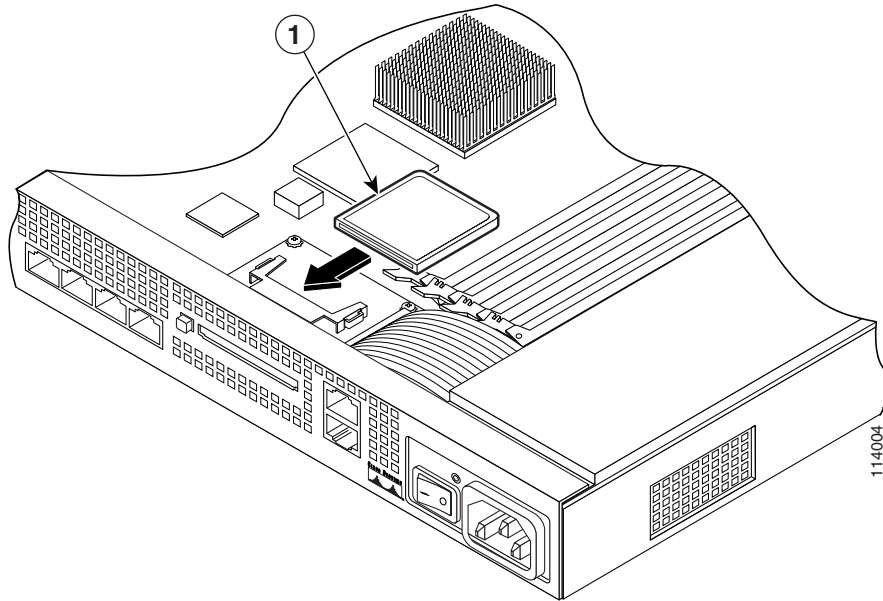
1	System CompactFlash
----------	---------------------

Replacing the System CompactFlash

To replace the system CompactFlash, perform the following steps:

-
- Step 1** Align the new system CompactFlash with the connector on the riser card.
 - Step 2** Push the system CompactFlash inward until it is fully seated in the connector, see [Figure B-12](#).

Figure B-12 Replacing the System CompactFlash



1	System CompactFlash
----------	---------------------

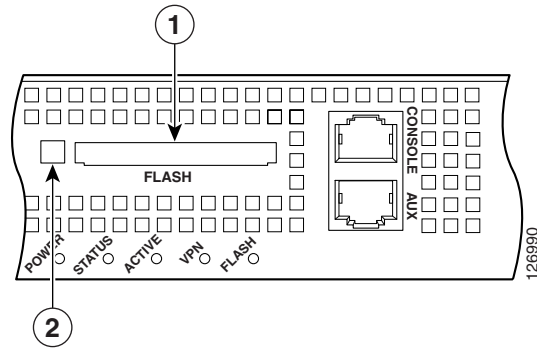
- Step 3** Replace the adaptive security appliance cover. See the “[Replacing the Chassis Cover](#)” section on [page B-3](#) for the procedure.
 - Step 4** Reinstall the network interface cables.
-

Removing the User CompactFlash

To remove the user CompactFlash, perform the following steps:

-
- Step 1** Locate the user CompactFlash in its slot in the rear panel of the chassis.
- Step 2** Press the release button to eject the card. See [Figure B-13](#).

Figure B-13 User CompactFlash Slot Release Button



1	User CompactFlash slot	2	Release button
----------	------------------------	----------	----------------

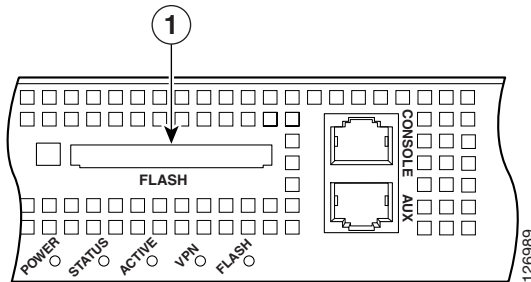
- Step 3** Carefully pull the card out of the slot.
- Step 4** Place the removed user CompactFlash on an antistatic surface or in a static shielding bag.
-

Replacing the User CompactFlash

To replace the user CompactFlash, perform the following steps:

- Step 1** Locate the user CompactFlash slot in the rear panel of the chassis. See [Figure B-14](#).

Figure B-14 User CompactFlash Slot



- | | |
|----------|------------------------|
| 1 | User CompactFlash slot |
|----------|------------------------|

- Step 2** With the label facing up, insert the connector end of the user CompactFlash into the slot until the card is seated in the connector and the release button is pushed out.



Note The user CompactFlash is keyed so that it cannot be inserted wrong.



Cable Pinouts

This appendix describes pinout information for 10/100/1000BaseT ports, console and the RJ-45 to DB-9 ports, and the Management 10/100/1000 Ethernet port, and includes the following sections:

- [10/100/1000BaseT Connectors, page C-1](#)
- [Console Port \(RJ-45\), page C-2](#)
- [RJ-45 to DB-9, page C-3](#)
- [MGMT 10/100/1000 Ethernet Port, page C-3](#)
- [Gigabit and Fibre Channel Ports, page C-4](#)

10/100/1000BaseT Connectors

The adaptive security appliance supports 10/100/1000BaseT ports. You must use at least a Category 5 cable for 100/1000baseT operations, but a Category 3 cable can be used for 10BaseT operations.

The 10/100/1000BaseT ports use standard RJ-45 connectors and supports MDI and MDI-X connectors. Ethernet ports normally use MDI connectors and Ethernet ports on a hub normally use an MDI-X connector.

Use an Ethernet straight-through cable to connect an MDI to an MDI-X port. Use a cross-over cable to connect an MDI to an MDI port, or an MDI-X to an MDI-X port.

[Figure C-1](#) shows the 10BaseT and the 100BaseTX connector (RJ-45).

Figure C-1 10/100 Port Pinouts

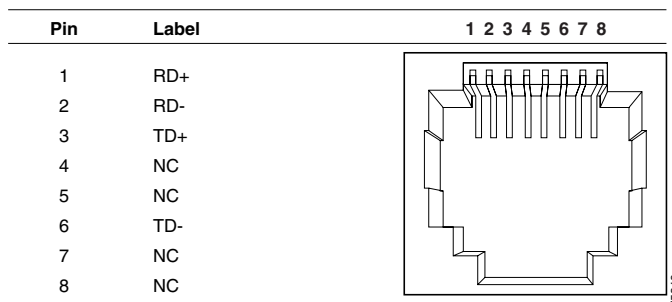
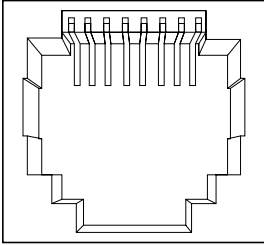


Figure C-2 10/100/1000 Port Pinouts

Pin	Label	1 2 3 4 5 6 7 8
1	TP0+	
2	TP0-	
3	TP1+	
4	TP2+	
5	TP2-	
6	TP1-	
7	TP3+	
8	TP3-	

Console Port (RJ-45)

Cisco products use the following three types of RJ-45 cables:

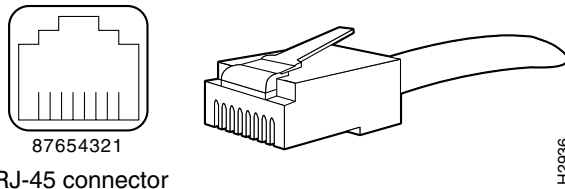
- Straight-through
- Crossover



Note

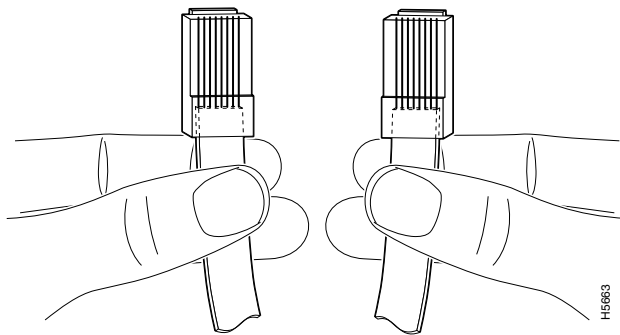
Cisco does not provide these cables; they are widely available from other sources.

Figure C-3 shows the RJ 45 cable.

Figure C-3 RJ-45 Cable

RJ-45 connector

To identify the RJ-45 cable type, hold the two ends of the cable next to each other so that you can see the colored wires inside the ends, as shown in Figure C-4.

Figure C-4 RJ-45 Cable Identification

Examine the sequence of colored wires to determine the type of RJ-45 cable, as follows:

- Straight-through—The colored wires are in the same sequence at both ends of the cable.
- Crossover—The first (far left) colored wire at one end of the cable is the third colored wire at the other end of the cable.

Table C-1 RJ-45 Rolled (Console) Cable Pinouts

Signal	Pin	Pin	Pin
-	1	8	-
-	2	7	-
-	3	6	-
-	4	5	-
-	5	4	-
-	6	3	-
-	7	2	-
-	8	1	-

RJ-45 to DB-9

Table C-2 lists the cable pinouts for RJ-45 to DB-9 or DB-25.

Table C-2 Cable Pinouts for RJ-45 to DB-9 or DB-25

Signal	RJ-45 Pin	DB-9 Pin
RTS	8	8
DTR	7	6
TxD	6	2
GND	5	5
GND	4	5
RxD	3	3
DSR	2	4
CTS	1	7

MGMT 10/100/1000 Ethernet Port

The MGMT 10/100/1000 Ethernet port is an Ethernet port with an RJ-45 connector. You can use a modular, RJ-45, straight-through UTP cable to connect the management port to an external hub, switch, or router.

Table C-3 lists the cable pinouts for 10/100/1000BASE-T Management Port Cable Pinouts (MDI).

Table C-3 10/100/1000BASE-T Management Port Cable Pinouts (MDI)

Signal	Pin
TD+	1
TD-	2
RD+	3
RD-	6
Not used	4
Not used	5
Not used	7
Not used	8

Gigabit and Fibre Channel Ports

Table C-4 lists the types of SFP modules and connectors used in the adaptive security appliance.

Table C-4 SFP Modules and Connectors

Port	Compliance	Connector	Fiber Type
Gigabit Ethernet	1000BASE-SX	SW	MMF
	1000BASE-LX	LW	SMF

Table C-5 lists the SFP port cabling specifications for the SFP modules and connectors used in the adaptive security appliance.

Table C-5 SFP Port Cabling Specifications

Cisco Product Number	Wavelength (nanometer)	Core Size (micron)	Baud Rate	Cable Distance
GLC-SX-MM=	850	62.5	1.0625	300 m
		50.0	1.0625	500 m
GLC-LH-SM=	1300	9.0	1.0625	10 km



Numerics

4GE SSM [A-3](#)

A

AIP SSM

see SSM [A-8](#)

AUX port [3-2](#)

C

chassis covers

removing [B-1](#)

replacing [B-3](#)

circuit breaker for DC unit [1-3](#)

Cisco warranty [1-2](#)

CompactFlash

External [3-2, 3-3](#)

Internal [B-10, B-13](#)

Console port [3-10](#)

CPU [3-5](#)

CSC SSM

see SSM [A-8](#)

E

electrostatic discharge

see ESD

equipment racks

tips [1-5](#)

ESD

preventing [1-4, B-4](#)

F

fans

ventilation [1-5](#)

G

grounding lug

attaching [B-9](#)

I

installing [2-3, 3-8](#)

L

LC connector [3-13](#)

LEDs [3-4, A-2, A-9](#)

M

Management Port [3-9](#)

memory requirements [3-5](#)

MGMT [3-2, 3-3, 3-9](#)

N

Network interfaces [3-2](#)

P

panel

removing [B-2](#)

power LEDs [3-4](#), [A-2](#), [A-9](#)
power supplies
 considerations [1-5](#)
product overview [2-2](#), [3-2](#)

R

rear panels (figure) [3-4](#)
Removing [B-10](#)
RJ-45 connector
 pinouts [C-3](#)
RJ-45 port [3-12](#)
rubber feet
 attaching [3-7](#)

S

safety [1-2](#)
Serial Console port [3-2](#), [3-3](#)
SFP [3-13](#), [A-4](#)
site environment [1-4](#)
SSM
 4GE SSM
 connecting [3-12](#)
 installing [A-3](#)
 LEDs [3-4](#), [A-2](#)
 replacing [A-4](#)
 Intelligent SSM [A-8](#)
 connecting [3-14](#)
 installing [A-9](#)
 LEDs [A-9](#)
 replacing [A-10](#)

V

ventilation fans [1-5](#)

W

warranty [1-2](#)