



Preface

This guide describes the Cisco Secure Access Control Server Release 4.0 Solution Engine, hereafter referred to as ACS.

Audience

This guide is for system administrators who use ACS, and who set up and maintain accounts and dial-in network security.

Organization

This document contains the following chapters and appendixes:

- **Chapter 1, “Overview”**—An overview of ACS and its features, network diagrams, and system requirements.
- **Chapter 2, “Deployment Considerations”**—A guide to deploying ACS that includes requirements, options, trade-offs, and suggested sequences.
- **Chapter 3, “Using the Web Interface”**—Concepts and procedures regarding how to use the Interface Configuration section of ACS to configure the HTML interface.
- **Chapter 4, “Network Configuration”**—Concepts and procedures for establishing ACS network configuration and building a distributed system.
- **Chapter 5, “Shared Profile Components”**—Concepts and procedures regarding ACS shared profile components: downloadable IP acls, network access filters, network access restrictions, and device command sets.
- **Chapter 6, “User Group Management”**—Concepts and procedures for establishing and maintaining ACS user groups.
- **Chapter 7, “User Management”**—Concepts and procedures for establishing and maintaining ACS user accounts.
- **Chapter 8, “System Configuration: Basic”**—Concepts and procedures regarding the basic features found in the System Configuration section of ACS.
- **Chapter 9, “System Configuration: Advanced”**—Concepts and procedures regarding RDBMS Synchronization, Cisco Secure Database Replication, and IP pools, found in the System Configuration section of ACS.

- **Chapter 10, “System Configuration: Authentication and Certificates”**—Concepts and procedures regarding the Global Authentication and ACS Certificate Setup pages, found in the System Configuration section of ACS.
- **Chapter 11, “Logs and Reports”**—Concepts and procedures regarding ACS logging and reports.
- **Chapter 12, “Administrators and Administrative Policy”**—Concepts and procedures for establishing and maintaining ACS administrators.
- **Chapter 13, “User Databases”**—Concepts about user databases and procedures for configuring ACS to perform user authentication with external user databases.
- **Chapter 14, “Posture Validation”**—Concepts and procedures for implementing Posture Validation (also known as Network Admission Control or NAC) and configuring posture validation policies.
- **Chapter 15, “Network Access Profiles”**—Concepts and procedures for creating Network Access Profiles and implementing profile-based policies in ACS.
- **Chapter 16, “Unknown User Policy”**—Concepts and procedures about using the Unknown User Policy with posture validation and unknown user authentication.
- **Chapter 17, “User Group Mapping and Specification”**—Concepts and procedures regarding the assignment of groups for users authenticated by an external user database.
- **Appendix A, “Troubleshooting”**—How to identify and solve certain problems you might have with ACS.
- **Appendix B, “TACACS+ Attribute-Value Pairs”**—A list of supported TACACS+ AV pairs and accounting AV pairs.
- **Appendix C, “RADIUS Attributes”**—A list of supported RADIUS AV pairs and accounting AV pairs.
- **Appendix D, “VPDN Processing”**—An introduction to Virtual Private Dial-up Networks (VPDN), including stripping and tunneling, with instructions for enabling VPDN on ACS.
- **Appendix E, “RDBMS Synchronization Import Definitions”**—A list of import definitions, for use with the RDBMS Synchronization feature.
- **Appendix F, “Internal Architecture”**—A description of ACS architectural components.

Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	boldface font
Variables for which you supply values and new or important terminology	<i>italic</i> font
Displayed session and system information, paths and file names	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> font
Menu items and button names	boldface font
Indicates menu items to select, in the order you select them.	Option > Network Preferences

**Tip**

Identifies information to help you get the most benefit from your product.

**Note**

Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

**Warning**

Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.

Product Documentation

**Note**

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

Table 1 describes the product documentation that is available.

Table 1 **Product Documentation**

Document Title	Available Formats
<i>Documentation Guide for Cisco Secure ACS Solution Engine, 4.0</i>	<ul style="list-style-type: none"> Shipped with product. PDF on the product CD-ROM. On Cisco.com.
<i>Release Notes for Cisco Secure ACS Solution Engine 4.0</i>	<ul style="list-style-type: none"> On Cisco.com.
<i>Installation and Setup Guide for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com. Printed document available by order (part number DOC-78-17249-01).¹
<i>User Guide for Cisco Secure Access Control Server Solution Engine</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com. Printed document available by order (part number DOC-78-17345-01).¹
<i>Installation and User Guide for Cisco Secure ACS User-Changeable Passwords</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com.

Table 1 **Product Documentation (continued)**

Document Title	Available Formats
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine Release 4.0</i>	<ul style="list-style-type: none"> On Cisco.com.
Online Documentation	In the ACS HTML interface, click Online Documentation.
Online Help	In the ACS HTML interface, online help appears in the right-hand frame when you are configuring a feature.

1. See [Obtaining Documentation](#), page xxvi.

Related Documentation



Note

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

A set of white papers about ACS are available on Cisco.com at:

<http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml>

For information on Network Admission Control, various NAC components, and ACS see:

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

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco ripostes at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

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

Documentation Feedback

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

You can send comments about Cisco 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

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

- Nonemergencies—psirt@cisco.com

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

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



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 linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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



Note

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

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

<http://www.ciscopress.com>

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

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

