



Preface

This document will help you configure and use Cisco Secure Access Control Server (ACS) and its features and utilities.

Audience

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

Organization

This document contains the following chapters and appendices:

- **Chapter 1, “Overview”**—An overview of Cisco Secure ACS and its features, network diagrams, and system requirements.
- **Chapter 2, “Deployment Considerations”**—A guide to deploying Cisco Secure ACS that includes requirements, options, trade-offs, and suggested sequences.
- **Chapter 3, “Interface Configuration”**—Concepts and procedures regarding how to use the Interface Configuration section of Cisco Secure ACS to configure the HTML interface.
- **Chapter 4, “Network Configuration”**—Concepts and procedures for establishing Cisco Secure ACS network configuration and building a distributed system.

- **Chapter 5, “Shared Profile Components”**—Concepts and procedures regarding Cisco Secure 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 Cisco Secure ACS user groups.
- **Chapter 7, “User Management”**—Concepts and procedures for establishing and maintaining Cisco Secure ACS user accounts.
- **Chapter 8, “System Configuration: Basic”**—Concepts and procedures regarding the basic features found in the System Configuration section of Cisco Secure ACS.
- **Chapter 9, “System Configuration: Advanced”**—Concepts and procedures regarding RDBMS Synchronization, CiscoSecure Database Replication, and IP pools, found in the System Configuration section of Cisco Secure 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 Cisco Secure ACS.
- **Chapter 11, “Logs and Reports”**—Concepts and procedures regarding Cisco Secure ACS logging and reports.
- **Chapter 12, “Administrators and Administrative Policy”**—Concepts and procedures for establishing and maintaining Cisco Secure ACS administrators.
- **Chapter 13, “User Databases”**—Concepts about user databases and procedures for configuring Cisco Secure ACS to perform user authentication with external user databases.
- **Chapter 14, “Network Admission Control”**—Concepts and procedures for implementing Network Admission Control (NAC) and configuring NAC databases, policies, and rules.
- **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 Cisco Secure 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, “CSUtil Database Utility”**—Instructions for using CSUtil.exe, a command line utility you can use to work with the CiscoSecure user database, to import AAA clients and users, to define RADIUS vendors and attributes, and to generate PAC files for EAP-FAST clients.
- **Appendix E, “VPDN Processing”**—An introduction to Virtual Private Dial-up Networks (VPDN), including stripping and tunneling, with instructions for enabling VPDN on Cisco Secure ACS.
- **Appendix F, “RDBMS Synchronization Import Definitions”**—A list of import definitions, for use with the RDBMS Synchronization feature.
- **Appendix G, “Internal Architecture”**—A description of Cisco Secure 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 font</i>
Displayed session and system information, paths and file names	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen font</i>
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>Release Notes for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com.

Table 1 Product Documentation (continued)

Document Title	Available Formats
<i>Installation Guide for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816529=).¹
<i>User Guide for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816530=).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.
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> • On Cisco.com.
<i>Recommended Resources for the Cisco Secure ACS User</i>	<ul style="list-style-type: none"> • On Cisco.com.
Online Documentation	In the Cisco Secure ACS HTML interface, click Online Documentation.
Online Help	In the Cisco Secure ACS HTML interface, online help appears in the right-hand frame when you are configuring a feature.

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

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.

Table 2 describes a set of white papers about Cisco Secure ACS. All white papers are available on Cisco.com. To view them, go to the following URL:

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

Table 2 *Related Documentation*

Document Title	Description and Available Formats
<i>Building a Scalable TACACS+ Device Management Framework</i>	This document discusses the key benefits of and how to deploy Cisco Secure ACS Shell Authorization Command sets, which provide the facilities constructing a scalable network device management system using familiar and efficient TCP/IP protocols and utilities supported by Cisco devices.
<i>Catalyst Switching and ACS Deployment Guide</i>	This document presents planning, design, and implementation practices for deploying Cisco Secure ACS for Windows Server in support of Cisco Catalyst Switch networks. It discusses network topology regarding AAA, user database choices, password protocol choices, access requirements, and capabilities of Cisco Secure ACS.
<i>Cisco Secure ACS for Windows vs. Cisco Secure ACS for UNIX</i>	This bulletin compares the overall feature sets of Cisco Secure ACS for Windows and CiscoSecure ACS for UNIX. It also examines the advantages and disadvantages of both platforms and discusses issues related to migrating from the UNIX-based product to the Windows version.
<i>Configuring LDAP</i>	This document outlines deployment concepts for Cisco Secure ACS when authenticating users of a Lightweight Directory Access Protocol (LDAP) directory server, and describes how to use these concepts to configure Cisco Secure ACS.
<i>Deploying Cisco Secure ACS for Windows in a Cisco Aironet Environment</i>	This paper discusses guidelines for wireless network design and deployment with Cisco Secure ACS.
<i>EAP-TLS Deployment Guide for Wireless LAN Networks</i>	This document discusses the Extensible Authentication Protocol Transport Layer Security (EAP-TLS) authentication protocol deployment in wireless networks. It introduces the EAP-TLS architecture and then discusses deployment issues.

Table 2 *Related Documentation (continued)*

Document Title	Description and Available Formats
<i>External ODBC Authentication</i>	This paper presents concepts and configuration issues in deploying Cisco Secure ACS for Windows Server to authenticate users against an external open database connectivity (ODBC) database. This paper also describes configuring, testing, and troubleshooting a relational database management system (RDBMS) with ODBC and Cisco Secure ACS, and provides sample Structured Query Language (SQL) procedures.
<i>Guidelines for Placing ACS in the Network</i>	This document discusses planning, design, and implementation practices for deploying Cisco Secure ACS for Windows Server in an enterprise network. It discusses network topology, user database choices, access requirements, integration of external databases, and capabilities of Cisco Secure ACS.
<i>Initializing MC Authorization on ACS 3.1</i>	This application note explains how to initialize Management Center authorization on Cisco Secure ACS.
<i>Securing ACS Running on Microsoft Windows Platforms</i>	This paper describes how the Cisco Secure ACS can be protected against the vulnerabilities of the Windows 2000 operating system and explains how to improve security on the computer running Cisco Secure ACS. It discusses making the system dedicated to Cisco Secure ACS, removing all unnecessary services, and other measures. It also discusses how to improve administrative security for Cisco Secure ACS through such methods as stronger passwords and controlled administrative access. This paper concludes with considerations of physical security for Cisco Secure ACS and its host.

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

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

Documentation Feedback

You can 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.

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>

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 automatically provides

recommended solutions. If your issue is not resolved using the recommended resources, your service request will be 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/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press 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>