



Preface

Audience

This guide is for security administrators who use ACS, and who set up and maintain network and application security.

Organization



Note

This release of the User Guide combines the Windows and Solution Engine platforms. Where necessary, the appropriate platform is clearly identified.

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, “Using the Web Interface”**—Concepts and procedures regarding how to use the Interface Configuration section of ACS to configure the HTML interface.
- **Chapter 3, “Network Configuration”**—Concepts and procedures for establishing ACS network configuration and building a distributed system.
- **Chapter 4, “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 5, “User Group Management”**—Concepts and procedures for establishing and maintaining ACS user groups.
- **Chapter 6, “User Management”**—Concepts and procedures for establishing and maintaining ACS user accounts.
- **Chapter 7, “System Configuration: Basic”**—Concepts and procedures regarding the basic features found in the System Configuration section of ACS.
- **Chapter 8, “System Configuration: Advanced”**—Concepts and procedures regarding RDBMS Synchronization, ACS Internal Database Replication, and IP pools, found in the System Configuration section of ACS.
- **Chapter 9, “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 10, “Logs and Reports”**—Concepts and procedures regarding ACS logging and reports.
- **Chapter 11, “Administrators and Administrative Policy”**—Concepts and procedures for establishing and maintaining ACS administrators.
- **Chapter 12, “User Databases”**—Concepts about user databases and procedures for configuring ACS to perform user authentication with external user databases.
- **Chapter 13, “Posture Validation”**—Concepts and procedures for implementing Posture Validation (also known as Network Admission Control or NAC) and configuring posture validation policies.
- **Chapter 14, “Network Access Profiles”**—Concepts and procedures for creating Network Access Profiles and implementing profile-based policies in ACS.
- **Chapter 15, “Unknown User Policy”**—Concepts and procedures about using the Unknown User Policy with posture validation and unknown user authentication.
- **Chapter 16, “User Group Mapping and Specification”**—Concepts and procedures regarding the assignment of groups for users authenticated by an external user database.
- **Appendix A, “TACACS+ Attribute-Value Pairs”**—A list of supported TACACS+ AV pairs and accounting AV pairs.
- **Appendix B, “RADIUS Attributes”**—A list of supported RADIUS AV pairs and accounting AV pairs.
- **Appendix C, “CSUtil Database Utility”**—Instructions for using CSUtil.exe, a command line utility you can use to work with the ACS internal database, to import AAA clients and users, to define RADIUS vendors and attributes, and to generate (Protected Access Credentials) PAC files for EAP-FAST clients.
- **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 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 I-1 describes the product documentation that is available.

Table I-1 **Product Documentation**

| Document Title | Available Formats |
|---|--|
| <i>Documentation Guide for Cisco Secure ACS Release 4.2</i> | <ul style="list-style-type: none"> Shipped with product. PDF on the product CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/roadmap/DGuide42.html |
| <i>Release Notes for Cisco Secure ACS Release 4.2</i> | <ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/release/notes/ACS42_RN.html |
| <i>Configuration Guide for Cisco Secure ACS Release 4.2</i> | <ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs42_config_guide.html |

Table I-1 **Product Documentation (continued)**

| Document Title | Available Formats |
|---|---|
| <i>Installation Guide for Cisco Secure ACS for Windows Release 4.2</i> | <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/IGwn42.html |
| <i>Installation Guide for Cisco Secure ACS Solution Engine Release 4.2</i> | <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/solution_engine/SE42.html |
| <i>User Guide for Cisco Secure Access Control Server 4.2</i> | <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/ACS4_2UG.html <p>You can also access the user guide by clicking Online Documentation in the ACS navigation bar. The user guide PDF is available on this page by clicking View PDF.</p> |
| <i>Regulatory Compliance and Safety Information for the Cisco Secure ACS Solution Engine Release 4.2</i> | <ul style="list-style-type: none"> • Shipped with product. • PDF on the product CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/regulatory/compliance/RCSI_42.html |
| <i>Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2</i> | <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/remote_agent/RA42.html |
| <i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine Release 4.2</i> | <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/device/guide/sdt42.html |
| <i>Installation and User Guide for Cisco Secure ACS User-Changeable Passwords</i> | <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/user_passwords/ucpNW42.html |

Table I-1 **Product Documentation (continued)**

| Document Title | Available Formats |
|---|--|
| <i>Cisco Secure Access Control Server Troubleshooting Guide</i> | <ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/trouble/guide/ACSTrbG42.html |
| 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. |

Related Documentation



Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on [Cisco.com](http://www.cisco.com) for any updates.

A set of white papers about ACS are available on [Cisco.com](http://www.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 and Submitting a Service Request

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

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

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

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (ey@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

