



## About This Guide

---

### Audience

This guide is for system administrators who install and configure Cisco Secure ACS, hereafter referred to as ACS, and set up and maintain accounts and dial-in network security.

### Organization

This document contains the following chapters:

- [Chapter 1, “Overview of ACS Configuration”](#)—Provides an overview of ACS configuration, including a summary of configuration steps and configuration flowchart that show the sequence of configuration steps.
- [Chapter 2, “Deploy the Access Control Servers”](#)—Describes factors to consider when deploying ACS, including the access type, network topology, and whether database synchronization and replication are required.
- [Chapter 3, “Password Policy Configuration Scenario”](#)—Describes how to configure Sarbanes-Oxley (SOX) support when adding administrators.
- [Chapter 4, “Agentless Host Support Configuration Scenario”](#)—Describes how to configure ACS for agentless host support (MAC authentication bypass).
- [Chapter 5, “PEAP/EAP-TLS Configuration Scenario”](#)—Describes how to configure ACS for PEAP/EAP-TLS support.
- [Chapter 6, “Syslog Logging Configuration Scenario”](#)—Describes how to configure ACS to log syslog messages.
- [Chapter 7, “NAC Configuration Scenario”](#)—Describes how to configure ACS in a Cisco Network Admission Control (NAC) environment.
- [“Glossary”](#)—Lists common terms used in ACS.

# Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	<b>boldface font</b>
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	<b>boldface screen font</b>
Variables you enter	<i>italic screen font</i>
Menu items and button names	<b>boldface font</b>
Indicates menu items to select, in the order you select them.	<b>Option &gt; Network Preferences</b>



## 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

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates. You can link to the documentation for Cisco Secure ACS for Windows is located from this location:

<http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html>

You can link to the documentation for Cisco Secure ACS Solution Engine from this location:

<http://www.cisco.com/en/US/products/sw/secursw/ps5338/index.html>

Table 1 describes the product documentation that is available.

**Table 1**      **Product Documentation**

<b>Document Title</b>	<b>Available Formats</b>
<i>Documentation Guide for Cisco Secure ACS Release 4.1</i>	<ul style="list-style-type: none"> <li>Shipped with product.</li> <li>PDF on the product CD-ROM.</li> <li>On <a href="http://www.cisco.com">Cisco.com</a> at: <a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_documentation_roadmaps_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_documentation_roadmaps_list.html</a></li> </ul>
<i>Release Notes for Cisco Secure ACS Release 4.1</i>	On <a href="http://www.cisco.com">Cisco.com</a> : <a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html</a>
<i>User Guide for Cisco Secure Access Control Server 4.1</i>	On <a href="http://www.cisco.com">Cisco.com</a> <a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html</a>
<i>Configuration Guide for Cisco Secure ACS Release 4.1</i>	On <a href="http://www.cisco.com">Cisco.com</a> : <a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html</a>
<i>Installation Guide for Cisco Secure ACS for Windows Release 4.1</i>	On <a href="http://www.cisco.com">Cisco.com</a> : <a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html</a>
<i>Installation Guide for Cisco Secure ACS Solution Engine Release 4.1</i>	On <a href="http://www.cisco.com">Cisco.com</a> : <a href="http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html</a>
<i>Regulatory Compliance and Safety Information for the Cisco Secure ACS Solution Engine Release 4.1</i>	<ul style="list-style-type: none"> <li>Shipped with product.</li> <li>PDF on the product CD-ROM.</li> <li>On <a href="http://www.cisco.com">Cisco.com</a>: <a href="http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html</a></li> </ul>
<i>Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.1</i>	On <a href="http://www.cisco.com">Cisco.com</a> : <a href="http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html</a>
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine Release 4.1</i>	On <a href="http://www.cisco.com">Cisco.com</a> : <a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_device_support_tables_list.html</a>
<i>Installation and User Guide for Cisco Secure ACS User-Changeable Passwords</i>	On <a href="http://www.cisco.com">Cisco.com</a> at the following location <a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html.html</a>
Online Documentation	In the ACS HTML interface, click <b>Online Documentation</b> .
Online Help	In the ACS HTML interface, online help appears in the right pane when you are configuring a feature.

# Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

## 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 websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

## Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

## Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

# 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](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to do the following:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—[security-alert@cisco.com](mailto: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.

- For nonemergencies—[psirt@cisco.com](mailto: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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key 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](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.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

# Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: <http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL: <http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

# 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 Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.

**Tip**

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box

and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

---

## 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 Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:  
<http://www.cisco.com/offer/subscribe>
- 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 channel product 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>
- *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 where networking professionals 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>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:  
<http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm>
- 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>