Installation and Configuration Guide for Cisco Secure ACS Remote Agents

Release 4.1

Americas 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: 408 527-0883

Text Part Number: OL-9975-02

Installation and Configuration Guide for Cisco Secure ACS Remote Agents

CONTENTS

Preface vii

- Audience vii
- Organization vii
- Conventions vii
- Product Documentation viii
- Related Documentation ix
- Obtaining Documentation x
  - Cisco.com x
  - Product Documentation DVD x
  - Ordering Documentation x
- Documentation Feedback xi
- Cisco Product Security Overview xi
  - Reporting Security Problems in Cisco Products xi
- Obtaining Technical Assistance xii
  - Cisco Technical Support & Documentation Website xii
  - Submitting a Service Request xiii
  - Definitions of Service Request Severity xiii
- Obtaining Additional Publications and Information xiii

CHAPTER 1 **Introduction to Cisco Secure ACS Remote Agents** 1-1

- Overview 1-1
- Limitations 1-2
- Remote Agent Concepts 1-2
  - Configuration Tools 1-2
  - Configuration Provider 1-2
  - Logging Overview 1-3
  - Authentication Overview 1-4
- Remote Agent Services 1-5
  - CSAgent 1-5
  - CSLogAgent 1-5
  - CSWinAgent 1-6
- Configuring ACS SE for a Remote Agent 1-7

CHAPTER 2 **Installing Cisco Secure ACS Remote Agent for Windows** 2-1

System Requirements 2-1
ACS Requirements 2-1
Hardware Requirements 2-2
Operating System Requirements 2-2
Tested Windows Security Patches 2-2
Network Requirements 2-3
Installing a Remote Agent for Windows 2-4
Uninstalling ACS Remote Agent for Windows 2-5
Upgrading ACS Remote Agent for Windows 2-5
Windows Authentication Configuration 2-6
Configuring for Domain Controller Authentication 2-6
Configuring for Member Server Authentication 2-9
Configuring Local Security Policies 2-13
Configuring the Remote Agent Service 2-15

CHAPTER 3 **Installing Cisco Secure ACS Remote Agent for Solaris** 3-1

System Requirements 3-1
ACS Requirements 3-1
Hardware Requirements 3-1
Operating System Requirements 3-2
Environment Variable Settings 3-2
Network Requirements 3-2
Installing a Remote Agent for Solaris 3-2
Uninstalling ACS Remote Agent for Solaris 3-5
Upgrading ACS Remote Agent for Solaris 3-6

CHAPTER 4 **Configuring and Maintaining a Remote Agent** 4-1

Configuring a Remote Agent 4-1
CSAgent.ini Location 4-1
CSAgent.ini Settings 4-2
Sample CSAgent.ini 4-5
Changing CSAgent.ini Settings 4-6
Maintaining a Remote Agent 4-7
Stopping and Starting Remote Agent Services 4-7
File and Directory Structure 4-8
Retrieving Support Logs 4-9
Running CSAgent in Debug Mode 4-9

Sample CSAgent Debug Output 4-11
Sample Debug Output for a Windows Remote Agent 4-11
Sample Debug Output for a Solaris Remote Agent 4-12

INDEX

Preface

This guide explains the roles of Cisco Secure Access Control Server (ACS) Remote Agents, and provides procedures for installing and configuring the remote agents for Microsoft Windows and Solaris.

Audience

This guide is written for network administrators and explains how Cisco Secure ACS Remote Agent works, and how to install and configure it for use with Cisco Secure ACS Solution Engine (ACS SE).

Organization

This document contains the following chapters:

- **Chapter 1, "Introduction to Cisco Secure ACS Remote Agents"**—Introduces remote agent concepts and features.
- **Chapter 2, "Installing Cisco Secure ACS Remote Agent for Windows"**—Provides installation information for Cisco Secure ACS Remote Agent for Windows Server, plus additional configuration information if the Windows authentication service is installed.
- **Chapter 3, "Installing Cisco Secure ACS Remote Agent for Solaris"**—Provides installation information for Cisco Secure ACS Remote Agent for Solaris.
- **Chapter 4, "Configuring and Maintaining a Remote Agent"**—Provides information about configuring and maintaining remote agents, including debugging information.

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	*italic* font
Displayed session and system information, paths and file names	`screen` font

Item	Convention
Information you enter	**`boldface screen`** font
Variables you enter	*italic screen* 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
Documentation Guide for Cisco Secure ACS Release 4.1	• Printed document with the product. • PDF on the product CD-ROM. • On Cisco.com.
Release Notes for Cisco Secure ACS Release 4.1	On Cisco.com.
Installation Guide for Cisco Secure ACS Solution Engine Release 4.1	• PDF on the product CD-ROM. • On Cisco.com.

Table 1 Product Documentation (continued)

Document Title	Available Formats
Product online help. Help topics for all pages in the ACS HTML interface.	Select an option from the ACS menu; the help appears in the right pane.
User Guide for Cisco Secure Access Control Server	• PDF on the product CD-ROM. • On Cisco.com. • You can also access the user guide by clicking **Online Documentation** in the ACS navigation menu. The user guide PDF is available on this page by clicking **View PDF**.
Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.1	• PDF on the product CD-ROM. • On Cisco.com.
Installation and User Guide for Cisco Secure ACS User-Changeable Passwords 4.1	• PDF on the product CD-ROM. • On Cisco.com.
Regulatory Compliance and Safety Information for the Cisco Secure ACS Solution Engine Release 4.1	• PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7817259).
Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine Release 4.1	On Cisco.com.

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 Cisco Secure ACS for Windows is available at:

http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/prod_white_papers_list.html

Much of the information in these papers is applicable to Cisco Secure ACS Solution Engine.

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 websites 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)—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, 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

- *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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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

CHAPTER 1

Introduction to Cisco Secure ACS Remote Agents

This chapter introduces Cisco Secure Access Control Server (ACS) Remote Agent for Windows and Cisco Secure ACS Remote Agent for Solaris.

This chapter contains:

- Overview, page 1-1
- Limitations, page 1-2
- Remote Agent Concepts, page 1-2
- Remote Agent Services, page 1-5
- Configuring ACS SE for a Remote Agent, page 1-7

Overview

ACS Remote Agent for Windows and ACS Remote Agent for Solaris are applications that support Cisco Secure ACS Solution Engine (ACS SE) for remote logging. Forwarding all accounting data from an appliance to a remote agent preserves disk space on the appliance. It also improves AAA performance by eliminating the frequent and time-consuming disk writes required for local logging on an appliance.

The Windows remote agent also supports Microsoft Windows authentication. If you want to support Microsoft Windows authentication with ACS SE, you must use ACS Remote Agent for Windows. Windows authentication requests must be submitted from a computer that is a member of a trusted Microsoft Windows domain. Because an ACS SE cannot be a member of a Microsoft Windows domain, ACS 4.1 provide ACS Remote Agent for Windows. As an application running on a computer that belongs to a trusted Microsoft Windows domain, the remote agent can successfully pass authentication requests to the domain. The remote agent submits to Microsoft Windows each authentication request that it receives from an appliance. When it receives the authentication response, the remote agent forwards the response to the appliance that initiated the request.

All communication between a remote agent and ACS SE is encrypted by using the Blowfish algorithm and a 128-bit key. Additionally, encryption session keys are randomized and exchanged between the remote agent and the appliances that it services by using a public key exchange protocol.

For more information, see Remote Agent Concepts, page 1-2.

Limitations

We designed ACS Remote Agent with these limitations:

- **Supports only ACS SE**—ACS for Windows is not supported.
- **Maximum number of appliances supported**—While a single ACS Remote Agent can provide services to many ACS SE appliances, support is limited to five concurrent connections by the appliances served. For example, if you have three primary ACS appliances, and three secondary ACS appliances that are used for failover purposes only, the remote agent can provide services to all six appliances and stay below the maximum of five concurrent connections.

Remote Agent Concepts

This section contains information about concepts fundamental to the operation and configuration of remote agents.

This section contains:

- Configuration Tools, page 1-2
- Configuration Provider, page 1-2
- Logging Overview, page 1-3
- Authentication Overview, page 1-4

Configuration Tools

ACS Remote Agent has no graphical user interface or command-line interface. Instead, it derives its configuration from:

- **CSAgent.ini**—A text file containing configuration values that the remote agent uses to configure itself when it starts. For more information, see Configuring a Remote Agent, page 4-1.
- **Configuration provider**—An ACS SE that provides additional configuration, especially for the remote agent logging service. For more information, see Configuration Provider, page 1-2.

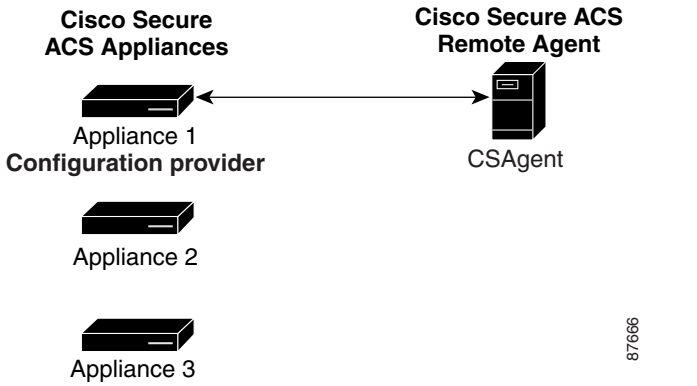
Configuration Provider

Although a remote agent can accept inbound communication from many appliances, it accepts configuration instructions from only a single appliance that you specify in the *CSAgent.ini* file. This special appliance is called a configuration provider.

When a remote agent starts, it reads its *CSAgent.ini* file to determine which services should be available and which appliance is its configuration provider. Then it contacts the configuration provider and requests its configuration.

After receiving its configuration from the configuration provider, the remote agent is available to provide the services configured in *CSAgent.ini*. The main service, CSAgent, controls overall remote agent startup and service availability. See Figure 1-1. For more information about the CSAgent service, see CSAgent, page 1-5.

Figure 1-1 Configuration Provider and a Remote Agent

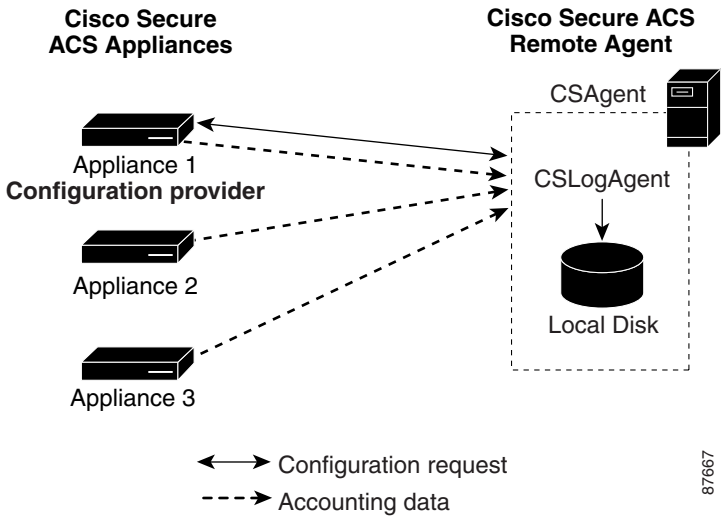


Logging Overview

The remote agent is particularly dependent on its configuration provider for logging configuration. The configuration provider determines the content of each log. You can configure remote agent logging on the Logging page of the System Configuration section of the configuration provider HTML interface. For more information, see *User Guide for Cisco Secure ACS Solution Engine*.

All ACS SE appliances that are configured to use the remote agent send logging data directly to the remote agent logging service, CSLogAgent. CSLogAgent writes the logging data to the hard disk in the location that the configuration provider specifies. The logs contain the columns that the configuration provider specifies. See Figure 1-2. For more information about the CSLogAgent service, see CSLogAgent, page 1-5.

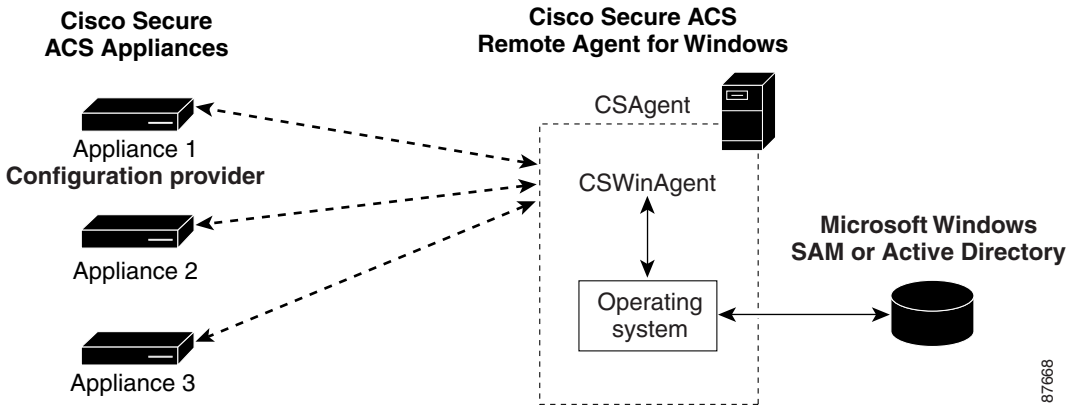
Figure 1-2 Multiple Appliances Logging to a Single Remote Agent



Authentication Overview

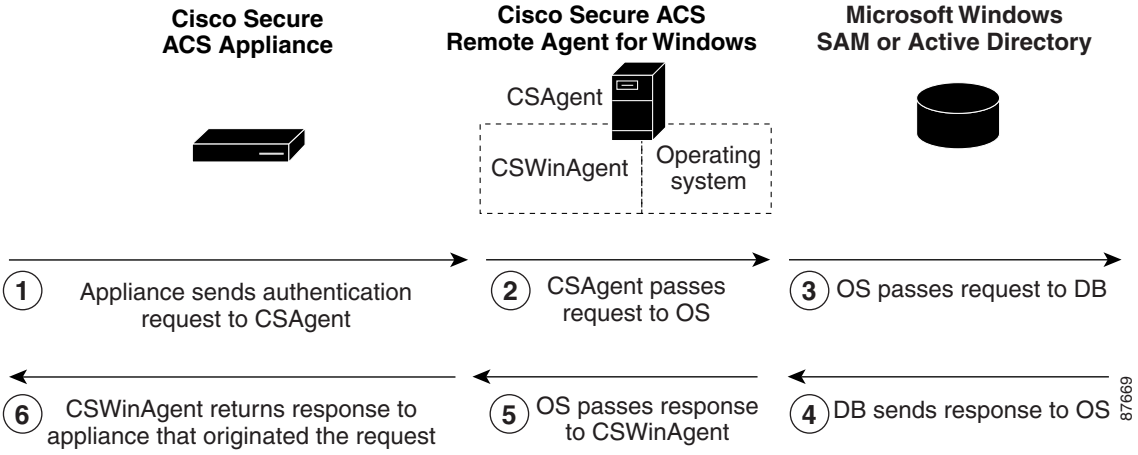
The Microsoft Windows authentication service, CSWinAgent, is available only in ACS Remote Agent for Windows. CSWinAgent processes several types of authentication-related requests from appliances. These include requests for user authentication, user lookup for EAP-TLS support, user group membership lookup, user dial-in permission lookup, and group enumeration (used for configuring group mapping on an appliance). All appliances that are configured to use the remote agent send Microsoft Windows authentication-related requests to CSWinAgent. See Figure 1-3.

Figure 1-3 Multiple Appliances Using Remote Agent for Windows Authentication



CSWinAgent acts as a middle-man by handling requests for multiple appliances. CSWinAgent passes requests to the operating system. The operating system returns the results of the requests to CSWinAgent. In turn, CSWinAgent passes the results of requests to the appliances originating the requests. See Figure 1-4. For more information about CSWinAgent, see CSWinAgent, page 1-6.

Figure 1-4 Windows Authentication Messaging



Remote Agent Services

This section describes the three separate services that ACS Remote Agent comprises:

- CSAgent, page 1-5
- CSLogAgent, page 1-5
- CSWinAgent, page 1-6

CSAgent

CSAgent is the main service. It controls the other services, CSLogAgent and, if you are using the Windows remote agent, CSWinAgent. When an appliance first contacts a remote agent, it queries CSAgent for its available services, as determined by the configuration of the *CSAgent.ini* file. If you use the Windows remote agent, it is the only service that is registered at installation as a Microsoft Windows service, named Cisco Secure ACS Agent.

This document provides information about the following aspects of the CSAgent service:

- **Central control of services**—CSAgent controls the other two services. To start the remote agent, you start CSAgent. To stop the remote agent, you stop CSAgent. CSAgent stops and starts the other services, as applicable. For more information, see Stopping and Starting Remote Agent Services, page 4-7.
- **Monitoring**—CSAgent performs basic monitoring of the other services. If CSLogAgent or CSWinAgent stops unexpectedly, CSAgent attempts to start it again. If restart fails, CSAgent waits ten seconds and attempts to restart the failed service.
- **Diagnostic log**—CSAgent records errors in its service log file, located in the Log subdirectory within the CSAgent directory. For more information, see File and Directory Structure, page 4-8.
- **Support log collection**—When an appliance sends it a request, CSAgent also collects diagnostic logs and compresses them into a single cabinet file. For more information, see Retrieving Support Logs, page 4-9.
- **Debug mode**—For debugging purposes, you can run CSAgent from an MS-DOS prompt, including verbose output. For more information, see Running CSAgent in Debug Mode, page 4-9.
- **Configurable TCP port**—By default, CSAgent listens on TCP port 2004 for requests from appliances. You can configure the port used. For more information, see Configuring a Remote Agent, page 4-1.
- **Restrictable client IP address range**—For additional security, you can restrict the IP addresses from which a remote agent will accept requests. For more information, see Configuring a Remote Agent, page 4-1.

CSLogAgent

CSLogAgent is the logging service. CSAgent controls the logging service but receives logging data from appliances directly. When CSLogAgent starts, it requests its configuration from the configuration provider specified in the *CSAgent.ini* file. After it has received its configuration, it is ready to perform logging services. If CSLogAgent encounters problems receiving its configuration from the configuration provider, it restarts periodically until it succeeds in receiving its configuration.

This document provides information about the following aspects of the CSLogAgent service:

- **Centralized collection of accounting data**—CSLogAgent writes logging data in comma-separated value (CSV) files, which are easily imported into many popular applications, such as spreadsheets and relational databases. You can also use a third-party reporting tool to manage accounting data. For example, aaa-reports! by Extraxi supports ACS. The values recorded in each report type are determined by the configuration provider. You configure the reports by using the HTML interface of the configuration provider defined in the *CSAgent.ini file*. For information about log locations, see File and Directory Structure, page 4-8. For information about configuring logs in the HTML interface of a configuration provider, see *User Guide for Cisco Secure ACS Solution Engine*.
- **Diagnostic log**—CSLogAgent records errors in its service log file, located in the Log subdirectory within the CSLogAgent directory. For more information, see File and Directory Structure, page 4-8.
- **Debug mode**—When you run CSAgent in debug mode, CSLogAgent is also run in debug mode, including support for verbose output. For more information, see Running CSAgent in Debug Mode, page 4-9.
- **Configurable TCP ports**—By default, CSLogAgent listens to TCP port 2006 for communication with the configuration provider and on TCP port 2007 for accounting data from any permitted appliance. For more information, see Configuring a Remote Agent, page 4-1.
- **Restrictable client IP address range**—For additional security, you can restrict the IP addresses from which a remote agent will accept logging-related requests or data. For more information, see Configuring a Remote Agent, page 4-1.

CSWinAgent

The CSWinAgent service is included only in the Windows remote agent. The CSWinAgent service supports Microsoft Windows authentication. The CSAgent controls this service; but it receives authentication requests from appliances directly on the ports on which it is configured to listen. It supports authentication of users and machines, user password changes, and retrieval of group memberships. CSWinAgent makes no decisions about user access. Instead, it passes the results of its Microsoft Windows queries to the appliance initiating the query.

CSWinAgent maintains an open pool of connections to provide better throughput during peaks in requests from appliances.

For PAP and EAP-GTC authentication requests, ACS SE converts the plaintext password to Microsoft-Challenge-Handshake Authentication Protocol (MS-CHAP) credentials before sending the request to a remote agent. This conversion is extra security because all communication between a remote agent and an appliance is 128-bit encrypted.

This document provides information about the following aspects of the CSWinAgent service:

- **Diagnostic log**—CSWinAgent records errors in its service log file, which reside in the Log subdirectory within the CSWinAgent directory. For more information, see File and Directory Structure, page 4-8.
- **Debug mode**—When you run CSAgent in debug mode, CSWinAgent is also run in debug mode, including support for verbose output. For more information, see Running CSAgent in Debug Mode, page 4-9.
- **Configurable TCP ports**—By default, CSWinAgent listens to TCP port 2005 for communication with the configuration provider. For more information, see Configuring a Remote Agent, page 4-1.
- **Restrictable client IP address range**—For additional security, you can restrict the IP addresses from which a remote agent will accept authentication-related requests. For more information, see Configuring a Remote Agent, page 4-1.

Configuring ACS SE for a Remote Agent

You can configure how ACS SE uses a remote agent. On the appliance that is configured as a configuration provider, the logging configuration determines how the remote agent performs its logging service.

The *User Guide for Cisco Secure ACS Solution Engine* contains information about:

- Adding a remote agent to the network configuration of ACS SE.
- Performing Windows authentication with remote agents.
- Logging with remote agents.

CHAPTER 2

Installing Cisco Secure ACS Remote Agent for Windows

This chapter provides information about installing Cisco Secure Access Control Server (ACS) Remote Agent for Windows.

This chapter contains:

- System Requirements, page 2-1
- Network Requirements, page 2-3
- Installing a Remote Agent for Windows, page 2-4
- Uninstalling ACS Remote Agent for Windows, page 2-5
- Upgrading ACS Remote Agent for Windows, page 2-5
- Windows Authentication Configuration, page 2-6

System Requirements

The computer running ACS Remote Agent for Windows must meet the minimum requirements detailed in:

- ACS Requirements, page 2-1
- Hardware Requirements, page 2-2
- Operating System Requirements, page 2-2

ACS Requirements

You must use ACS Remote Agent for Windows, version 4.1, with ACS Solution Engine, version 4.1. Other releases of Cisco Secure ACS are not supported.

Note ACS Remote Agent 4.1 for Windows does not support 64-bit operating systems.

Hardware Requirements

The computer running ACS Remote Agent for Windows must contain:

- Pentium III processor, 550 MHz or faster.
- 256 MB of RAM.
- At least 250 MB of free disk space.

Operating System Requirements

The computer running ACS Remote Agent for Windows must use one of the following operating systems:

- Windows 2000 Server, with Service Pack 3 or Service Pack 4 installed.
- Windows 2000 Advanced Server:
  - With Service Pack 3 or Service Pack 4 installed.
  - Without Microsoft clustering service installed.
  - Without other features specific to Windows 2000 Advanced Server enabled.

Note We have not tested and cannot support the multiprocessor feature of Windows 2000 Advanced Server. Windows 2000 Datacenter Server is not a supported operating system.

- Windows Server 2003, Standard Edition.
- Windows Server 2003, Enterprise Edition.

ACS Remote Agent for Windows 4.1 is also supported on Japanese Operating System (JOS) Windows 2000 and Windows 2003.

Tested Windows Security Patches

ACS Remote Agent for Windows has been tested with the Windows Server 2003 patches documented in the following Microsoft Knowledge Base articles:

- 819696
- 823182
- 823559
- 824105
- 824141
- 824146
- 825119
- 828028
- 828035
- 828741
- 832894

- 835732
- 837001
- 837009
- 839643
- 840374

ACS Remote Agent for Windows has been tested with the Windows 2000 Server patches documented in the following Microsoft Knowledge Base Articles:

- 329115
- 823182
- 823559
- 823980
- 824105
- 824141
- 824146
- 825119
- 826232
- 828035
- 828741
- 828749
- 835732
- 837001
- 839643

Network Requirements

Your network must meet the following requirements before you begin installing ACS.

- The computer running ACS Remote Agent for Windows must be able to ping the ACS Solution Engines that it supports.
- Gateway devices must permit traffic between the computer running ACS Remote Agent for Windows and the ACS SE. Specifically, the remote agent must receive TCP communication on TCP ports that you configure in *CSAgent.ini*. The default TCP ports, if all services are used, are 2004, 2005, 2006, and 2007. The appliance must receive TCP communication on TCP port 2003.

Note By using the *CSAgent.ini* file, you can configure the ports that the remote agent uses to communicate with ACS. If you change the ports used, you must configure intervening gateway devices to permit TCP traffic on the ports that you configure the remote agent to use. For more information about changing the ports that a remote agent uses, see Configuring a Remote Agent, page 4-1.

Installing a Remote Agent for Windows

Before You Begin

Determine the IP address of the Cisco Secure ACS SE that will be the configuration provider for this remote agent. For more information about configuration providers, see Configuration Provider, page 1-2.

To install ACS Remote Agent for a Windows operating system:

Step 1 By using the local administrator account, log in to the Microsoft Windows server on which you want to install ACS Remote Agent.

Step 2 Insert the ACS Software Migration CD into a CD-ROM drive on the Microsoft Windows server.

If the CD-ROM drive supports the Windows autorun feature, a dialog box might appear. Click **Cancel** to close the dialog box.

Note If the computer does not have a required service pack installed, a dialog box may appear. You can apply Windows service packs before or after installing ACS Remote Agent. You can continue with the installation, but the required service pack must be applied after the installation is complete; otherwise, ACS Remote Agent may not function reliably.

Step 3 On the ACS Software Migration CD, locate the Windows remote agent subdirectory.

Step 4 From the Windows remote agent subdirectory, run `Setup.exe`.

The Welcome dialog box displays basic information about the setup program.

Step 5 After you have read the information in the Welcome dialog box, click **Next**.

The Choose Destination Location dialog box appears.

Step 6 The installation location appears under Destination Folder. You can change the installation location.

Click **Next**.

Step 7 The Agent Services dialog box appears with a list of options that ACS Remote Agent for Windows supports.

Step 8 Select the agent services that you want to use:

- Logging Service
- Windows Authentication Service

Click **Next**. The Configuration Provider dialog box appears.

Step 9 In the **Hostname** box, type the hostname or IP address of the ACS Solution Engine that should control the configuration of this remote agent.

Note If you type a hostname, be sure that DNS is operating correctly or that the appliance hostname is in the local hosts file.
You can add the IP address or hostname at a later time, before using Remote Agent, by editing the configuration file, *CSAgent.ini*.

Step 10 Click **Next**.

The setup program installs ACS Remote Agent for Windows.

The Setup Complete dialog box lists options for restarting the computer.

Step 11 Select the reboot option that you want.

Note To complete the installation successfully you must reboot. If you chose not to reboot now, do so before you use remote agent services.

Step 12 Click **Finish**.

The setup program exits. If you chose to reboot the computer automatically, Windows restarts.

Where to go next:

- If want to authenticate users with a Windows domain user database, you must perform the additional Windows configuration discussed in Windows Authentication Configuration, page 2-6.

  Note If you are reinstalling the remote agent after uninstalling it, the previous configuration of the remote agent service was lost during the uninstallation. For more information, see Windows Authentication Configuration, page 2-6.

- If you want to use the Logging Service, you must perform additional configuration in ACS SE. See *User Guide for ACS Solution Engine* for more information.

Uninstalling ACS Remote Agent for Windows

Use Windows Control Panel to uninstall ACS Remote Agent for Windows. No special steps are required.

Note If you do not intend to reinstall ACS Remote Agent for Windows on this computer, remove the applicable remote agent configurations from all ACS Solution Engines.

Upgrading ACS Remote Agent for Windows

The upgrade process entails uninstalling the old version of the remote agent and installing the new version.

To upgrade ACS Remote Agent for Windows software:

Step 1 Remove the old version of the remote agent by performing the steps in Uninstalling ACS Remote Agent for Windows, page 2-5.

Step 2 By using the version of ACS Remote Agent for Windows to which you want to upgrade, perform the steps in Installing a Remote Agent for Windows, page 2-4.

Windows Authentication Configuration

If ACS uses Windows databases to authenticate users, you must perform additional configuration for reliable user authentication and group mapping. Requirements vary depending on whether you installed the remote agent on a domain controller or member server.

This section contains:

- Configuring for Domain Controller Authentication, page 2-6
- Configuring for Member Server Authentication, page 2-9

Configuring for Domain Controller Authentication

When ACS Remote Agent for Windows runs on a domain controller and you need to authenticate users with a Windows user database, the additional configuration required varies, depending upon your Windows networking configuration. Some of the subsequent steps are always applicable when the remote agent runs on a domain controller; other steps are required only in certain conditions, as noted at the beginning of the step.

Perform only those steps that always apply and those that apply to your Windows networking configuration:

Step 1 Add CISCO workstation.

To satisfy Windows requirements for authentication requests, ACS must specify the Windows workstation in to which the user tries to log. Because ACS cannot determine this information from authentication requests that AAA clients send, it uses a generic workstation name for all requests. Use *CISCO* as the name of the workstation.

In the local domain, and in each trusted domain and child domain that ACS will use to authenticate users, ensure that:

- A computer account named *CISCO* exists.
- All users that Windows will authenticate have permission to log in to the computer named *CISCO*.

For more information, see the Microsoft documentation for your operating system.

Step 2 Verify the server service status.

The remote agent depends on the Server service, which is a standard service in Microsoft Windows. On the computer that is running the remote agent, verify that the Server service is running and that its Startup Type is set to *Automatic*.

Tip To configure the Server service, use the local administrator account to log in to the computer that is running ACS. Choose **Start > Programs Administrative Tools > Services**. The services appear alphabetically.

For more information, see the Microsoft documentation for your operating system.

Step 3 Verify the NTLM version.

Note This step is required only if ACS authenticates users who belong to trusted domains or child domains.

ACS supports authentication of Windows credentials by using LAN Manager (LM), NTLM version 1, or NTLM version 2 protocols. LAN Manager is considered the weakest protocol and NTLM version 2 is the strongest. You can support one or more protocols, but must ensure that:

a. Regardless of the version of NTLM that you use, you must configure the LAN Manager Authentication level settings. In the applicable Windows security policy editor, choose **Local Policies > Security Options**; locate the **LAN Manager Authentication Level policy**; and set the policy. For example, if you are using LM or NTLM version 1, set it to **Send LM & NTLM responses**. For information on the various options and NTLM version 2 settings, see the appropriate NTLM authentication-level documentation on the Microsoft website.

b. In addition to the previous setting, if you want to use NTLM version 2, you must also ensure that:

   – *Each* Windows 2000 domain controller involved in user authentication has the Windows 2000 Service Pack 2 or the Microsoft hot fix KB893318 found on the Microsoft website.

     or

   – *Each* domain controller involved in user authentication has the Windows 2003 Service Pack 1. This version does not require any patch.

Step 4 Create a user account.

Tip If you have upgraded or reinstalled the remote agent and you created a user account for the previous installation, complete this step only if you want to use a different user account to run the remote agent service.

In the domain of the domain controller that is running the remote agent, you must have a domain user account that you can use to run the remote agent service (as explained in subsequent steps in this procedure).

a. Create a domain user account. Use this user account to run the remote agent service. The user account does not require any particular group membership in the domain.

Tip Give the user account an easily recognizable name, such as *ACSuser*. If you enable audit policies, Event Viewer entries with this username will make it easier to diagnose permissions problems that are related to failed ACS authentication attempts.

b. To the user account that you create, grant **Read all properties** permission for all Active Directory folders containing users that ACS must be able to authenticate. To grant permission for Active Directory folders, access Active Directory from the Microsoft Management Console and configure the security properties for the folders that contain users whom ACS will authenticate.

Tip You can access the security properties of an Active Directory folder of users by right-clicking the folder, selecting **Properties**, and choosing the Security tab. Click **Add** to include the username.

For more information, see Windows 2000 Server Active Directory.

Step 5 Configure Local Security policies.

Note This step is required only if ACS authenticates users who belong to trusted domains or child domains.

Tip If you have upgraded or reinstalled the remote agent and you completed this step for the previous installation, it is required only if you want to use a different user account to run the remote agent service.

For the user account that you created in the preceding step, add the user to the following local security policies:

- Act as part of the operating system.
- Log on as a service.

For more information, see Configuring Local Security Policies, page 2-13.

Step 6 Configure services.

Note This step is required only if ACS authenticates users who belong to trusted domains or child domains.

Configure the remote agent service to run as the user that you added to the security policies in the preceding step.

For more information, see Configuring the Remote Agent Service, page 2-15.

Step 7 Enable NetBIOS.

ACS requires NetBIOS for communications with domain controllers of trusted or child domains. Therefore, you must enable NetBIOS on the:

- Domain controller that is running the remote agent.
- Trusted domain controllers for domains containing users that ACS must authenticate.
- Domain controllers for child domains containing users whom ACS must authenticate.

To enable NetBIOS:

a. Access the advanced TCP/IP properties of the network connections on each domain controller.

b. Click the **WINS** tab.

c. Configure NetBIOS as applicable.

For more information, see the appropriate Microsoft documentation.

Step 8 Ensure DNS operation.

Especially for authentication of users in Active Directory, the remote agent needs DNS to operate correctly on your network. Other ACS features might also use DNS, such as RADIUS-based token server authentication or an ACS Service Management event notification e-mail. If you configure such features by using hostnames, rather than IP addresses, and DNS does not operate correctly, those features might fail, as would authentication requests that are sent to Active Directory.

For more information, see the Microsoft documentation for your operating system.

Step 9 Specify DNS suffixes.

Note This step is required only if ACS authenticates users with the Active Directory of more than one domain.

On the domain controller that is running the remote agent, configure the network connection that the remote agent uses so that the network connection lists each trusted and child domain as a DNS suffix:

a. Access the advanced TCP/IP properties of the network connection.

b. Choose the DNS tab.

c. Configure the **Append these DNS suffixes** list, as applicable.

For more information, see:

- Microsoft.com: Configure TCP/IP to use DNS (Windows 2000).
- Microsoft.com: Configure TCP/IP to use DNS (Windows 2003).

Step 10 Configure WINS.

You must enable WINS on your network if ACS must authenticate users belonging to a trusted or child domain, and if the remote agent cannot rely on DNS to contact the domain controllers in those domains.

For more information, see the Microsoft documentation for your operating system.

Step 11 Configure *LMHOSTS* file.

Note Only perform this step if, after performing the preceding steps, Windows authentication and group mapping for users who belong to trusted domains or child domains are unreliable.

As a final means of ensuring communication with other domain controllers, on the domain controller that is running ACS, configure a *LMHOSTS* file to include entries for each domain controller of a trusted or child domain containing users whom ACS must authenticate.

Tip The format of an *LMHOSTS* file is very particular. You must understand the requirements of configuring the *LMHOSTS* file.

For more information, see the appropriate Microsoft documentation.

The example *LMHOSTS* file is included with the Windows operating system. The default location and filename for the sample file is *<systemroot>\system32\drivers\etc\lmhosts.sam.*

Configuring for Member Server Authentication

When the remote agent runs on a member server and you must authenticate users with a Windows user database, the additional configuration that is required varies, depending on your Windows networking configuration. Most of the following steps are always applicable when the remote agent runs on a member server; other steps are required only in certain conditions, as noted at the beginning of the step. Perform only those steps that always apply and that apply to your Windows networking configuration.

Complete these steps to configure member server authentication:

Step 1 Verify domain membership.

One common configuration error that prevents Windows authentication is the erroneous assignment of the member server to a workgroup with the same name as the Windows domain that you want to use to authenticate users. While this error might seem obvious, ensure that you verify that the computer running the remote agent is a member server of the correct domain.

Tip To determine domain membership of a computer, on the Windows desktop, choose **My Computer > Properties > Network Identification**, and read the information on that tab.

If the computer that is running the remote agent is not a member of the domain that your deployment plans require, correct this situation before continuing the procedure.

For more information, see the Microsoft documentation for your operating system.

Step 2 Add the *CISCO* workstation.

To satisfy Windows requirements for authentication requests, ACS must specify the Windows workstation in to which the user is attempting to log. Because ACS cannot determine this information from authentication requests that AAA clients send, it uses a generic workstation name for all requests. Use *CISCO* as the name of the workstation.

In the local domain, and in each trusted domain and child domain that ACS will use to authenticate users, ensure that:

- A computer account named *CISCO* exists.
- All users that Windows will authenticate have permission to log in to the computer named *CISCO*.

For more information, see the Microsoft documentation for your operating system.

Step 3 Verify the server service status.

The ACS authentication service depends on the server service, which is a standard service in Microsoft Windows. On the computer that is running the remote agent, verify that the server service is running and that its Startup Type is set to ***Automatic***.

Tip To configure the Server service, use the local administrator account to log in to the computer that is running ACS and choose **Start > Programs Administrative Tools > Services**. The services appear alphabetically.

For more information, see the Microsoft documentation for your operating system.

Step 4 Verify the NTLM version.

Note This step is required only if ACS authenticates users who belong to trusted domains or child domains. No changes are required on ACS, only Windows.

ACS supports authentication of Windows credentials by using LAN Manager (LM), NTLM version 1, or NTLM version 2 protocols. LAN Manager is considered the weakest protocol and NTLM version 2 is the strongest. You can support one or more protocols, but must ensure that:

a. Regardless of the version of NTLM that you use, you must configure the LAN Manager Authentication level settings. In the applicable Windows security policy editor, choose **Local Policies > Security Options**; locate the **LAN Manager Authentication Level policy**; and set the policy. For example, if you are using LM or NTLM version 1, set it to **Send LM & NTLM responses**. For information on the various options and NTLM version 2 settings, see the appropriate NTLM authentication-level documentation on the Microsoft website.

b. In addition to the setting in step a, if you use NTLM version 2 you must also ensure that:

   – *Each* Windows 2000 domain controller involved in user authentication has the Windows 2000 Service Pack 2 or the Microsoft hot fix KB893318 found on the Microsoft website.

or

– *Each* domain controller involved in user authentication has Windows 2003 Service Pack 1. This version does not require any patch.

Step 5 Create a user account.

Tip If you have upgraded or reinstalled the remote agent and you completed this item previously, this step is required only if you want to use a different user account to run the remote agent service.

The domain of the domain controller that is running the remote agent must contain a domain user account that you can use to run the remote agent service (as explained in subsequent steps of this procedure).

a. Create a domain user account. Use this user account to run the remote agent service. The user account does not require any particular group membership in the domain.

Tip Give the user account an easily recognizable name, such as *ACSuser*. If you enable audit policies, Event Viewer entries with this username will make it easier to diagnose permissions problems with failed ACS authentication attempts.

b. To the user account that you create, grant **Read all properties** permission for all Active Directory folders containing users that ACS must be able to authenticate. To grant permission for Active Directory folders, access Active Directory by using the Microsoft Management Console and configure the security properties for the folders that contain users whom ACS will authenticate.

Tip You can access the security properties of an Active Directory folder of users by right-clicking the folder, and selecting **Properties > Security**. Click **Add** to include the username.

For more information, see Windows 2000 Server Active Directory.

Step 6 Configure local security policies.

To the user account that you created in the preceding step, add the user to the following local security policies:

- Act as part of the operating system.
- Log on as a service.

For more information, see Configuring Local Security Policies, page 2-13.

Step 7 Configure services.

Configure the remote agent service to run as the user that you added to the security policies in the preceding step.

For more information, see Configuring the Remote Agent Service, page 2-15.

Step 8 Enable NetBIOS.

ACS requires NetBIOS for communications with all domain controllers to which it submits user authentication requests. Therefore, you must enable NetBIOS on the:

- Member server that is running the remote agent computer.
- Domain controller of the domain containing ACS.
- Domain controllers of trusted domains containing users that ACS must authenticate.

- Domain controllers of child domains containing users whom ACS must authenticate.

To enable NetBIOS:

- Access the advanced TCP/IP properties of the network connections on each domain controller.
- Click the **WINS** tab.
- Configure NetBIOS as applicable.

For more information, see the appropriate Microsoft documentation.

Step 9 Ensure DNS operation.

Especially for authentication of users in Active Directory, the remote agent requires DNS to operate correctly on your network. Other ACS features might also use DNS, such as RADIUS-based token server authentication or an ACS Service Management event-notification e-mail. If you configure such features by using hostnames, rather than IP addresses, and DNS does not operate correctly, those features might fail, as would authentication requests that are sent to Active Directory.

For more information, see the Microsoft documentation for your operating system.

Step 10 Specify DNS suffixes.

Note This step is required only if ACS authenticates users with the Active Directory of more than one domain.

On the member server that is running the remote agent, configure the network connection that the remote agent uses so that the network connection lists each domain as a DNS suffix:

a. Access the advanced TCP/IP properties of the network connection.

b. Choose the DNS tab.

c. Configure the Append these DNS suffixes list, as applicable.

For more information, see the appropriate Microsoft documentation.

Step 11 Configure WINS.

If ACS must authenticate users belonging to a trusted or child domain, and if the remote agent cannot rely on DNS to contact the domain controllers in those domains, you must enable WINS on your network.

For more information, see the Microsoft documentation for your operating system.

Step 12 Configure *LMHOSTS* file.

Note Only perform this step if, after performing the preceding steps, Windows authentication and group mapping are unreliable.

As a final means of ensuring communication with domain controllers, on the member server that is running the remote agent, configure a *LMHOSTS* file to include entries for each domain controller containing users that ACS must authenticate. You should also include domain controllers of child domains.

Tip The format of an *LMHOSTS* file is very specific. Ensure that you understand the requirements of configuring the *LMHOSTS* file.

For more information, see the appropriate Microsoft documentation.

The example *LMHOSTS* file is included with the Windows operating system. The default location and filename for the sample file is *<systemroot>\system32\drivers\etc\lmhosts.sam.*

Configuring Local Security Policies

Before You Begin

This procedure is required only if one of the following conditions is true. The remote agent runs on a:

- Member server and must authenticate users with a Windows user database.
- Domain controller and must authenticate users in trusted domains or child domains.

You should have already created a user account that you intend to use to run the remote agent. For full configuration requirements, see the applicable procedure: Configuring for Member Server Authentication, page 2-9, or Configuring for Domain Controller Authentication, page 2-6.

To configure local security policies:

Step 1 By using the local administrator account, log in to the computer that is running ACS.

Step 2 Choose **Start > Settings > Control Panel > Administrative Tools > Local Security Policy**.

Tip If Control Panel is not expanded on the Start menu, choose **Start > Settings > Control Panel**. Double-click **Administrative Tools.** and then double-click **Local Security Policy**.

The Local Security Settings window appears.

Step 3 In the Name column, double-click **Local Policies**, and then double-click **User Rights Assignment**.

The Local Security Settings window displays a list of policies with associated settings. You must configure these two policies:

- Act as part of the operating system.
- Log on as a service.

Step 4 For the **Act as part of the operating system** policy and **Log on as a service** policy:

a. Double-click the policy name.

The Local Policy Setting dialog box appears.

b. Click **Add.**

The Select Users or Groups dialog box appears.

c. In the box below the **Add** button, type the username for the user account.

Note The username *must* be in domain-qualified format. For example, if you created a user named *ACSuser* in the *CORPORATE* domain, type *CORPORATE\ACSuser.*

d. Click **Check Names**.

The Enter Network Password dialog box appears.

e. Complete:

- **Connect as**—Type a domain-qualified username. The username must exist in the domain specified in c. For example, if the domain specified is *CORPORATE* and *echamberlain* is a valid user in that domain, type *CORPORATE\echamberlain*.
- **Password**—Type the password for the user account that you specified. Click **OK**.

Windows verifies the existence of the username in c. The Enter Network Password dialog box closes.

f. In the **Select Users or Groups** dialog box, click **OK**.

The Select Users or Groups dialog box closes.

Windows adds the username to the Assign To list in the Local Policy Setting dialog box.

g. Click **OK**.

The Local Policy Setting dialog box closes. The domain-qualified username specified in c. appears in the settings associated with the policy that you configured.

h. Verify that the username that is specified in c. appears in the Local Setting column for the policy that you modified. If it does not, repeat these steps.

Tip To see the username that you added, you might have to widen the Local Setting column.

Note The Effective Setting column does not dynamically update. This procedure includes subsequent verification steps for ensuring that the Effective Setting column contains the required information.

After you have configured the Act as part of the operating system policy and the Log on as a service policy, the user account appears in the Local Setting column for the policy that you configured.

Step 5 Verify that the security policy settings that you changed are in effect on the computer that is running ACS:

a. Close the Local Security Settings window.

To refresh the information in the Effective Setting column, close the window.

b. Open the Local Security Settings window again. Choose **Start > Programs > Administrative Tools > Local Security Policy**.

c. In the Name column, double-click **Local Policies** and double-click **User Rights Assignment**.

The Local Security Settings window displays an updated list of policies with their associated settings.

d. For the **Act as part of the operating system** policy and again for the **Log on as a service** policy, verify that the username that you added to the policy appears in the Effective Setting column.

Note If the username that you configured the policies to include does not appear in the Effective Setting column for both policies, the security policy settings on the domain controller might conflict with the local setting. Resolve the conflict by configuring security policies on the domain controller to allow the local settings to be the effective settings for these two policies. For more information about configuring security policies on the domain controller, see the Microsoft documentation for your operating system.

The user account has the required privileges to run the remote agent service and support Windows authentication.

Step 6 Close the Local Security Settings window.

The specified user account has the permissions necessary to run the remote agent service successfully.

Configuring the Remote Agent Service

Before You Begin

This procedure is required only if one of the following conditions is true. the remote agent runs on a:

- Member server and must authenticate users with a Windows user database.
- Domain controller and must authenticate users in trusted domains or child domains.

You should have already created a user account that you intend to use to run the remote agent and assigned it the permissions necessary to run the remote agent service. For full configuration requirements, see the applicable procedure: Configuring for Member Server Authentication, page 2-9, or Configuring for Domain Controller Authentication, page 2-6.

To configure ACS services:

Step 1 Using the local administrator account, log in to the computer that is running the remote agent.

Step 2 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Tip If the Control Panel is not expanded on the Start menu, choose **Start > Settings > Control Panel**. Double-click **Administrative Tools** and then double-click **Services**.

The Services window displays a list of service groups and a list of all registered services for the current group. The list of service groups is labeled *Tree*. The registered services for the current group appear in the list to the right of the Tree list.

Step 3 In the Tree list, click **Services (local)**.

The Windows service installed to support the remote agent appears in the lists of services as CiscoSecure ACS Agent. The service name is CSAgent.

Step 4 For the remote agent service:

a. In the list of services, right-click the CiscoSecure ACS Agent service and, from the shortcut menu, choose **Properties**.

The Computer Browser Properties (Local Computer) dialog box appears.

b. Choose the **Log On** tab.

c. Select the **This account** option.

d. In the box next to the **This account** option, type the username for the account.

Note The username *must* be in domain-qualified format. For example, if you created a user named *ACSuser* in the *CORPORATE* domain, type *CORPORATE\ACSuser*.

e. In the **Password** box and in the **Confirm Password** box, type and retype the password for the user account.

f. Click **OK**.

The CSAgent service is configured to run by using the privileges of the user account.

Step 5 To restart the CSAgent service:

a. On the Computer Browser Properties (Local Computer) dialog box, select the **General** tab.

b. Click **Stop**.

The Service Control dialog box appears while the service is stopping.

c. Click **Start**.

The Service Control dialog box appears while the service is starting.

The remote agent service runs by using the privileges of the user account specified.

CHAPTER 3

Installing Cisco Secure ACS Remote Agent for Solaris

This chapter provides information about installing Cisco Secure Access Control Server (ACS) Remote Agent for Solaris.

This chapter contains:

- System Requirements, page 3-1
- Network Requirements, page 3-2
- Installing a Remote Agent for Solaris, page 3-2
- Uninstalling ACS Remote Agent for Solaris, page 3-5
- Upgrading ACS Remote Agent for Solaris, page 3-6

System Requirements

The computer running ACS Remote Agent for Solaris must meet the minimum requirements detailed in the following sections:

- ACS Requirements, page 3-1
- Hardware Requirements, page 3-1
- Operating System Requirements, page 3-2
- Environment Variable Settings, page 3-2

ACS Requirements

You must use ACS Remote Agent for Solaris, version 4.1, with ACS Solution Engine (ACS SE), version 4.1. Other releases of ACS are not supported.

Hardware Requirements

The computer running ACS Remote Agent for Solaris must meet these requirements:

- SPARC architecture
- 256 MB of RAM

- 250 MB of free disk space

For the most recent information about tested hardware, see the *Release Notes for Cisco Secure ACS Solution Engine*. The current version of the release notes are posted on Cisco.com.

Operating System Requirements

The computer running ACS Remote Agent for Solaris must use Solaris 2.8 or Solaris 2.9.

For the most recent information about tested operating systems, see the *Release Notes for Cisco Secure ACS Solution Engine*. The current version of the release notes are posted on Cisco.com.

Environment Variable Settings

The environment variable LD_LIBRARY_PATH must be set with the path for the file *libstdc++.so**.

Example:

If *libstdc++.so* is in directory */router/lib*, then root must have the following settings in the .profile:

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/router/lib
export LD_LIBRARY_PATH
```

Network Requirements

Before you install ACS Remote Agent, ensure that:

- The computer running ACS Remote Agent for Solaris can ping the ACS Solution Engines that it is to support.
- The gateway devices permit traffic between the computer running ACS Remote Agent for Windows and the ACS SE. Specifically, the remote agent must receive TCP communication on TCP ports you configure in *CSAgent.ini*. The default TCP ports, if all services are used, are 2004, 2006, and 2007. The appliance must receive TCP communication on TCP port 2003.

Note By using the *CSAgent.ini* file, you can configure the ports that the remote agent uses to communicate with ACS. If you change the ports used, configure intervening gateway devices to permit TCP traffic on the ports that you configure the remote agent to use. For more information about changing the ports that a remote agent uses, see Configuring a Remote Agent, page 4-1.

Installing a Remote Agent for Solaris

Before You Begin

Determine the IP address of the ACS Solution Engine that will be the configuration provider for this remote agent. For more information about configuration providers, see Configuration Provider, page 1-2.

For information about what must be completed before installing ACS Remote Agent for Solaris, see System Requirements, page 3-1.

If a previous version of ACS Remote Agent for Solaris is installed on the machine, you must uninstall it before you install ACS Remote Agent for Solaris 4.1. See Upgrading ACS Remote Agent for Solaris, page 3-6.

To install ACS Remote Agent for Solaris:

Step 1 On the ACS Software Migration CD, find the installation file for ACS Remote Agent for Solaris. The file name is typically `CSCOacsag.`*version*`.`*platform*`.tar`.

Note You can also download the installation file from Cisco.com. Log in to Cisco.com, choose **Technical Support > Downloads**, and then locate the software download page for ACS Solution Engine. Remote agent software is located on the Strong Cryptographic 3DES Software page for ACS Solution Engine software.

Step 2 Place the Solaris remote agent file in a location accessible from the Solaris server on which you want to install the remote agent.

Step 3 On the Solaris server on which you want to install the Solaris remote agent, log in as root.

Note If you cannot access the server as root, log in to the server as any user that has permission to use the **sudo** command.

Step 4 Access a shell command prompt and change directories to the directory in which you saved the downloaded Solaris remote agent file.

Step 5 Copy the remote agent installation package to the */tmp* directory. For example, type:

`cp CSCOacsag.`*version*`.`***platform*`.tar /tmp`**

where *version* is the version of the remote agent and *platform* is the platform identifier string.

Step 6 Change directories to the `/tmp directory`. Type:

```
cd /tmp
```

Press **Enter**.

Step 7 Unpack the remote agent software package. Type:

`tar xf CSCOacsag.`*version*`.`***platform*`.tar`**

Press **Enter**.

Step 8 Install the remote agent software package. Type:

```
pkgadd -d . CSCOacsag
```

Press **Enter**.

Tip If you are not logged in as root, use the **sudo** command, for example, **sudo pkgadd -d . CSCOacsag**.

The software installation begins. The `Enter Appliance name/IP:` prompt appears. The appliance referred to is the configuration provider for the remote agent.

Step 9 Type the hostname or IP address of the ACS Solution Engine that is the configuration provider for this remote agent. Press **Enter**.

Note If you type a hostname, be sure that DNS is operating correctly or that the appliance hostname is in the local hosts file.

Tip You can edit the IP address or hostname of the configuration provider after completing the installation. For more information, see Configuring a Remote Agent, page 4-1.

The installation script verifies the IP address or hostname specified, records the validated information in the CSAgent.ini file, and continues the installation. The following message and prompt appear:

```
Do you like to use CSUnix output format? [n] [y,n,?]
```

Step 10 Do one of the following, depending on what format you want to use:

- For the CSUnix log format, type **Y**, and press **Enter**.
- For the CSV log format, type **N**, and press **Enter**.

For more information about CSUnix log format, see the discussion of the CSUnixOutput option in CSAgent.ini Settings, page 4-2.

Tip You can edit the setting for the CSUnixOutput option after completing the installation. For more information, see Configuring a Remote Agent, page 4-1.

The installation script records your log format selection in the *CSAgent.ini* file and continues the installation. The following message and prompt appear:

```
This package contains scripts which will be executed with super-user permission during the
process of installing this package.

Do you want to continue with the installation of <CSCOacsag> [y,n,?]
```

Step 11 To continue with the installation, type **Y**, and press **Enter**.

Note If you type **N**, the installation exits and the remote agent software is not installed.

The Solaris remote agent software is installed on the Solaris server.

Where to go next

- If you want to configure the remote agent, see Configuring a Remote Agent, page 4-1.

Note The installation provides a default configuration, including specifying the configuration provider; however, you may want to configure the ports on which the remote agent communicates with the configuration provider and with other ACS Solution Engines.

- To start remote agent services, see Stopping and Starting Remote Agent Services, page 4-7.

Uninstalling ACS Remote Agent for Solaris

Note If you do not intend to reinstall ACS Remote Agent for Solaris on this computer, remove the applicable remote agent configurations from all ACS Solution Engines.

Before You Begin

Note Uninstalling a Solaris remote agent requires root privileges or permission to use the **sudo** command.

To uninstall ACS Remote Agent for Solaris:

Step 1 On the Solaris server running the remote agent, log in as root.

Note If you cannot access the server as root, log in to the server as any user that has permission to use the **sudo** command.

Step 2 Access a shell command prompt.

Step 3 Type:

```
pkgrm CSCOacsag
```

Press **Enter**.

Tip If you are not logged in as root, use the **sudo** command, for example, **sudo pkgrm CSCOacsag**.

The following prompt appears:

```
Do you want to remove this package?
```

Step 4 Type **Y**, and press **Enter**.

The following prompt appears:

```
This package contains scripts which will be executed
with super-user permission during the process of removing
this package.

Do you want to continue with the removal of this package
[y,n,?,q] ?
```

Step 5 Type **Y**, and press **Enter**.

The Solaris remote agent software is removed from the Solaris server.

Upgrading ACS Remote Agent for Solaris

The upgrade process entails uninstalling the old version of the remote agent and installing the new version.

To upgrade ACS Remote Agent for Solaris:

Step 1 Remove the old version of the remote agent by performing the steps in Uninstalling ACS Remote Agent for Solaris, page 3-5.

Step 2 Using the version of ACS Remote Agent for Solaris to which you want to upgrade, perform the steps in Installing a Remote Agent for Solaris, page 3-2.

CHAPTER 4

Configuring and Maintaining a Remote Agent

This chapter provides information about configuring and maintaining a Cisco Secure Access Control Server (ACS) Remote Agent, for Windows or Solaris.

This chapter contains:

- Configuring a Remote Agent, page 4-1
- Maintaining a Remote Agent, page 4-7

Configuring a Remote Agent

You do all manual configuration of ACS Remote Agent by configuring the *CSAgent.ini* file. This section describes how to configure ACS Remote Agent by using the *CSAgent.ini* file.

This section contains:

- CSAgent.ini Location, page 4-1
- CSAgent.ini Settings, page 4-2
- Sample CSAgent.ini, page 4-5
- Changing CSAgent.ini Settings, page 4-6

CSAgent.ini Location

When you install ACS Remote Agent for Windows in the default location, *CSAgent.ini* is located in the directory *C:\Program Files\Cisco\CiscoSecure ACS Agent*

When you install ACS Remote Agent for Solaris, *CSAgent.ini* is located in the directory */opt/CSCOacsag*

Regardless of where you install the remote agent, *CSAgent.ini* is located in the highest directory of the remote agent installation.

For more information about the directory structure created when you install a remote agent, see File and Directory Structure, page 4-8.

CSAgent.ini Settings

You do all manual configuration of ACS Remote Agent by configuring the *CSAgent.ini* file. This topic discusses the settings possible in *CSAgent.ini*.

CSAgent.ini has one section for each service that the remote agent provides, one each for CSAgent and CSLogAgent. If you are using ACS Remote Agent for Windows, *CSAgent.ini* also contains a section for CSWinAgent. Each section of *CSAgent.ini* has several options for configuring the applicable service. All options have the format:

OptionName=Value

where *OptionName* is the name of the option and *Value* is the setting for that option. For options that accept multiple values, separate the values with commas (,).

OptionName=Value1,. . .,ValueN

To disable optiona setting, use a semicolon (;) at the beginning of the line. For example, the PermittedClients option is not mandatory and is disabled by default.

```
; PermittedClients=192.168.1.*,10.49.*.*
```

The following list describes each option. For an example of a *CSAgent.ini* file, see Sample CSAgent.ini, page 4-5.

- **CSAgent section**—You can configure the following options for the CSAgent service:
  - **Port**—The TCP port on which the CSAgent service listens. The default value is 2004. An ACS Solution Engine (ACS SE) using the remote agent first contacts the agent on this port.

    Note The port number provided here must match the port number specified in ACS when you configure it to communicate with the remote agent.

  - **ConfigProviderHost**—The IP address or the hostname of the ACS SE that is the configuration provider for the remote agent. The default value is the IP address or hostname specified during the installation process. If you specify a hostname, ensure that DNS is functioning correctly on your network or that the computer running the remote agent has a hosts file entry for the ACS SE.
  - **ConfigProviderPort**—The TCP port of the ACS SE that is the configuration provider for the remote agent. The appliance listens to this port for communications from the remote agent. The default is 2003.

    Note It is highly unlikely that you will need to change the ConfigProviderPort value from the default of 2003. The port that an appliance listens to is not configurable.

  - **Agents**—The agent services that CSAgent should enable. The default setting is determined at installation, when you specify which services should be active.

    If you are using ACS Remote Agent for Solaris, the only valid service is CSLogAgent.

    If you are using ACS Remote Agent for Windows, the two valid services are CSLogAgent and CSWinAgent. You can enable either service, or both services. If you enable both services, the order in which you list them is irrelevant.

- **PermittedClients**—A comma-separated list of IP addresses from which CSAgent will accept requests. This setting is disabled by default. If you enable this option, the remote agent provides services only to appliances whose IP addresses are included in the list of IP addresses.

  Note The restrictions that the CSAgent PermittedClients value imposes override restrictions that the CSLog Agent or CSWinAgent PermittedClients values impose. ACS SEs with IP addresses not included in the PermittedClients value in the CSAgent section are always denied remote agent services, even if you have included the IP addresses in the PermittedClients values of the CSLogAgent or CSWinAgent sections.

  In each IP address that you specify, you have three options for each octet in the address:

- **Number**—You can specify a number, for example, 10.3.157.98.
- **Numeric Range**—You can specify the low and high numbers of the range in the octet, separated by a hyphen (-), for example, 10.3.157.10-50.
- **Wildcard**—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

  As a further example, the PermittedClients value can use these options in each IP address in its list:

  ```
  PermittedClients=10.3.157.10-50,10.3.157.52,10.3.158.*
  ```

- **CSLogAgent section**—You can configure the following options for the CSLogAgent service.
  - **Executable**—The directory path and executable file name for the CSLogAgent service. This option is intended primarily for support use. The path can be relative to the directory containing *CSAgent.exe*. For information about the directory containing *CSAgent.exe*, see File and Directory Structure, page 4-8.
  - **Port**—The TCP port that CSLogAgent listens to for ACS SE messages, other than accounting records. The default value is 2006.
  - **AccountingPort**—The TCP port that CSLogAgent listens to for accounting records from ACS SEs. The default value is 2007.
  - **PermittedClients**—A comma-separated list of IP addresses that CSLogAgent will accept requests from. This setting is disabled by default, which has the effect of a PermittedClients value of `*.*.*.*`. If you enable this option, the remote agent provides logging services only to appliances whose IP addresses are included in the list of IP addresses. If you also enable the PermittedClients value in the CSAgent section, the CSLogAgent PermittedClients value provides a means to restrict the remote agent logging service to a subset of the IP addresses specified in the CSAgent PermittedClients value.

    Note You cannot use the CSLogAgent PermittedClients value to permit an IP address that the CSAgent PermittedClients value does not permit.

    In each IP address you specify, you have three options for each octet in the address:

  - **Number**—You can specify a number, for example, 10.3.157.98.
  - **Numeric Range**—You can specify the low and high numbers of the range in the octet, separated by a hyphen (-), for example, 10.3.157.10-50.
  - **Wildcard**—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

- **CSUnixOutput**—Whether CSLogAgent records logs in comma-separated value (CSV) format or in the format that ACS Remote Agent for Solaris uses.

  Note The CSUnixOutput option is applicable only to ACS Remote Agent for Solaris. The CSUnixOutput option does not exist in the *CSAgent.ini* file of a Windows remote agent.

  The only valid values for this option are:

  – **0**—Zero (0) specifies that the remote agent records logs in CSV format and that log filenames end with *.csv*. In CSV format, each record in the log is written on a single line, with commas (,) that separate values into columns. The names of the columns appear at the top of each column. An abbreviated example of the first two lines of a CSV log is:

  ```
  Date,Time,User-Name,Acct-Status-Type
  11/26/2003,10:48:36,jwiedman,Start
  ```

  – **1**—One (1) specifies that the remote agent records logs in CSUnix format and that log filenames end with *.log*. In CSUnix log format, each record in the log is written on multiple lines, beginning with the date and time. After the date, each line of a record includes the name of the attribute recorded, an equal sign (=), and the attribute value. Records are separated by two blank lines. An abbreviated example of a single record in CSUnix format is:

  ```
  Tue Nov 26 10:48:36 2003
     User-Name = "jwiedman"
     Acct-Status-Type = Start
  ```

- **CSWinAgent section**—You can configure the following options for the CSWinAgent service:

  Note CSWinAgent is applicable only to ACS Remote Agent for Windows. The CSWinAgent section does not exist in the *CSAgent.ini* file of a Solaris remote agent.

  – **Executable**—The directory path and executable file name for the CSWinAgent service. This option is intended primarily for support use. The path can be relative to the directory containing *CSAgent.exe*. For information about the directory containing *CSAgent.exe*, see File and Directory Structure, page 4-8.

  – **Port**—The TCP port that CSWinAgent listens to for ACS SE messages. The default value is 2005.

  – **PermittedClients**—A comma-separated list of IP addresses that CSWinAgent will accept requests from. This setting is disabled by default, which has the effect of a PermittedClients value of `*.*.*.*`. If you enable this option, the remote agent provides Windows authentication services only to appliances whose IP addresses are included in the list of IP addresses. If you also enable the PermittedClients value in the CSAgent section, the CSWinAgent PermittedClients value provides a means to restrict the remote agent Windows authentication service to a subset of the IP addresses specified in the CSAgent PermittedClients value.

  Note You cannot use the CSWinAgent PermittedClients value to permit an IP address that the CSAgent PermittedClients value does not permit.

  In each IP address that you specify, you have three options for each octet in the address:

  – **Number**—You can specify a number, for example, 10.3.157.98.

- **Numeric Range**—You can specify the low and high numbers of the range in the octet, separated by a hyphen (-), for example, 10.3.157.10-50.
- **Wildcard**—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

The PermittedClients value can use these options in each IP address in its list, for example:

```
PermittedClients=10.3.157.10-50,10.3.157.52,10.3.158.*
```

Sample CSAgent.ini

The following sample *CSAgent.ini* file combines all options for Windows and Solaris remote agents. With the exception of the CSWinAgent section, this example file is valid for a Solaris remote agent. With the exception of the CSUnixOutput option, this example file is valid for a Windows remote agent.

Settings for your *CSAgent.ini* file will differ. For information about each setting in the *CSAgent.ini* file, see CSAgent.ini Settings, page 4-2.

```
[CSAgent]

; This is the main service's configuration section...
; To change the local port:
; Port=2004

; To set the config provider hostname/IP address:
; ConfigProviderHost=servername
; or
; ConfigProviderHost=127.0.0.1
ConfigProviderHost=192.168.1.102

; To set the config provider port:
ConfigProviderPort=2003

; To define the list of agents to activate:
;Agents=CSLogAgent,CSWinAgent
Agents=CSWinAgent

; To define a list of permitted clients
; PermittedClients=192.168.1.*,10.49.*.*

[CSLogAgent]

; This is the log agent's configuration section...
; Name of the agent's executable:
Executable=..\CSLogAgent\CSLogAgent.exe

; To change the local port:
Port=2006

; To change the accounting port:
AccountingPort=2007

; PermittedClients=192.168.1.*,10.49.*.*

; Use CSUnix output format
; possible values: 0 - csv, 1 - CSUnix format
; default is no (0)
; This option doesn't exist in a Windows remote agent CSAgent.ini file
CSUnixOutput=1

[CSWinAgent]
```

```
; This is the Windows agent's configuration section...
; This section doesn't exist in a Solaris remote agent CSAgent.ini file
; Name of the agent's executable:
Executable=..\CSWinAgent\CSWinAgent.exe

; To change the local port:
Port=2005

; PermittedClients=192.168.1.*,10.49.*.*
```

Changing CSAgent.ini Settings

You configure ACS Remote Agent by specifying settings in its *CSAgent.ini* file. Some default settings are determined at installation while others are preset by Cisco. You can change any of the settings in the *CSAgent.ini* file using this procedure.

Before You Begin

If you are using remote agents in a production environment, consider making changes when use of remote agent services is low. Putting changes to *CSAgent.ini* into effect requires restarting the CSAgent service. While CSAgent is restarting, no remote agent services are available.

To change *CSAgent.ini* settings:

Step 1 By using an ASCII text editor, open the *CSAgent.ini* file for the remote agent you want to configure.

Tip If you chose the default installation directory, the *CSAgent.ini* file for a Windows remote agent is located at *C:\Program Files\Cisco\CiscoSecure ACS Agent*. For a Solaris remote agent, the *CSAgent.ini* file is located at */opt/CSCOacsag*.

Step 2 Change the settings that you want to modify. For more information about settings and their significance, see CSAgent.ini Settings, page 4-2.

Note Editing *CSAgent.ini* for the Solaris remote agent requires root access. If you cannot access the computer running the remote agent as root, use the **sudo** command, for example, **sudo vi CSAgent.ini**.

Step 3 Save your changes. If you have no further changes to make, close the *CSAgent.ini* file.

Step 4 Restart the CSAgent service. If you do not restart CSAgent, the agent does not implement the changes. For detailed steps, see Stopping and Starting Remote Agent Services, page 4-7.

Note Restarting the CSAgent service briefly interrupts all services that the remote agent provides. Consider performing this step when use of remote agent services is low.

During startup, the remote agent notifies its configuration provider of its configuration, including changes to *CSAgent.ini* that are relevant to the configuration provider. After startup is complete, remote agent services are available.

Maintaining a Remote Agent

This section provides information about maintaining and debugging a remote agent.

This section contains:

- Stopping and Starting Remote Agent Services, page 4-7
- File and Directory Structure, page 4-8
- Retrieving Support Logs, page 4-9
- Running CSAgent in Debug Mode, page 4-9
- Sample CSAgent Debug Output, page 4-11

Stopping and Starting Remote Agent Services

CSAgent controls the CSLogAgent and CSWinAgent applications. To stop or start any part of the remote agent, you must stop or start CSAgent.

Before You Begin

While CSAgent is stopped, no remote agent services are available. If you are restarting remote agent services, consider restarting CSAgent when use of remote agent services is low.

To stop or restart Windows remote agent services:

Step 1 Use a user account that has local administrator privileges to log in to the computer running the Windows remote agent.

Step 2 Open an MS DOS command prompt.

Step 3 To stop remote agent services, type:

```
net stop csagent
```

Press **Enter**.

The CSAgent service stops, as do the CSLogAgent and CSWinAgent applications, if they were running. Remote agent services are unavailable to any appliance.

Step 4 To start remote agent services, type:

```
net start csagent
```

Press **Enter**.

The CSAgent service starts. CSAgent also starts the remote agent services that the *CSAgent.ini* specifies. After startup is complete, the applicable remote agent services are available.

To stop or restart Solaris remote agent services:

Step 1 On the computer running the Solaris remote agent, access a shell command prompt as the root user.

Tip If you do not have root access to the computer running the remote agent, use the **sudo** command to execute the commands in the following steps.

Step 2 To stop remote agent processes, type:

```
/etc/init.d/csagent stop
```

Press **Enter**.

Tip You can also use the **kill** command to stop remote agent processes. To list remote agent processes, use the command: `ps -ef | grep "CS[AL]"`

The CSAgent service stops, as does CSLogAgent if it was running. Remote agent services are unavailable to any appliance.

Step 3 To start remote agent processes, type:

```
/etc/init.d/csagent start
```

Press **Enter**.

Tip You can also start the CSAgent process by using this command: `/opt/CSCOacsag/CSAgent/CSAgent &`. The CSAgent process reads the *CSAgent.ini* file and starts the CSLogAgent process if the *.ini* file indicates that the log service is enabled.

The CSAgent service starts. CSAgent also starts the remote agent services that the *CSAgent.ini* specifies. After startup is complete, the applicable remote agent services are available.

File and Directory Structure

When you install ACS Remote Agent for Windows, you select an installation location, the default location being *C:\Program Files\Cisco\CiscoSecure ACS Agent*. When you install ACS Remote Agent for Solaris, the installation location is */opt/CSCOacsag*. Regardless of where you choose to install the remote agent, the files and directories created at that location are the same.

The following list describes those directories and their contents:

- **bin**—Contains all the executable files and required DLL files.
- **CSAgent**—Contains a Logs directory for CSAgent service logging.
- **CSLogAgent**—Contains a Logs directory for CSLogAgent service logging, and a Datafile directory for information from the configuration provider.
- **CSWinAgent**—Contains a Logs directory for CSWinAgent service logging. This directory is only present in installations of the Windows remote agent.
- **Logs**—Contains the following directories for storing accounting and administrative reports from appliances:
  - **AdminAudit**—Contains CSV files for Administrative Audit logs.
  - **Appliance Admin**—Contains CSV files for Appliance Administration Audit logs.
  - **Backup and Restore**—Contains CSV files for ACS Backup and Restore logs.
  - **DBReplicate**—Contains CSV files for Database Replication logs.
  - **DbSync**—Contains CSV files for RDBMS Synchronization logs.

  - **Failed Attempts**—Contains CSV files for Failed Attempts logs.
  - **Passed Authentications**—Contains CSV files for Passed Authentications logs.
  - **RADIUS Accounting**—Contains CSV files for RADIUS Accounting logs.
  - **ServiceMonitoring**—Contains CSV files for ACS Service Monitoring logs.
  - **TACACS+ Accounting**—Contains CSV files for TACACS+ Accounting logs.
  - **TACACS+ Administration**—Contains CSV files for TACACS+ Administration logs.
  - **VoIP Accounting**—Contains CSV files for VoIP Accounting logs.
  - **PasswordLogs**—Contains CSV files for User Password Changes logs.

  The logging files that appear in the directories depend on the logging configuration of the configuration provider.

- **Support**—Contains other files that remote agent services use, particularly CSLogAgent.

Retrieving Support Logs

ACS SE includes a feature called Support, found in the System Configuration section of the HTML Interface. When you select the Run Support Now option on the Support page of an appliance that is configured to use a remote agent for any service, the appliance instructs the remote agent to collect copies of its diagnostic logs. The Windows agent produces a cabinet file containing the log files. The Solaris agent produces a *.tar* file containing the log files.

The remote agent places the resulting support file directly under the Remote Agent installation directory. The file name includes the date and time; previous support files are not overwritten when a new one is created.

To retrieve the support file, on the computer running the remote agent, access the Remote Agent installation directory. For more information about the directory structure under the installation directory, see File and Directory Structure, page 4-8.

Running CSAgent in Debug Mode

CSAgent supports a debug mode that you can use to see error messages as they occur and other normal diagnostic output. The debug mode is helpful if you encounter difficulty running a remote agent; or, if you suspect communication problems between a remote agent and appliances configured to use it, especially its configuration provider.

For examples of debug output, see Sample Debug Output for a Windows Remote Agent, page 4-11.

To run a *Windows* remote agent in debug mode:

Step 1 Use a user account that has local administrator privileges to log in to the computer running the Windows remote agent.

Note When debugging Windows authentication with Active Directory, you may need to log in with a user account that has the **Act as part of the operating system** local security privilege. For more information, see Windows Authentication Configuration, page 2-6.

Step 2 Open an MS DOS command prompt.

Step 3 Change directories to the location of the *CSAgent.exe* file. The *CSAgent.exe* file is located in the CSAgent folder under the installation directory of the remote agent. For more information about the directory structure under the installation directory, see File and Directory Structure, page 4-8.

Step 4 If CSAgent is running, type:

```
net stop csagent
```

Press **Enter**.

The CSAgent service stops. Remote agent services are unavailable to any appliance.

Step 5 Type:

```
csagent.exe -z -p
```

Press **Enter**.

Tip To view the version of *CSAgent.exe*, type `csagent.exe -v` and press **Enter**.

The CSAgent service starts. For each remote agent service enabled in the *CSAgent.ini* file, a console window opens. For example, if CSLogAgent and CSWinAgent are enabled in the *CSAgent.ini* file, two console windows open, one for each service. The console windows show debug output for the applicable service. The command window where you entered the CSAgent command displays debug output from CSAgent. For a sample of debug output, see Sample Debug Output for a Windows Remote Agent, page 4-11.

Step 6 To end the debugging session, press **Enter**.

The debug session ends. All remote agent services stop. The Console window for CSWinAgent or CSLogAgent closes.

For information about restarting the remote agent, see Stopping and Starting Remote Agent Services, page 4-7.

To run a Solaris remote agent in debug mode:

Step 1 On the computer running the Solaris remote agent, access a shell command prompt as the root user.

Tip If you do not have root access to the computer running the remote agent, use the **sudo** command to execute the commands in the following steps.

Step 2 If the remote agent is running, type:

```
/etc/init.d/csagent stop
```

Press **Enter**.

Tip You can also use the **kill** command to stop remote agent processes. To list remote agent processes, use the command: `ps -ef | grep "CS[AL]"`

The CSAgent service stops, as does CSLogAgent if it was running. Remote agent services are unavailable to any appliance.

Step 3 Change directories to the CSAgent directory. Type:

```
cd /opt/CSCOacsag/CSAgent
```

Press **Enter**.

Step 4 Type:

```
CSAgent -z -p
```

Press **Enter**.

Tip To view the version of CSAgent, type `CSAgent -v` and press **Enter**.

The CSAgent service starts. Output is shown in the shell that you used to run the remote agent. For a sample of debug output, see Sample Debug Output for a Windows Remote Agent, page 4-11.

Step 5 To end the debugging session, press **Enter**.

Note If you press Ctrl + C to end the debug session, the CSLogAgent process is not stopped. In this event, use the **ps** command to determine the process ID of CSLogAgent and use the **kill** command to stop it.

The debug session ends. All remote agent processes stop.

For information about restarting the remote agent, see Stopping and Starting Remote Agent Services, page 4-7.

Sample CSAgent Debug Output

This section provides sample output of remote agents run in debug mode. Much of the startup output for remote agents in debug mode reflects the settings made in the *CSAgent.ini* file. Startup output also show various steps in establishing contact with the configuration provider for the remote agent.

This section contains:

- Sample Debug Output for a Windows Remote Agent, page 4-11
- Sample Debug Output for a Solaris Remote Agent, page 4-12

Sample Debug Output for a Windows Remote Agent

This topic shows normal debug output from a Windows remote agent, including CSAgent, CSLogAgent, and CSWinAgent.

The following output is from CSAgent at startup:

```
D:...\CSAgent 33: csagent -p -z
Debug printing on..
Running CSAgent server from command line..
CSAgent server starting ============================
Running as console application.
Will listen on port 2004
Configuration will be fetched from 192.168.12.208:2003
Agents: CSLogAgent,CSWinAgent
```

```
CSLogAgent File: ..\CSLogAgent\CSLogAgent.exe
CSLogAgent Port: 2006
CSWinAgent File: ..\CSWinAgent\CSWinAgent.exe
CSWinAgent Port: 2005
2 agents configured
Permitted CSAgent Clients: 192.168.12.1-127
Hit Return/Enter to stop...

Watchdog activated
Listener activated
CSLogAgent launched
CSWinAgent launched
```

The following normal output is from CSAgent after you press **Enter** to end the debug session:

```
Service stopping
Shutting down EndPoint library
Listener terminating
```

The following output is from CSLogAgent:

```
CSLogAgent server starting ==============================
Running as console application.
Configuration will be fetched from 192.168.12.208:2003
Permitted CSLogAgent Clients: *.*.*.*
Cant get max number of connections maxNumberOfConnections using default 32
Agent library initialisedAgentLib: Attempting to connect to config provider at
192.168.12.208:2003
AgentLib: Connection established, handle 0x7e4af8
AgentLib: GetLogConfig reply received
AgentLib: Disconnecting from config provider, handle 0x7e4af8
Config downloaded
Will listen on port 2007
Will not log to a datafile.
Stream thread N started
Stream N waiting for connection
Will use the Loglib library.
Listening thread started...
```

The following output is from CSWinAgent:

```
CSWinAgent server starting ==============================
Running as console application.
Will listen on port 2005
Permitted CSWinAgent Clients: *.*.*.*
NTLIB: Library behaviour mode 2
NTLIB: Initialising locally
NTLIB: The local computer name is ENG-IIS-WEST2
NTLIB: We are NOT a domain controller
NTLIB: We are a member of the ENGINEERING domain
Listener activated
```

Sample Debug Output for a Solaris Remote Agent

The following is startup output from a Solaris remote agent that is configured to run CSLogAgent:

```
cmi-xdm5:5> CSAgent -z -p
Running CSAgent server from command line..
Debug printing on..
CSAgent server starting ==============================
Running as console application.
Will listen on port 2004
Configuration will be fetched from 192.168.12.208:2003
```

```
Agents: CSLogAgent
CSLogAgent File: /opt/CSCOacsag/CSLogAgent/CSLogAgent
CSLogAgent Port: 2006
1 agents configured
Permitted CSAgent Clients: *.*.*.*
Listener activated
Hit Return/Enter to stop...

Watchdog activated
check_sys_limits set max file descriptors to 1024
Running CSLogAgent server from command line..
CSLogAgent server starting ============================
Running as console application.
Configuration will be fetched from 192.168.12.208:2003
Permitted CSLogAgent Clients: *.*.*.*
Cant get max number of connections maxNumberOfConnections using default 32
CreateProcess cd /opt/CSCOacsag/CSLogAgent; /opt/CSCOacsag/CSLogAgent/CSLogAgent -z & pid
= 8686
CSLogAgent launched
Agent library initialised
AgentLib: Attempting to connect to config provider at 192.168.12.208:2003
AgentLib: Connection established, handle 0x916c8
AgentLib: GetLogConfig reply received
AgentLib: Disconnecting from config provider, handle 0x916c8
Config downloaded
Will listen on port 2007
Will not log to a datafile.
g_started_ok=1
Listening thread started...

Rollover on /opt/CSCOacsag/Logs/Failed Attempts\Failed Attempts active.csv reset to
manual.
Rollover on /opt/CSCOacsag/Logs/RADIUS Accounting\RADIUS Accounting active.csv reset to
manual.
Rollover on /opt/CSCOacsag/Logs/TACACS+ Accounting\TACACS+ Accounting active.csv reset to
manual.
Rollover on /opt/CSCOacsag/Logs/TACACS+ Administration\Tacacs+ Administration active.csv
reset to manual.
Will use the Loglib library.
Stream thread N started
Stream N waiting for connection
```

The following is normal output when you press **Enter** to end the debug session:

```
Service stopping
Shutting down EndPoint library
Watchdog done. send kill to 8714
```

INDEX

C

cautions
  significance of 1-viii
Cisco Secure ACS for Windows Server 1-2
concurrent connections 1-2
configuration
  methods 1-2
  settings 4-2
configuration provider
  configuring 1-7
  definition 1-2
  logging configuration 1-3
conventions 1-vii
CSAgent
  description 1-5
  settings 4-2
  use at startup 1-2
CSAgent.ini
  configuring 4-6
  location 4-1
  options 4-2
  sample 4-5
  use at startup 1-2
CSLogAgent
  description 1-5
  process overview 1-3
  settings 4-3
CSWinAgent
  description 1-6
  process overview 1-4
  purpose 1-4
  settings 4-4

D

debugging 4-9
directories 4-8
documentation
  conventions 1-vii

E

encryption 1-1

I

installation
  for Solaris 3-2
  for Windows 2-4

L

local security setting, configuring in Windows 2-13
log format 4-4
logs
  location 4-8
  support 4-9

M

maintenance 4-7
member server
  configuring Windows 2-9

N

NTLM 2-6, 2-10

P

ports
- configuration provider 4-2
- CSAgent 4-2
- CSLogAgent
  - for accounting 4-3
  - for appliance messages 4-3
- CSWinAgent 4-4
- permitted by gateway devices 2-3, 3-2

R

requirements
- network 2-3, 3-2
- Solaris
  - hardware 3-1
  - operating system 2-2, 3-2
- Windows
  - hardware 2-2

restarting services 4-7

S

security 1-1
- service configuration 2-15

services
- starting 4-7
- stopping 4-7

services, configuring in Windows 2-15
starting services 4-7
stopping services 4-7
support logs 4-9

U

uninstalling
- for Solaris 3-5
- for Windows 2-5

upgrading
- for Solaris 3-6
- for Windows 2-5

W

warnings
- significance of 1-viii

Windows authentication
- member server 2-9