



Overview of Cisco Secure ACS Remote Agent

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

This chapter contains the following topics:

- [Description, page 1-1](#)
- [Limitations, page 1-2](#)
- [Remote Agent Concepts, page 1-2](#)
- [Remote Agent Services, page 1-7](#)
- [Configuring a Cisco Secure ACS Solution Engine, page 1-10](#)

Description

Cisco Secure ACS Remote Agent for Windows and Cisco Secure ACS Remote Agent for Solaris are applications that support Cisco Secure ACS Solution Engine 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 Cisco Secure ACS Solution Engine, you must use Cisco Secure 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 a Cisco Secure ACS Solution Engine cannot be a member of a Microsoft Windows domain, we provide Cisco Secure 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 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 a Cisco Secure ACS Solution Engine is encrypted, using the Blowfish algorithm and a 128-bit key. Additionally, encryption session keys are randomized and exchanged between the remote agent and the appliances it services using a public key exchange protocol.

For more information, see [Remote Agent Concepts, page 1-2](#).

Limitations

We designed Cisco Secure ACS Remote Agent with the following limitations.

- **Cisco Secure ACS Solution Engine only**—Cisco Secure ACS Remote Agent supports only Cisco Secure ACS Solution Engine. It cannot support Cisco Secure ACS for Windows Server.
- **Maximum number of appliances supported**—While a single Cisco Secure ACS Remote Agent can provide services to many Cisco Secure ACS Solution Engine appliances, support is limited to five concurrent connections by the appliances served. For example, if you have three appliances that are primary Cisco Secure ACSes and three appliances that are secondary Cisco Secure ACSes 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 the following topics:

- [Configuration Tools](#), page 1-3
- [Configuration Provider](#), page 1-3
- [Logging Overview](#), page 1-4
- [Authentication Overview](#), page 1-5

Configuration Tools

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

- **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**—A Cisco Secure ACS Solution Engine that provides additional configuration, especially for the remote agent logging service. For more information, see [Configuration Provider](#), page 1-3.

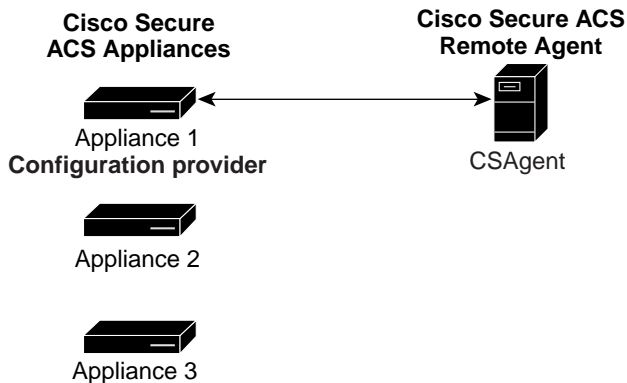
Configuration Provider

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 referred to as 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 1-7.

Figure 1-1 Configuration Provider and a Remote Agent



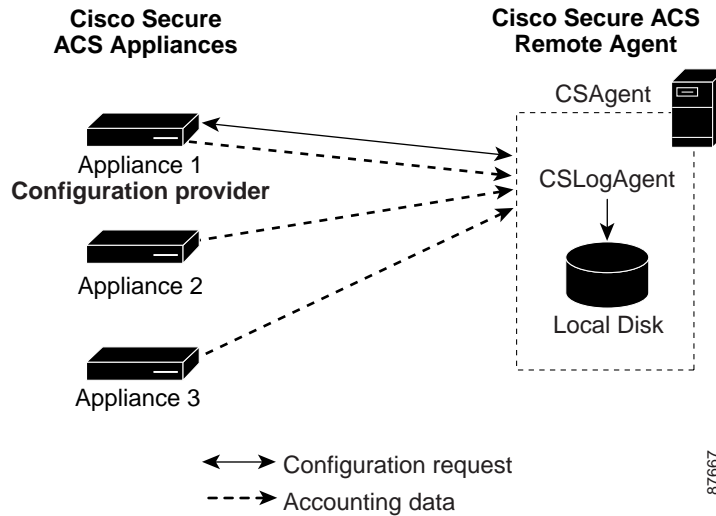
87666

Logging Overview

The remote agent is particularly dependent upon 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 Cisco Secure ACS Solution Engine appliances configured to use the remote agent send logging data directly to the remote agent logging service, CSLogAgent. CSLogAgent writes the logging data to hard disk in the location specified by the configuration provider. The logs contain the columns specified by the configuration provider. See [Figure 1-2](#). For more information about the CSLogAgent service, see [CSLogAgent, page 1-8](#).

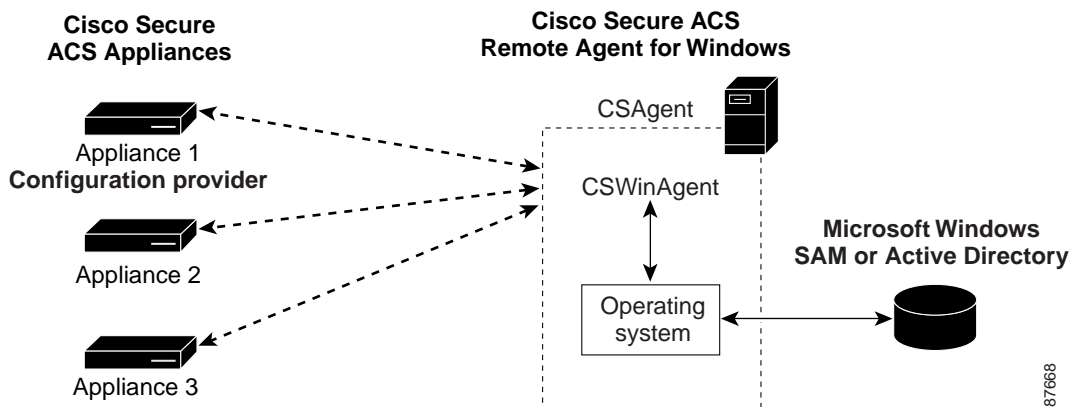
Figure 1-2 Multiple Appliances Logging to a Single Remote Agent



Authentication Overview

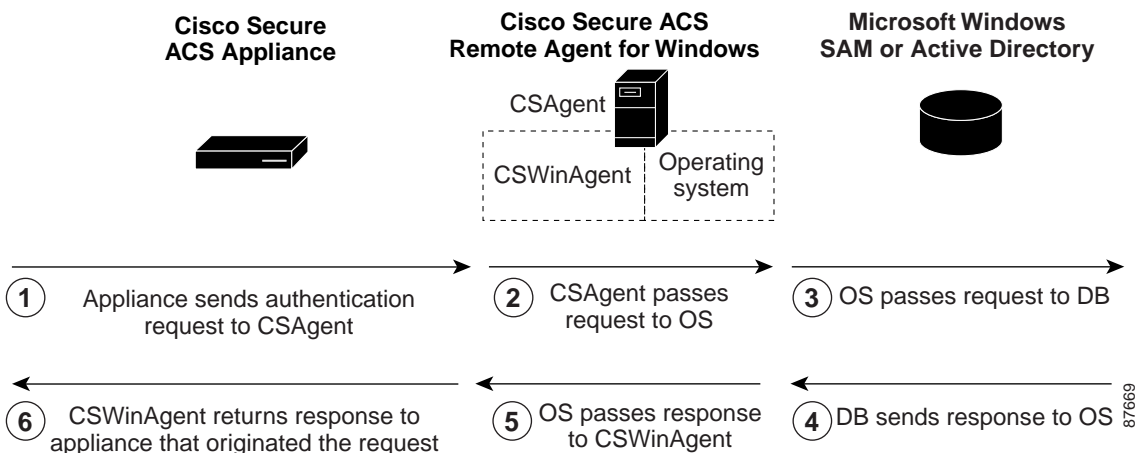
The Microsoft Windows authentication service, CSWinAgent, is available only in Cisco Secure ACS Remote Agent for Windows. CSWinAgent processes several types of authentication-related requests from appliances. These include requests for user authentication, user lookup for EAP-TLS support, user group membership lookup, user dial-in permission lookup, and group enumeration (used for configuring group mapping on an appliance). All appliances 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, 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 1-9](#).

Figure 1-4 Windows Authentication Messaging



Remote Agent Services

As an application, Cisco Secure ACS Remote Agent is made up of separate services.

This section contains the following topics:

- [CSAgent, page 1-7](#)
- [CSLogAgent, page 1-8](#)
- [CSWinAgent, page 1-9](#)

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 “CiscoSecure 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 4-10](#).
- **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 again.
- **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 4-12](#).
- **Support log collection**—When requested to do so by an appliance, CSAgent also collects diagnostic logs and compresses them into a single cabinet file. For more information, see [Retrieving Support Logs, page 4-14](#).

- **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 4-14](#).
- **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. It is controlled by CSAgent 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 Cisco Secure ACS (<http://www.extraxi.com>). The values recorded in each report type are determined by the configuration provider. You configure the reports by using the HTML interface of configuration provider defined in the CSAgent.ini file. For information about log locations, see [File and Directory Structure, page 4-12](#). 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 4-12](#).

- **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 4-14](#).
- **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. It is the service that supports Microsoft Windows authentication. It is controlled by CSAgent but it receives authentication requests from appliances directly on the ports it is configured to listen to. 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 on to the appliance initiating the query.

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

For PAP and EAP-GTC authentication requests, Cisco Secure ACS Solution Engine converts the plaintext password to MS-CHAP credentials before sending the request to a remote agent. This 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, located in the Log subdirectory within the CSWinAgent directory. For more information, see [File and Directory Structure, page 4-12](#).
- **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 4-14](#).

- **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 a Cisco Secure ACS Solution Engine

You can configure how a Cisco Secure ACS Solution Engine uses a remote agent. On the appliance that a remote agent is configured to use as its 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 the following topics.

- Adding a remote agent to the network configuration of a Cisco Secure ACS Solution Engine.
- Performing Windows authentication with remote agents.
- Logging with remote agents.