



CHAPTER 1

Introduction to Cisco Secure ACS Remote Agents

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

This chapter contains:

- [Overview](#)
- [Limitations](#)
- [Remote Agent Concepts](#)
- [Remote Agent Services](#)
- [Configuring ACS SE for a Remote Agent](#)

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 4.2 provides 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 each authentication request that it receives from an appliance to Microsoft Windows. When it receives the authentication response, the remote agent forwards the response to the appliance that initiated the request.

The Blowfish algorithm and a 128-bit key are used to encrypt all communication between a remote agent and ACS SE. 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](#).

Limitations

ACS Remote Agent has been designed 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](#)
- [Configuration Provider](#)
- [Logging Overview](#)
- [Authentication Overview](#)

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 that contains configuration values that the remote agent uses for self-configuration when it starts. See [Configuring a Remote Agent](#).
- **Configuration provider**—An ACS SE that provides additional configuration, especially for the remote agent logging service. For more information, see [Configuration Provider](#).

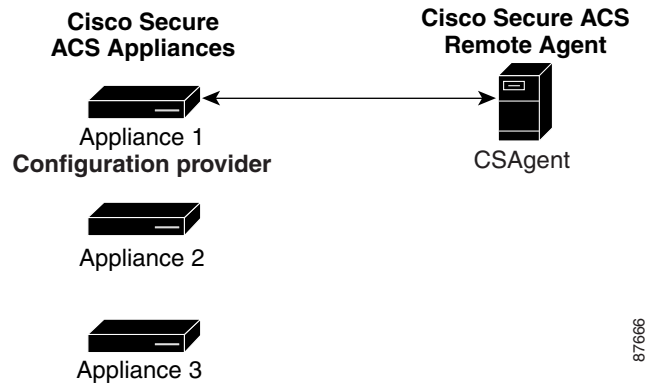
Configuration Provider

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](#).

Figure 1-1 Configuration Provider and a Remote Agent

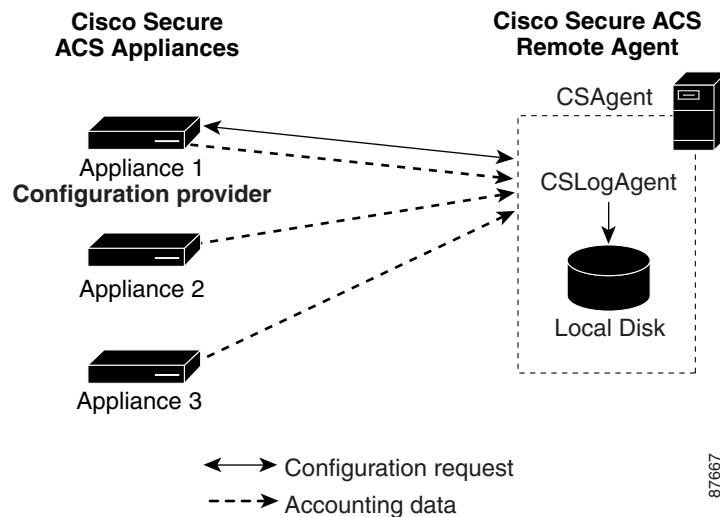


Logging Overview

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 4.2*.

All ACS SE appliances that you 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**.

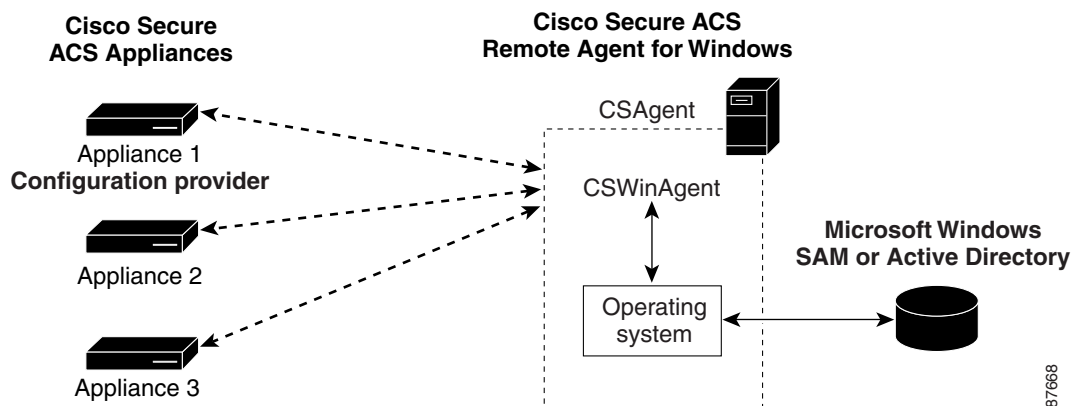
Figure 1-2 Multiple Appliances Logging to a Single Remote Agent



Authentication Overview

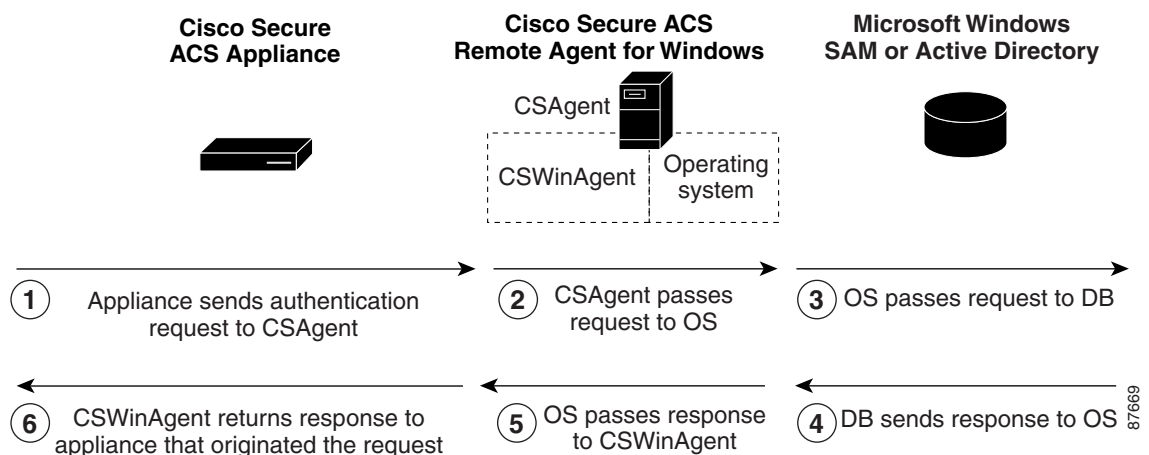
The Microsoft Windows authentication service, **CSWinAgent**, is available only in ACS Remote Agent for Windows. **CSWinAgent** processes several types of authentication-related requests from appliances. These include requests for user authentication, user lookup for Extensible Authentication Protocol - Transport Layer Security (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 middleman 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](#).

Figure 1-4 Windows Authentication Messaging



Remote Agent Services

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

- [CSAgent](#)
- [CSLogAgent](#)
- [CSWinAgent](#)

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 the configuration of the *CSAgent.ini* file determines. 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](#).
- **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, in the Log subdirectory in the **CSAgent** directory. For more information, see [File and Directory Structure](#).
- **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](#).
- **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](#).
- **Configurable TCP port**—By default, **CSAgent** listens on TCP port 2004 for requests from appliances. You can configure the port that the system uses. For more information, see [Configuring a Remote Agent](#).
- **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](#).

CSLogAgent

CSLogAgent is the logging service. **CSAgent** controls the logging service but receives logging data directly from appliances. When **CSLogAgent** starts, it requests its configuration from the configuration provider that the *CSAgent.ini* file specifies. After it receives its configuration, it is ready to provide 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 that the *CSAgent.ini* file defines. For information about log locations, see [File and Directory Structure](#). For information about configuring logs in the HTML interface of a configuration provider, see *User Guide for Cisco Secure ACS Solution Engine 4.2*.
- **Diagnostic log**—**CSLogAgent** records errors in its service log file, in the *Log* subdirectory in the **CSLogAgent** directory. For more information, see [File and Directory Structure](#).
- **Debug mode**—When you run **CSAgent** in debug mode, **CSLogAgent** also runs in debug mode, including support for verbose output. For more information, see [Running CSAgent in Debug Mode](#).
- **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](#).
- **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](#).

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 directly from appliances 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 the 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 in the **CSWinAgent** directory. For more information, see [File and Directory Structure](#).
- **Debug mode**—When you run **CSAgent** in debug mode, **CSWinAgent** also runs in debug mode, including support for verbose output. For more information, see [Running CSAgent in Debug Mode](#).
- **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](#).
- **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](#).

Configuring ACS SE for a Remote Agent

You can configure how ACS SE uses a remote agent. On the appliance that you 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 4.2* contains information about:

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

