



APPENDIX **F**

Internal Architecture

This appendix describes the architectural components of the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS. ACS is modular and flexible to fit the needs of simple and large networks. This appendix includes the following topics:

- [Windows Services, page F-1](#)
- [Windows Registry \(ACS for Windows Only\), page F-2](#)
- [Solution Engine Services, page F-3](#)
- [CSAdmin, page F-7](#)
- [CSAgent \(ACS SE Only\), page F-8](#)
- [CSAuth, page F-9](#)
- [CSDBSync, page F-9](#)
- [CSLog, page F-9](#)
- [CSMon, page F-10](#)
- [CSTacacs and CSRADIUS, page F-12](#)
- [Disabling NetBIOS, page F-12](#)

Windows Services

ACS includes the following service modules:

- **CSAdmin**
- **CSAuth**
- **CSDBSync**
- **CSLog**
- **CSMon**
- **CSTacacs**
- **CSRADIUS**

You can stop or restart ACS services as a group, except for **CSAdmin**, by using the ACS web interface. For more information, see [Service Control, page 7-1](#).

ACS for Windows

You can start, stop, and restart individual ACS services from the Services window in the Control Panel.

ACS SE

You can start, stop, and restart individual ACS services from the appliance serial console. For more information about starting, stopping, and restarting services by using the serial console, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

Windows Registry (ACS for Windows Only)

**Warning**

Do not modify the Windows Registry unless you have enough knowledge and experience to edit the file without destroying or corrupting crucial data.

Only general ACS application information (such as the installation directory location) will continue to use the Windows registry.

The ACS information is located in the following Windows Registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\CISCO

Unless a Cisco representative advises you to do so, we strongly recommend that you do not modify Windows Registry settings pertaining to ACS.

SQL Registry

In order to create a unified data storage model, ACS has moved from multiple data storages to a standard SQL-based relational database.

The SQL registry contains table information on all user and configuration data. SQL data is not made available for viewing and is protected by an encrypted password.

SQL Tables	Description
ConfigKey	Information that is not stored in the other tables. The data corresponds to registry keys.
ConfigValue	Data corresponding to registry values.
DictKey	Tree of attribute keys. The data is corresponds to registry keys of the ACS dictionary.
DictValue	Values for attributes keys from the ACSDictionaryKeys table.
Host	Information regarding all hosts in ACS.
HostService	Additional data for hosts of type remote agent.
Admin	ACS administrators. The permissions for each administrator are represented as a bitset inside a binary blob.
NetworkModel	Network model section.
Users	All user-specific information that was previously stored in the <i>user.dat</i> file. This table structure represents ACS UDB_ACCOUNT structure. However, some fields will not appear.
VarsDB	Currently in use but will be moved to a new table.

Solution Engine Services

The ACS SE includes the CSAgent service in addition to the Windows services.

The operating system for the ACS SE is customized version of the Windows 2003 R2 operating system which is minimized for performance. The ACS SE removes all extraneous services, blocks all unused ports, and prevents all other access to the ACS server system, thereby dramatically increasing the security posture of the Solution Engine.

The minimization of the operating system's services is reflected as follows:

- [Operating System Services the ACS SE Automatically Runs](#), page F-3
- [Disabled Operating System Services in the ACS SE](#), page F-4

Operating System Services the ACS SE Automatically Runs

Table F-1 lists the operating services that the ACS SE automatically runs.

Table F-1 *Operating Services that the ACS SE Automatically Runs*

Service Name	Description
COM+ Event System	Provides automatic distribution of events to subscribing COM components.
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.
DNS Client	Resolves and caches Domain Name System (DNS) names.
Event Log	Logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer.
IPSEC Policy Agent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.
License Logging Service	Tracks Client Access License usage for a server product.
Logical Disk Manager	Performs the Logical Disk Manager Watchdog Service.
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which you can view local area network and remote connections.
Plug and Play	Manages device installation and configuration and notifies programs of device changes.
Protected Storage	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.
Remote Procedure Call (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.
Removable Storage	Manages removable media, drives, and libraries.

Table F-1 *Operating Services that the ACS SE Automatically Runs*

Service Name	Description
RunAs Service	Enables starting processes under alternate credentials.
Security Accounts Manager	Stores security information for local user accounts.
Server	Provides RPC support and file, print, and named pipe sharing.
System Event Notification	Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.
Telnet	Allows a remote user to log on to the system and run console programs by using the command line.
Windows Management Instrumentation	Provides system management information.
Windows Management Instrumentation Driver Extensions	Provides systems management information to and from drivers.

Disabled Operating System Services in the ACS SE

[Table F-2](#) below lists the operating system services that are not run on the ACS SE.

Table F-2 *Operating System Services Not Run on the ACS SE*

Service Name	Description
Alerter	Notifies selected users and computers of administrative alerts.
Application Management	Provides software installation services such as Assign, Publish, and Remove.
Automatic Updates	Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site.
Background Intelligent Transfer Service	Transfers files in the background by using idle network bandwidth. If the service is stopped, features such as Windows Update, and MSN Explorer will be unable to automatically download programs and other information. If this service is disabled, any services
ClipBook	Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.
Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.
Distributed File System	Manages logical volumes distributed across a local or wide area network.

Table F-2 *Operating System Services Not Run on the ACS SE (continued)*

Service Name	Description
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.
Distributed Link Tracking Server	Stores information so that files moved between volumes can be tracked for each volume in the domain.
Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction-protected resource managers.
Fax Service	Helps you send and receive faxes.
File Replication	Maintains file synchronization of file directory contents among multiple servers.
Indexing Service	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.
Internet Connection Sharing	Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.
Intersite Messaging	Allows sending and receiving messages between Windows Advanced Server sites.
Kerberos Key Distribution Center	Generates session keys and grants service tickets for mutual client/server authentication.
Logical Disk Manager Administrative Service	Performs administrative service for disk management requests.
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.
Net Logon	Supports pass-through authentication of account logon events for computers in a domain.
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop by using NetMeeting.
Network DDE	Provides network transport and security for dynamic data exchange (DDE).
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE
NT LM Security Support Provider	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.
Performance Logs and Alerts	Configures performance logs and alerts.
Print Spooler	Loads files to memory for later printing.
QoS RSVP	Provides network signaling and local traffic control setup functionality for Quality of Service (QoS)-aware programs and control applets.

Table F-2 Operating System Services Not Run on the ACS SE (continued)

Service Name	Description
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.
Remote Access Connection Manager	Creates a network connection.
Remote Procedure Call (RPC) Locator	Manages the RPC name service database.
Remote Registry Service	Allows remote Registry manipulation.
Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.
Smart Card	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.
Smart Card Helper	Provides support for legacy smart card readers attached to the computer.
Task Scheduler	Enables a program to run at a designated time.
TCP/IP NetBIOS Helper Service	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.
Telephony API (TAPI)	Provides Telephony API (TAPI) support for programs that control telephony devices and IP-based voice connections on the local computer and, through the LAN, on servers that are also running the service.
Terminal Services	Provides a multisession environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server.
Uninterruptible Power Supply	Manages an uninterruptible power supply (UPS) connected to the computer.
Utility Manager	Starts and configures accessibility tools from one window.
WMDM PMSP Service	-
Workstation	Provides network connections and communications.
Windows Installer	Installs, repairs, and removes software according to instructions contained in the .msi files.
Windows Time	Sets the computer clock.

Packet Filtering

Packet Filtering is the service that blocks the traffic on all but necessary IP ports.

[Table F-3](#) lists the ports that are open for input traffic for the ACS SE.

Table F-3 *Input Traffic Open Ports for the Packet Filter*

Service Name	UDP	TCP
DHCP	68	
RADIUS authentication & authorization (original draft RFC)	1645	
RADIUS accounting (original draft RFC)	1646	
RADIUS authentication & authorization (revised RFC)	1812	
RADIUS accounting (original draft RFC)	1813	
Proxy DLLs (RSA)	5500-5509	
TACACS+ authentication, authorization & accounting		49
ACS replication		2000
ACS logging		2001
ACS distributed logging		2003
ACS HTTP admin		2002
ACS HTTPS admin		2002
ACS administration port range		Dynamic

CSAdmin

CSAdmin is the service that provides the web server for the ACS web interface. After ACS is installed, you must configure it from its web interface; therefore, **CSAdmin** must be running when you configure ACS.

Because the ACS web server uses port 2002, rather than the standard port 80 that is usually associated with HTTP traffic, you can use another web server on the same machine to provide other web services. We have not performed interoperability testing with other web servers, but unless a second web server is configured to use either port 2002 or one of the ports within the range specified in the HTTP Port Allocation feature, you should not encounter port conflicts for HTTP traffic. For more information about the HTTP Port Allocation feature, see [Configuring Access Policy, page 11-8](#) and [Access Policy Setup Page, page 11-18](#).

Although you can start and stop services from within the ACS web interface, you cannot start or stop **CSAdmin**.

ACS for Windows

If **CSAdmin** stops abnormally because of an external action, you cannot access ACS from any computer other than the Windows server on which it is running. You can start or stop **CSAdmin** from the Windows Control Panel.

ACS SE

If **CSAdmin** stops abnormally because of an external action, you can restart the service by using only the appliance serial console. For more information about starting, stopping, and restarting services by using the serial console, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

Both Platforms

CSAdmin is multi-threaded, which enables several ACS administrators to access it at the same time. Therefore, **CSAdmin** is well suited for distributed, multiprocessor environments.

CSAgent (ACS SE Only)

CSAgent is the service that is used for protecting the ACS SE from viruses, worms, and attacks. **CSAgent** operates in standalone mode on the Solution Engine. You can start, stop, and restart the **CSAgent** using the serial console. For more information about starting, stopping, and restarting services by using the serial console, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

**Note**

The **CSAgent** imposes the following restrictions on ACS when it is enabled. You cannot apply upgrades or patches by using the Appliance Upgrade Status page in the System Configuration section or the upgrade command on the appliance console. To upgrade ACS or apply patches, **CSAgent** must be disabled.

CSAgent Policies

The **CSAgent** service for the ACS SE is configured with the following policies:

- **Application Control**—**CSAgent** permits execution applications that are required for ACS to operate correctly.
- **File Access Control**—**CSAgent** permits file system access for applications that are required for ACS to operate correctly.
- **IP and Transport Control**—**CSAgent** provides the following protections:
 - Discards invalid IP headers.
 - Discards invalid transport headers.
 - Detects TCP/UDP port scans.
 - Cloaks the appliance to prevent port scans.
 - Prevents TCP blind session spoofing.
 - Prevents TCP SYN floods.
 - Blocks ICMP covert channels.
 - Blocks dangerous ICMP messages, including ping.
 - Prevents IP source routing.
 - Prevents trace routing.
- **E-mail Worm Protection**—**CSAgent** guards the appliance against e-mail worms.
- **Registry Access Control**—**CSAgent** permits registry access to only those applications requiring access for proper operation of the appliance.

- **Kernel Protection**—CSAgent does not allow kernel modules to be loaded after system startup is complete.
- **Trojan and Malicious Application Protection**—CSAgent provides the following protections. Applications cannot:
 - Write code to space owned by other applications.
 - Download and execute ActiveX controls.
 - Automatically execute downloaded programs.
 - Directly access operating system password information.
 - Write into memory owned by other processes.
 - Monitor keystrokes while accessing the network.

CSAuth

CSAuth is the authentication and authorization service. It permits or denies access to users by processing authentication and authorization requests. **CSAuth** determines if access should be granted and defines the privileges for a particular user. **CSAuth** is the ACS database manager.

To authenticate users, ACS can use the internal database or one of many external databases. When a request for authentication arrives, ACS checks the database that is configured for that user. If the user is unknown, ACS checks the database(s) configured for unknown users. For more information about how ACS handles authentication requests for unknown users, see [About Unknown User Authentication, page 15-3](#).

For more information about the various database types supported by ACS, see [Chapter 12, “User Databases.”](#)

When a user has authenticated, ACS obtains a set of authorizations from the user profile and the group to which the user is assigned. This information is stored with the username in the ACS internal database. Some of the authorizations included are the services to which the user is entitled, such as IP over PPP, IP pools from which to draw an IP address, access lists, and password-aging information. The authorizations, with the approval of authentication, are then passed to the **CSTacacs** or **CSRADIUS** modules to be forwarded to the requesting device.

CSDBSync

CSDBSync is the service used to synchronize the ACS database with third-party relational database management system (RDBMS) systems. **CSDBSync** synchronizes AAA client, AAA server, network device groups (NDGs) and Proxy Table information with data from a table in an external relational database. For information on RDBMS Synchronization, see [RDBMS Synchronization, page 8-17](#).

CSLog

CSLog is the service used to capture and place logging information. **CSLog** gathers data from the TACACS+ or RADIUS packet and **CSAuth**, and then manipulates the data to be placed into the comma-separated value (CSV) files. CSV files can be imported into spreadsheets that support this format.

CSMon

CSMon is a service that helps minimize downtime in a remote access network environment. **CSMon** works for TACACS+ and RADIUS and automatically detects which protocols are in use.

You can use the ACS web interface to configure the **CSMon** service. The ACS Active Service Management feature provides options for configuring **CSMon** behavior. For more information, see [ACS Active Service Management, page 7-18](#).



Note

CSMon is not intended as a replacement for system, network, or application management applications but is provided as an application-specific utility that can be used with other, more generic system management tools.

CSMon performs four basic activities, outlined in the following topics:

- [Monitoring, page F-10](#)
- [Recording, page F-11](#)
- [Notification, page F-11](#)
- [Response, page F-11](#)

Monitoring

CSMon monitors the overall status of ACS and the system on which it is running. **CSMon** actively monitors three basic sets of system parameters:

- **Generic host system state**—**CSMon** monitors the following key system thresholds:
 - Available hard disk space
 - Processor utilization
 - Physical memory utilization

All events related to generic host system state are categorized as warning events.

- **Application-specific performance**
 - **Application viability**—**CSMon** periodically performs a test login by using a special built-in test account (the default period is one minute). Problems with this authentication can be used to determine if the service has been compromised.
 - **Application performance thresholds**—**CSMon** monitors and records the latency of each test authentication request (the time it takes to receive a positive response). Each time this is performed, **CSMon** updates a variable containing the average response time value. Additionally, it records whether retries were necessary to achieve a successful response. By tracking the average time for each test authentication, **CSMon** can build up a picture of expected response time on the system in question. **CSMon** can therefore detect whether excess retries are required for each authentication or if response times for a single authentication exceed a percentage threshold over the average.
- **System resource consumption by ACS**—**CSMon** periodically monitors and records the usage by ACS of a small set of key system resources and compares it against predetermined thresholds for indications of atypical behavior. The parameters monitored include the following:
 - Handle counts

- Memory utilization
- Processor utilization
- Thread used
- Failed log-on attempts

CSMon cooperates with **CSAuth** to keep track of user accounts being disabled by exceeding their failed attempts count maximum. This feature is more oriented to security and user support than to system viability. If configured, it provides immediate warning of brute-force attacks by alerting the administrator to a large number of accounts becoming disabled. In addition, it helps support technicians anticipate problems with individual users gaining access.

Recording

CSMon records exception events in logs that you can use to diagnose problems.

- **CSMon Log**—Like the other ACS services, **CSMon** maintains a CSV log of its own for diagnostic recording and error logging. Because this logging consumes relatively small amounts of resources, **CSMon** logging cannot be disabled.
- **Windows Event Log**—**CSMon** can log messages to the Windows Event Log. Logging to the Windows Event Log is enabled by default but can be disabled.

Notification

CSMon can be configured to notify system administrators in the following cases:

- Exception events
- Response
- Outcome of the response

Notification for exception events and outcomes includes the current state of ACS at the time of the message. The default notification method is simple mail-transfer protocol (SMTP) e-mail, but you can create scripts to enable other methods.

Response

CSMon detects exception events that affect the integrity of the service. For information about monitored events, see [Monitoring, page F-10](#). These events are application-specific and hard-coded into ACS. The two types of responses are:

- **Warning events**—Service is maintained but some monitored threshold is breached.
- **Failure events**—One or more ACS components stop providing service.

CSMon responds to the event by logging the event, sending notifications (if configured) and, if the event is a failure, taking action. The two types of actions are:

- **Predefined actions**—These actions are hard-coded into the program and are always carried out when a triggering event is detected. Because these actions are hard-coded, they are integral to the application and do not need to be configured. These actions include running the **CSSupport** utility, which captures most of the parameters dealing with the state of the system at the time of the event.

If the event is a warning event, it is logged and the administrator is notified. No further action is taken. **CSMon** also attempts to fix the cause of the failure after a sequence of retries and individual service restarts.

- **Customer-Definable Actions**—If the predefined actions built into **CSMon** do not fix the problem, **CSMon** can execute an external program or script.

CSTacacs and CSRADIUS

The **CSTacacs** and **CSRADIUS** services communicate between the **CSAuth** module and the access device that is requesting authentication and authorization services. For **CSTacacs** and **CSRADIUS** to work properly, the system must meet the following conditions:

- **CSTacacs** and **CSRADIUS** services must be configured from **CSAdmin**.
- **CSTacacs** and **CSRADIUS** services must communicate with access devices such as access servers, routers, switches, and firewalls.
- The identical shared secret (key) must be configured both in ACS and on the access device.
- The access device IP address must be specified in ACS.
- The type of security protocol being used must be specified in ACS.

CSTacacs is used to communicate with TACACS+ devices and **CSRADIUS** to communicate with RADIUS devices. Both services can run at the same time. When only one security protocol is used, only the applicable service needs to be running; however, the other service will not interfere with normal operation and does not need to be disabled. For more information about TACACS+ AV pairs, see [Appendix A, “TACACS+ Attribute-Value Pairs.”](#) For more information about RADIUS+ AV pairs, see [Appendix B, “RADIUS Attributes.”](#)

Disabling NetBIOS

NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a LAN. Since the late 1980s, Microsoft has adopted NetBIOS as its LAN Manager product, and, from there, it found its way into early versions of Windows and all the way into Windows NT.

Since the Windows 2000 release, DNS has become the default name resolution method for Windows-based networks and is required if you want to deploy Active Directory domains.

Although you can use Windows 2000, Windows XP, and Windows Server 2003 to disable NetBIOS over TCP/IP (NetBT), many corporate networks remain reluctant to do so, since most of them still have legacy (Windows 9x or Windows NT) machines on their network. These machines need NetBIOS to function properly on a network, since they use NetBIOS to log in to domains, find one another, and establish sessions for accessing shared resources.

However, with networks that are free of legacy systems, administrators may want to consider disabling the NetBT transport on all of the computers. ACS supports the Windows server with NetBIOS disabled.

For more details about disabling NetBIOS, refer to your Windows Operating system guide.