

Windows Service Advisement

The operating system for the Cisco Secure ACS SE is a customized and minimized version of the Windows 2003 operating system. The ACS SE removes all extraneous services, blocks all unused ports, and otherwise prevents all other access to the ACS server system, thereby dramatically increasing the security posture of ACS.

The following sections present details regarding the minimization of the operating system's services:

- [Services that are Run, page C-1](#)
- [Services that are Not Run, page C-3](#)

Services that are Run

[Table C-1](#) lists the services that are run on the ACS SE.

Table C-1 Operating System Services Automatically Run by ACS SE

Service Name	Description
AppLPFSvr	—
AppLPFSvr Monitor	—
Application Experience Lookup Service	Process application compatibility lookup requests for applications as they are launched.
Cisco Security Agent	—
COM+ Event System	Provides automatic distribution of events to subscribing COM components.
Computer Browser	Maintains an updated list of computers on the network and supplies this list to computers designated as browsers. If this service is stopped, this list will not be updated or maintained. If this service is disabled, any services that explicitly depend on it will fail to start.
CSAdmin	Cisco Secure WWW Server. Allows administration of Cisco Secure using WWW browsers.
CSAuth	Cisco Secure Authentication Service. Provides core Cisco Secure functionality.
CSDbSync	Cisco Secure Database Synchronization Service. Allows synchronization with external database.

Table C-1 Operating System Services Automatically Run by ACS SE (continued)

Service Name	Description
CSLog	Cisco Secure Log Service. Generates accounting log files.
CSMon	Cisco Secure Monitor Service. Provides monitoring, alert and auto-restart of Cisco Secure services for high availability.
CSRADIUS	Cisco Secure RADIUS Server. Provides authentication, authorization and accounting using the RADIUS protocol.
CSTacacs	Cisco Secure RADIUS Server. Provides authentication, authorization and accounting using the RADIUS protocol.
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.
DNS Client 5t	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 the Event Viewer.
Error Reporting Service	Collects, stores, and reports unexpected application crashes to Microsoft. If this service is stopped, then Error Reporting will occur only for kernel faults and some types of user mode faults. If this service is disabled, any services that explicitly depend on it will not start.
Help and Support	Enables Help and Support Center to run on this computer. If this service is stopped, Help and Support Center will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
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.
Network Location Awareness (NLA)	Collects and stores network configuration and location information, and notifies applications when this information changes.
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.
Secondary logon (Run as Service in Windows 2000)	Enables starting processes under alternate credentials.
Security Accounts Manager	Stores security information for local user accounts.
System Event Notification	Tracks system events such as Windows login, network, and power events. Notifies COM+ Event System subscribers of these events.
SNMP	Simple Network Management Protocol

Table C-1 Operating System Services Automatically Run by ACS SE (continued)

Service Name	Description
Telnet	Allows a remote user to log on to the system and run console programs using the command line.
Terminal Services	Allows you to connect interactively to a remote computer. Remote Desktop, Fast User Switching, Remote Assistance, and Terminal Server depend on this service. Stopping or disabling this service may make your computer unreliable
Transport	—
Windows Management Instrumentation	Provides system management information.
Windows Management Instrumentation Driver Extensions	Provides systems management information to and from drivers.
Workstation	Creates and maintains client network connections to remote servers. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Services that are Not Run

Table C-2 lists the operating system services that are not run on the ACS SE.

Table C-2 Disabled Operating System Services in 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 website.
Application Layer Gateway Service	Provides support for 3rd party protocol plug-ins for Internet Connection Sharing and the Windows Firewall
Background Intelligent Transfer Service	Transfers files in the background 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.

Table C-2 Disabled Operating System Services in ACS SE (continued)

Service Name	Description
COM+ System Application	Manages the configuration and tracking of Component Object Model (COM)+-based components. If the service is stopped, most COM+-based components will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.
Distributed File System	Manages logical volumes distributed across a local or wide area network.
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.
File Replication	Maintains file synchronization of file directory contents among multiple servers.
HTTP SSL	This service implements the secure hypertext transfer protocol (HTTPS) for the HTTP service, using the Secure Socket Layer (SSL). If this service is disabled, any services that explicitly depend on it will fail to start.
Human Interface Device Access	Enables generic input access to Human Interface Devices (HID), which activates and maintains the use of predefined hot buttons on keyboards, remote controls, and other multimedia devices. If this service is stopped, hot buttons controlled by this service will no longer function. If this service is disabled, any services that explicitly depend on it will fail to start.
IMAPI CD-Burning COM Service	Manages CD recording using Image Mastering Applications Programming Interface (IMAPI). If this service is stopped, this computer will be unable to record CDs. If this service is disabled, any services that explicitly depend on it will fail to start.
Indexing Service	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.
Intersite Messaging	Allows sending and receiving of messages between Windows Advanced Server sites.
IPSEC Services	Provides end-to-end security between clients and servers on TCP/IP networks. If this service is stopped, TCP/IP security between clients and servers on the network will be impaired. If this service is disabled, any services that explicitly depend on it will fail to start.
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.

Table C-2 Disabled Operating System Services in ACS SE (continued)

Service Name	Description
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.
Microsoft Software Shadow Copy Provider	Manages software-based volume shadow copies taken by the Volume Shadow Copy service. If this service is stopped, software-based volume shadow copies cannot be managed. If this service is disabled, any services that explicitly depend on it will fail to start.
Net Logon	Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start.
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop 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.
Network Provisioning Service	Manages XML configuration files on a domain basis for automatic network provisioning.
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.
Portable Media Serial Number Service	Retrieves the serial number of any portable media player connected to this computer. If this service is stopped, protected content might not be down loaded to the device.
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	Enables remote procedure call (RPC) clients using the RpcNs* family of APIs to locate RPC servers. If this service is stopped or disabled, RPC clients using RpcNs* APIs may be unable to locate servers or fail to start. RpcNs* APIs are not used internally in Windows.
Remote Registry Service	Allows remote Registry manipulation.
Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.
Remote Desktop Help Session Manager	Manages and controls Remote Assistance. If this service is stopped, Remote Assistance will be unavailable. Before stopping this service, see the Dependencies tab of the Properties dialog box.

Table C-2 Disabled Operating System Services in ACS SE (continued)

Service Name	Description
Resultant Set of Policy Provider	Enables a user to connect to a remote computer, access the Windows Management Instrumentation database for that computer, and either verify the current Group Policy settings made for the computer or check settings before they are applied. If this service is stopped, remote verification will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
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.
SNMP TRAP service	—
Special Administration Console Helper	Allows administrators to remotely access a command prompt using Emergency Management Services.
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 Session Directory	Enables a user connection request to be routed to the appropriate terminal server in a cluster. If this service is stopped, connection requests will be routed to the first available server.
Themes	Provides user experience theme management.
Uninterruptible Power Supply	Manages an uninterruptible power supply (UPS) connected to the computer.
Virtual Disk Service	Provides software volume and hardware volume management service.
Volume Shadow Copy	Manages and implements Volume Shadow Copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. If this service is disabled, any services that explicitly depend on it will fail to start.
WebClient	Enables Windows-based programs to create, access, and modify Internet-based files. If this service is stopped, these functions will not be available. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Audio	Manages audio devices for Windows-based programs. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

Table C-2 Disabled Operating System Services in ACS SE (continued)

Service Name	Description
Windows Firewall/Internet Connection Sharing (ICS)	Provides network address translation, addressing, name resolution and/or intrusion prevention services for a home or small office network.
Windows Installer	Installs, repairs, and removes software according to instructions contained in the <i>.msi</i> files.
Windows Image Acquisition (WIA)	Provides image acquisition services for scanners and cameras.
Windows User Mode Driver Framework	Enables Windows user mode drivers.
Windows Time	Sets the computer clock.
WinHTTP Web Proxy Auto-Discovery Service	Implements the Web Proxy Auto-Discovery (WPAD) protocol for Windows HTTP Services (WinHTTP). WPAD is a protocol to enable an HTTP client to automatically discover a proxy configuration. If this service is stopped or disabled, the WPAD protocol will be executed within the HTTP client's process instead of an external service process; there would be no loss of functionality as a result.
Wireless Configuration	Provides authenticated network access control using IEEE 802.1x for wired and wireless Ethernet networks.
WMI Performance Adapter	Provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network. This service only runs when Performance Data Helper is activated.

■ Services that are Not Run