



APPENDIX **B**

Windows Service Advisement

The operating system for the Cisco Secure ACS Solution Engine (ACS SE) is a customized and minimized version of the Windows 2000 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 B-1](#)
- [Services That Are Not Run, page B-2](#)

Services That are Run

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

Table B-1 *Operating System Services Automatically Run by ACS SE*

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.

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

Service Name	Description
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.
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.

Services That Are Not Run

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

Table B-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 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 B-2 Disabled Operating System Services in 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.
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.

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

Service Name	Description
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 <i>.msi</i> files.
Windows Time	Sets the computer clock.