

Cisco Secure Access Control Server Solution Engine 4.2

Q. What is Cisco® Secure Access Control Server (ACS) Solution Engine?

A. Cisco ACS Solution Engine is a one-rack-unit (1RU) appliance that is preloaded with Cisco Secure ACS 4.2 software.

Q. What's new in Cisco Secure ACS Solution Engine 4.2 for access control functions and features?

A. Version 4.2 is a minor update to Cisco Secure ACS and adds the following main features:

- Extensible Authentication Protocol (EAP) protocol options:
 - EAP-Flexible Authentication via Secure Tunneling (FAST) enhancement for anonymous Transport Layer Security (TLS) renegotiation: ACS allows an anonymous TLS handshake between the end-user client and ACS.
 - EAP-FAST enhancement for invalid Protected Access Credentials (PAC): ACS provides an option to run EAP-FAST without issuing or accepting any tunnel or machine PAC when an invalid PAC is received.
 - EAP-TLS with no PAC and no Active Directory processing: ACS supports EAP-FAST tunnel establishment without PAC and without client certificate lookup.
- Group filtering at the Network Access Profile (NAP) level with Lightweight Directory Access Protocol (LDAP): When using LDAP to query an external user data store, ACS capabilities have been extended to allow group filtering at the NAP level. Depending on the user's external database group membership, ACS can either reject or accept access to the network based on the group filtering settings.
- RSA authentication with LDAP group mapping: ACS can authenticate with RSA and at the same time perform group mapping with LDAP. This option allows ACS to control authorization based on a user's LDAP group membership.
- Active Directory multiforest support: ACS supports authentication in a multiforest environment.
- Time-based restrictions: ACS administrators may configure a user to be in an alternative group for a restricted period of time.
- Relational database management system (RDBMS) synchronization enhancements: ACS has programmatic interface additions for downloadable ACL synchronization. ACS Solution Engine now also supports scriptable RDBMS synchronization through a Secure Shell (SSH) Protocol client.
- Internet Control Message Protocol (ICMP) ping on/off: ICMP ping response can be turned on or off.
- Native RSA support: Support of the RSA proprietary interface on the ACS Solution Engine provides parity with ACS for Windows.
- Upgrade of Windows operating system.

Please refer to the product release notes at

http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_release_notes_list.html for a complete list of new and changed features.

Q. Why did Cisco add an appliance to the existing Windows server software packaging for Cisco Secure ACS?

A. The decision to create a dedicated appliance version of Cisco Secure ACS was made for several reasons:

- **Ease of deployment:** The appliance is shipped preinstalled with Cisco Secure ACS application software, greatly reducing the time it takes to set up and deploy a Cisco Secure ACS solution in your network.
- **Security:** The appliance creates a turnkey security-hardened service that focuses exclusively on running the Cisco Secure ACS service. The appliance provides an ability to remove all extraneous services, block all unused ports, and otherwise prevent all other access to the Cisco Secure ACS system, all of which serve to dramatically increase its security posture.
- **Manageability:** The appliance is a dedicated, exclusive service for authentication, authorization, and accounting (AAA) with no ability to install or run other services or applications. This greatly improves the support and day-to-day management of the Cisco Secure ACS system.
- **Reliability:** By targeting only the OS services required by Cisco Secure ACS, the appliance offers greater operational reliability and security of the Cisco Secure ACS system.
- **Total cost of ownership:** There is considerable benefit to customers choosing the appliance in optimizing cost of ownership. Cisco end-to-end support now includes full support, maintenance, and serviceability of the Cisco Secure ACS system—not just the Cisco Secure ACS software running on various hardware configurations that are supported by various third-party vendors.
- **SNMP support:** The appliance supports Simple Network Management Protocol (SNMP) Version 1 and Version 2c (read only), so that external systems can monitor the appliance. SNMP support includes support for MIB II and Host-Resources MIB.

Q. What additional features are available on Cisco Secure ACS Solution Engine but not available on Cisco Secure ACS for Windows?

A. To help ensure a high security posture for Cisco Secure ACS Solution Engine, additional functions specific to operating and managing the appliance are added:

- Security-hardened underlying OS
- Port-based packet filtering, allowing connections only to the ports necessary for Cisco Secure ACS operation
- Serial console interface for initial configuration, subsequent management of IP connections, Web interface, and application of upgrades and remote reboots. The serial console interface supports both serial line and Telnet connections.
- SNMP read-only support to monitor the appliance from external systems
- Backup/restore of the Cisco Secure ACS data over FTP
- Recovery procedures

- Network Timing Protocol (NTP) support for maintaining network time consistency with other appliances or network devices

Q. What are the differences between Cisco Secure ACS for Windows software and Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine is designed to provide the same features and functions as Cisco Secure ACS for Windows in a dedicated, security-hardened, application-specific appliance package. The appliance includes additional features specific to the operation and management of Cisco Secure ACS Solution Engine; in addition, specific software features needed to be customized or removed due to the different underlying system architectures:

- Authentication
 - Authentication against the Windows domain requires a Cisco Secure ACS remote agent running on a domain controller or member server. The Cisco Secure ACS remote agent is necessary to establish a Windows member or domain controller trust relationship.
 - Authentication against an Open Database Connectivity (ODBC) source is not supported.
 - Authentication against one-time password (OTP) directories is performed using the generic RADIUS-based OTP interface on the appliance. Any OTP vendor that provides an RFC-compliant RADIUS interface can interface with Cisco Secure ACS Solution Engine. Cisco Secure ACS provides native support for RSA and use of the RADIUS interface is not required.
- User database synchronization
 - User database synchronization with an ODBC source is not supported. Instead, the administrator can configure Cisco Secure ACS Solution Engine to synchronize its user database with a comma-separated value (CSV) file on a remote FTP server.
- ODBC logging
 - ODBC logging is not supported. Administrators can alternatively use local or remote CSV logging.
- Backup/restore and appliance diagnostics
 - Backup and restore as well as gathered appliance diagnostics are performed through a remote FTP server and configured using the current Cisco Secure ACS HTML GUI.

Q. What Windows services are run on Cisco Secure ACS Solution Engine?

A. The Cisco Secure ACS Solution Engine runs only the following Windows OS services. These services are automatically started upon appliance power up:

- DHCP Client (only if the appliance is using Dynamic Host Control Protocol [DHCP])
- DNS Client
- Event Log
- IPSec Policy Agent
- License Logging Service
- Logical Disk Manager
- Plug and Play
- Protected Storage
- Remote Procedure Call (RPC)
- Removable Storage

- RunAs Service
- Security Accounts Manager
- Server
- System Event Notification
- Telnet (for console access only)
- Windows Management Instrumentation

The following Windows OS services are not started automatically but can be started manually if required:

- Application Management
- ClipBook
- COM+ Event System
- Distributed Link Tracking Server
- Distributed Transaction Coordinator
- Fax Service
- File Replication
- Indexing Service
- Internet Connection Sharing
- Logical Disk Manager Administrative Service
- Net Logon
- NetMeeting Remote Desktop Sharing
- Network Connections
- Network DDE
- Network DDE DSDM
- NT LM Security Support Provider
- Performance Logs and Alerts
- Print Spooler
- QoS RSVP
- Remote Access Auto Connection Manager
- Remote Procedure Call (RPC) Locator
- Smart Card
- Smart Card Helper
- Uninterruptible Power Supply
- Utility Manager
- Windows Installer
- Windows Management Instrumentation Driver Extensions
- Windows Time

Q. What Windows OS services are disabled on Cisco Secure ACS Solution Engine?

A. The following Windows OS services are disabled on Cisco Secure ACS Solution Engine:

- Alerter

- Automatic Updates
- Background Intelligent Transfer Service
- Computer Browser
- Distributed File System
- Distributed Link Tracking Client
- Intersite Messaging
- Kerberos Key Distribution Center
- Messenger
- Remote Access Connection Manager
- Remote Registry Service
- Routing and Remote Access
- Task Scheduler
- TCP/IP NetBIOS Helper Service
- Telephony API (TAPI)
- Terminal Services
- Windows Media Device Manager Pre-Message Security Protocol (WMDM PMSP) Service
- Workstation

Q. Are there any additions to the existing Cisco Secure ACS GUI to support Cisco Secure ACS Solution Engine?

A. Yes. New pages specific to Cisco Secure ACS Solution Engine have been added to the Cisco Secure ACS GUI. These pages cover specific features related to the operation and management of the appliance and include:

- Appliance configuration page
- Appliance remote agent configuration page
- Appliance upgrade page
- Appliance status page
- Appliance diagnostics log view

Q. What is the hardware platform specification for Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine is a dedicated security-hardened Cisco Secure ACS server in a dedicated, one-rack unit, mountable box with the following configuration:

- Pentium IV (3.4 GHz)
- 1 GB of RAM
- Two built-in 10/100 Ethernet controllers
- 80 GB SATA hard drive
- CD/DVD combo drive

- Q. How does Cisco Secure ACS Solution Engine authenticate to Windows domains?**
- A.** In general, in order to authenticate Windows NT 4.0 or Active Directory domain users, you must establish a Windows member or domain controller trust relationship. Since Cisco Secure ACS Solution Engine does not run the necessary Windows server services to establish this trust, an external Cisco Secure ACS remote agent is provided with the appliance solution. The Cisco Secure ACS remote agent can be installed on member servers, domain controllers, or backup domain controllers. Note: The best practice would be to install the remote agent on a full domain controller — this would allow it to perform its authentication functions with the least extra configuration requirements.
- Q. Why did Cisco build a standalone remote agent for Windows authentication?**
- A.** Without a standalone remote agent, NetBIOS would be required to be installed on Cisco Secure ACS Solution Engine, which would expose Cisco Secure ACS to NetBIOS security vulnerabilities.
- Q. What is the main purpose of the Cisco Secure ACS remote agent?**
- A.** The Cisco Secure ACS remote agent has dual roles. It facilitates authentication against Windows domains and allows remote logging of accounting records.
- Q. What operating systems can the Cisco Secure ACS remote agent be installed on?**
- A.** There are two versions of the Cisco Secure ACS remote agent — a Windows version that can be installed on a Windows server (Windows domain controller or member server supported) and a Solaris version that can be installed on Sun Solaris. Please refer to the Cisco Secure ACS remote agent installation guide for the exact OS versions and service packs supported.
- Q. What are the differences in capabilities between the Windows and Solaris versions for Cisco Secure ACS remote agents?**
- A.** While the Windows version supports both Windows authentication and remote logging, the Solaris version supports only the remote logging capability.
- Q. Can a Cisco Secure ACS remote agent and Cisco Secure ACS for Windows coexist on the same server?**
- A.** No. The Cisco Secure ACS remote agent cannot be installed on a server that already has Cisco Secure ACS for Windows installed.
- Q. Can Cisco Secure ACS Solution Engine be configured to use several remote agents?**
- A.** Yes. Cisco Secure ACS Solution Engine appliance can be configured to use one or more agents. There is no restriction that the same agent be used for Windows services and logging services. For Windows services, an appliance can point to a primary agent and a backup agent, in the event that the primary agent is unavailable.
- Q. Can a Cisco Secure ACS remote agent be shared with multiple appliances?**
- A.** Yes. The Cisco Secure ACS remote agent can be shared with multiple appliances. Cisco will support configurations with up to five appliances sharing a single Cisco Secure ACS remote agent.
- Q. Can I still do local logging on Cisco Secure ACS Solution Engine instead of using the remote logging capability of the Cisco Secure ACS remote agent?**
- A.** Yes. However, local logging on Cisco Secure ACS Solution Engine is constrained in size, forcing log files to be recycled after seven days. The Cisco Secure ACS remote agent provides full, unconstrained logging capability to a remote server.

Q. Are user credentials ever sent in the clear between Cisco Secure ACS Solution Engine and its remote agent for Windows authentication?

A. No. Passwords are never sent in the clear between Cisco Secure ACS Solution Engine and its remote agent. Cisco Secure ACS Solution Engine always converts the plaintext password into the Microsoft version of the Challenge Handshake Authentication Protocol (MS-CHAP) prior to sending the request to the Cisco Secure ACS remote agent. In addition, all communication between a remote agent and Cisco Secure ACS Solution Engine is encrypted, using the Blowfish algorithm and a 128-bit key. Also, encryption session keys are randomized and exchanged between the remote agent and the appliances it services, using a public key exchange protocol.

Q. What ports and protocols are accessing Cisco Secure ACS Solution Engine?

A. Table 1 lists the ports and protocols associated with Cisco Secure ACS Solution Engine.

Table 1. Cisco Secure ACS Ports and Protocols

Service Name	UDP	TCP
DHCP	68	–
RADIUS Authentication and Authorization (original draft RFC)	1645	–
RADIUS Accounting (original draft RFC)	1646	–
RADIUS Authentication and Authorization (revised draft RFC)	1812	–
RADIUS Accounting (revised draft RFC)	1813	–
TACACS+ AAA	–	49
Replication and RDBMS Synchronization	–	2000
Cisco Secure ACS Remote Logging	–	2001
Cisco Secure ACS Distributed Logging (appliance only)	–	2003
HTTP Administrative Access (at login)	–	2002
Administrative Access (after login) Port Range	–	Configurable (default 1024–65535)*

* Cisco Secure ACS assigns a unique port number from the range to each administration session.

Q. What happens with third-party software tools, such as backup services from Legato?

A. Cisco Secure ACS Solution Engine is designed to be a standalone, dedicated box for running Cisco Secure ACS. At present, there are no interfaces or abilities to add third-party software; only Cisco Secure ACS images and patches downloaded over FTP can be added. For Cisco Secure ACS backup, Cisco will create an export file that is automatically exported to an external FTP server. Backup tools can be installed and used to back up the external server.

Q. Can I run Cisco Secure ACS in “mixed mode” (for example, run instances of Cisco Secure ACS for Windows and additional instances of the Cisco Secure ACS Solution Engine)?

A. Yes. Cisco supports environments using both Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine.

Q. How is Cisco Secure ACS replication affected with the introduction of Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS replication will remain unchanged with the introduction of Cisco Secure ACS Solution Engine. Replication between Cisco Secure ACS Solution Engine and Cisco Secure ACS for Windows, as well as replication among the appliances, will be supported with no impact on any of the appliance- or Windows-specific configurations.

Q. Is there any restriction on whether Cisco Secure ACS for Windows or Cisco Secure ACS Solution Engine needs to be a master in a replicated configuration?

A. No. Either Cisco Secure ACS for Windows or Cisco Secure ACS Solution Engine can be the master databases replicating to Cisco Secure ACS for Windows slaves, Cisco Secure ACS Solution Engine slaves, or both Windows and appliance slaves at the same time.

Q. Are there any changes to single logon and password aging capabilities in Cisco Secure ACS Solution Engine?

A. No. With the appropriate Windows or domain controller, trust relationships established with the Cisco Secure ACS remote agent and single logon and password aging capabilities remain unchanged from Cisco Secure ACS for Windows.

Q. Why does Cisco Secure ACS use an embedded, proprietary Web server and not Microsoft Internet Information Services (IIS) or Apache?

A. The Cisco Secure ACS dedicated Web server is simpler in nature than IIS or Apache. Because of its targeted usage with only the Cisco Secure ACS service, the Web server is less at risk of security vulnerability compared to other widely used Web servers.

Q. How scalable is an appliance-based Cisco Secure ACS server?

A. An appliance-based Cisco Secure ACS server follows at a minimum the same scalability performance of a Windows-based Cisco Secure ACS server. Cisco Secure ACS guidelines and performance analysis show that each ACS server can support anywhere from 20,000 to 80,000 users per server and can scale to support up to 35,000 devices, depending on configuration, platform, and usage scenarios. The real challenge in scaling a user access control framework is on the back end. Linked to a high-performance back-end database such as Oracle or Sybase, Cisco has deployed Cisco Secure ACS for Windows in clustered deployments into customers with hundreds of thousands of user records.

Q. What Cisco Secure ACS Solution Engine features enhance Cisco Secure ACS reliability and remote management?

A. The operating system is configured to reboot automatically on system crash. In addition, the serial console service is configured to restart automatically if it fails. Cisco Secure ACS software implements the monitor that restarts Cisco Secure ACS services if they fail. Cisco Secure ACS Solution Engine also provides a remote administrator command-line interface (CLI). The CLI supports both serial line and Telnet connections, and the Cisco Secure ACS service can be reimaged, reloaded, upgraded, and rebooted from the CLI remotely.

Q. What support is there for Lightweight Directory Access Protocol?

A. Support for LDAP on Cisco Secure ACS Solution Engine is identical to support on the Cisco Secure ACS software version. Cisco Secure ACS supports user authentication against records kept in a directory server through LDAP. Cisco Secure ACS supports the most popular directory servers, including Novell and Netscape, through a generic LDAP interface. Password Authentication Protocol (PAP) passwords can be used when authenticating against the directory server. In addition, Cisco Secure ACS also supports the Active Directory Service (ADS) in Windows 2000/2003. For more information on Microsoft ADS, see your Microsoft documentation. Cisco Secure ACS also has the ability to define multiple, different LDAP sources for user lookups. This lets you define a different LDAP repository to search for users. In addition, users are able to define secondary, backup LDAP servers, such that after timeouts against a primary LDAP repository, Cisco Secure ACS can search against secondary and backup sources.

Q. Will Cisco Secure ACS Solution Engine allow “single login” for Windows networking?

A. Yes. Cisco Secure ACS Solution Engine can be set up such that a user will need to enter a user name and password only once, also known as “single login.” The Cisco Secure ACS remote agent must be installed on a Windows network server with the necessary trust relationships to the domain defined.

Q. Does Cisco Secure ACS support OTP and token systems such as RSA’s SecurID tokens?

A. Yes. Cisco Secure ACS can be configured to communicate with token solutions from ActiveCard, Cryptocard, PassGo Technologies, RSA Data Security, Secure Computing, and Vasco. Cisco Secure ACS Solution Engine includes a generic RADIUS interface for expanding OTP coverage to new vendors. Any OTP products for which the vendor provides an RFC-compliant RADIUS interface should work with Cisco Secure ACS Solution Engine.

Q. How is Cisco Secure ACS Solution Engine software licensed?

A. Cisco Secure ACS Solution Engine appliance software is licensed per server, with unlimited ports, users, and network access servers. The following appliance packages will be available for ordering. For exact part numbers, refer to the Cisco Secure ACS 4.2 product bulletin at <http://www.cisco.com/go/acs>.

Q. Does Cisco support migration from Cisco Secure ACS for UNIX to Cisco Secure ACS Solution Engine?

A. No. At this time, no automatic migration mechanism is available.

Q. Can I purchase or license a backup Cisco Secure ACS Solution Engine server?

A. No. An additional Cisco Secure ACS Solution Engine server must be purchased as a separate Cisco Secure ACS server license to be used for recovery/backup purposes. Cisco Secure ACS servers can be run in a recovery or failover server configuration. Because Cisco Secure ACS is a central control service in your network, Cisco highly recommends that customers configure a backup server for failover and recovery.

Q. Do I need to patch the appliance with newer operating system releases or patches?

A. No. All OS software updates and patches are handled by the Cisco Secure ACS Solution Engine upgrades performed by Cisco.

Q. Where can I find end of life and end of support information?

A. You can find that information at http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_eol_notices_list.html.

Q. How can I obtain a demo of Cisco Secure ACS Solution Engine?

A. Please contact your assigned Cisco account manager, who will be able to arrange for a demonstration version Cisco Secure ACS Solution Engine to be delivered for a limited time.

For More Information

For additional product information, please visit <http://www.cisco.com/go/acs>. For additional information contact your local Cisco account representative.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

Printed in USA

C67-453393-01 07/08