

Cisco Secure Access Control Server 4.2 for Windows

Overview

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

A. Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized RADIUS or TACACS+ server system and controls the authentication, authorization, and accounting (AAA) of users who access corporate resources through a network. Cisco Secure ACS allows you to control user access to the network, authorize different types of network services for users or groups of users, and keep a record of all network user actions. Cisco Secure ACS supports access control and accounting for dialup access servers, cable and DSL broadband solutions, firewalls, VPNs, voice-over-IP (VoIP) solutions, storage, and switched and wireless LANs. In addition, network managers can use the same AAA framework to manage (through TACACS+) administrative roles and groups and control how they change, access, and configure the network internally. Cisco Secure ACS for Windows runs on Windows 2003.

Q. Why do I need Cisco Secure ACS?

A. Changing network dynamics and increased security threats have created new demands in access control management. As AAA becomes more available throughout the network through new technologies such as IEEE 802.1x and the requirements to control user access expand, new trends emerge that require identity networking to be pervasive throughout the network. Cisco Secure ACS extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking solution. This allows greater flexibility and mobility, increased security, and user productivity gains.

Q. Is Cisco Secure ACS a software or a hardware product?

A. Cisco Secure ACS is offered as Cisco Secure ACS for Windows — software for installation on Windows servers, and as the Cisco Secure ACS Solution Engine — a 1-rack-unit (1RU) appliance with a preinstalled Cisco Secure ACS license.

Q. What is the difference between Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine provides the same features and functions as Cisco Secure ACS for Windows in a dedicated, security-hardened, application-specific appliance package along with additional features specific to the operation and management of Cisco Secure ACS Solution Engine. For more information, refer to the [Cisco Secure ACS Solution Engine Q&A](#).

Q. Should I purchase Cisco Secure ACS for Windows or Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS for Windows is suitable for customers who prefer to control their operating environment (this may include the type of hardware servers, OS, and installed services). In many cases, where security operations and server/OS operations are different departments in an IT organization, having a security solution in a dedicated appliance facilitates the manageability. In addition, the appliance solution provides benefits such as enhanced security, one-stop support, and a “plug-and-play” solution.

Device Support

Q. What network access gateways does Cisco Secure ACS support?

A. Cisco Secure ACS supports a broad set of networking access products, including all Cisco IOS[®] routers, VPN access products, VoIP solutions, cable broadband access, content networks, wireless solutions, storage networks, and 802.1x-enabled Cisco Catalyst[®] switches. As a fully standards-compliant RADIUS and TACACS+ server, Cisco Secure ACS also works with a range of third-party access- and device-management consoles that support either RADIUS or TACACS+.

New Features and Protocol Support

Q. What are the new features in Cisco Secure ACS 4.2?

A. Cisco Secure ACS 4.2 adds the following features:

- Extensive Authentication Protocol (EAP) 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 when using 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 for Windows also now supports comma-separated value (CSV)-based RDBMS synchronization.
- NetBIOS disabling: ACS for Windows allows NetBIOS to be disabled on the server it is running on.

Please refer to the product release notes at

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html for a complete list of new and changed features.

Q. With an EAP-type authentication, which user databases can I use with Cisco Secure ACS?

- A.** Depending on the EAP authentication type used, Cisco Secure ACS supports an extended range of user databases, as highlighted in Table 1.

Table 1. User Database-to-EAP Compatibility Support Matrix

Databases	LEAP	EAP-MD5	EAP-TLS	PEAP (EAP-GTC)	PEAP (EAP-MSCHAP v2)	EAP-FAST (Phase 0)	EAP-FAST (Phase 2)
Cisco Secure ACS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows	Yes	No	Yes	Yes	Yes	Yes	Yes
Active Directory	-	-	-	-	-	-	-
LDAP	No	No	Yes	Yes	No	No	Yes
Novell NDS	No	No	No	Yes	No	No	Yes
Open Database Connectivity (ODBC)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LEAP proxy RADIUS server	Yes	No	No	Yes	Yes	Yes	Yes
All token servers	No	No	No	Yes	No	No	No

Q. What support does Cisco Secure ACS provide for LDAP?

- A.** 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 Sun LDAP servers, through a generic LDAP interface. Password Authentication Protocol passwords can be used when authenticating against the directory server.

In addition, Cisco Secure ACS supports the Active Directory Service in Windows 2003. Cisco Secure ACS can process multiple LDAP authentication requests in parallel as opposed to sequential processing. This feature greatly improves Cisco Secure ACS 4.2 performance in task-intensive applications such as wireless deployments. For more information about LDAP, see the white paper “Configuring LDAP for Cisco Secure ACS,” which is available at http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_white_papers_list.html.

Q. Does Cisco Secure ACS support One-Time Password (OTP) and token systems such as RSA SecurID tokens?

- A.** Yes. Cisco Secure ACS can be configured to communicate with token solutions from ActivCard, Cryptocard, PassGo Technologies, RSA Data Security, Secure Computing, and Vasco. Cisco Secure ACS includes a generic RADIUS interface for expanding OTP coverage to new vendors. Any OTP vendor that provides an RFC-compliant RADIUS interface should work with Cisco Secure ACS. The token authentication server can be installed on any operating system — Windows NT, NetWare, or UNIX.

Q. What ports and protocols does Cisco Secure ACS use?

- A.** Cisco Secure ACS uses the TCP/User Datagram Protocol (UDP) ports listed in Table 2.

Table 2. Cisco Secure ACS Port Usage

Service Name	UDP	TCP
Dynamic Host Configuration Protocol (DHCP)	68	–
RADIUS Authentication and Authorization (Original Draft RFC)	1645	–
RADIUS Accounting (Original Draft RFC)	1646	–

RADIUS Authentication and Authorization (Revised RFC)	1812	–
RADIUS Accounting (Original Draft RFC)	1813	–
TACACS+ AAA	–	49
Replication and Relational Database Management Synchronization	–	2000
Cisco Secure ACS Remote Logging	–	2001
HTTP Administrative Access (at Login)	–	2002
Cisco Secure ACS Distributed Logging (Appliance Only)	–	2003
Administrative Access (after Login) Port Range	–	1024
Configurable Default	–	65,535

Q. What should be the security context of a Cisco Secure ACS server running on a member server to help ensure proper Windows authentication to a domain controller?

A. The security context is defined by the local service account. See the Cisco Secure ACS installation guide for guidelines on setting the requisite privileges for running Cisco Secure ACS on a member server and performing Windows authentication.

Q. Can Cisco Secure ACS service TACACS+ and RADIUS requests at the same time?

A. Yes.

Q. How are user passwords stored in Cisco Secure ACS?

A. For users who are authenticated by using the ACS internal database, ACS stores user passwords in a database which is protected by an administration password and encrypted by using the AES 128 algorithm. For users who are authenticated with external user databases, ACS does not store passwords in the ACS internal database.

Q. Does Cisco Secure ACS support forced password change based on password age and other criteria?

A. Password aging is available for users in the ACS internal database and users in a Microsoft Windows Active Directory database.

Q. Does Cisco Secure ACS for Windows have to be installed only on a Microsoft Windows domain controller?

A. No. Cisco Secure ACS can be installed on a Windows 2000/2003 server that is not a domain controller. It can still be configured to authenticate Windows users against a Windows database such as Microsoft Windows Active Directory.

Q. What is the licensing for Cisco Secure ACS 4.2?

A. The Cisco Secure ACS product is licensed per server, with unlimited ports, users, and network access servers. For available part numbers and descriptions, refer to the Cisco Secure ACS 4.2 product bulletin at <http://www.cisco.com/go/acs>.

Scalability

Q. How scalable is a Cisco Secure ACS solution?

A. Although many customers perceive that high-scale access servers need to run on UNIX platforms, this is not the case with Cisco Secure ACS. Cisco Secure ACS guidelines and performance analysis show that each copy of Cisco Secure ACS for Windows can support from 10,000 to 300,000 users per server and in excess of 35,000 devices, depending on configuration, platform, and use scenarios. The primary 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 2003 clustered deployments for customers with hundreds of thousands of user records.

Q. Is there any limit on the number of user domains a single copy of Cisco Secure ACS can handle?

A. No. There is no hardware limitation on the number of user domains a copy of Cisco Secure ACS can handle.

Q. What patches are tested with Cisco Secure ACS for Windows?

A. Cisco officially supports and encourages the installation of all Microsoft security patches for Windows 2000 Server and Windows Server 2003 as used for Cisco Secure ACS for Windows. Our experience has shown that these patches do not cause any problems with the operation of Cisco Secure ACS for Windows. If the installation of one of these security patches does cause a problem with Cisco Secure ACS, please contact the Cisco Technical Assistance Center (TAC), and Cisco will provide full support for the resolution of the problem as quickly as possible.

Q. In a large distributed environment with several hundred user domains, what is the best Cisco Secure ACS deployment practice to avoid authentication timeouts?

A. The main factor that can affect authentication timeout is where a Cisco Secure ACS server is located with respect to where the users reside (that is, location of the domain controllers). Increasing your AAA client timeouts at the device level is one option to resolve longer responses from Cisco Secure ACS. If this is not feasible, other options such as providing domain names (during authentication) or locating the Cisco Secure ACS closer to user domains are possible options.

Ordering Information

Q. How do I order Cisco Secure ACS 4.2 for Windows?

A. If you are a new customer of Cisco Secure ACS with no previous version installed in your network, purchase part number CSACS-4.2-WIN-K9. For Cisco Secure ACS 4.1 customers, 4.2 is a minor release, and the upgrade will be covered by the Software Application Support (SAS) contract.

If you are a current Cisco Secure ACS customer with Cisco Secure ACS 1.x, 2.x, or 3.x for Windows, purchase part number CSACS-4.2-WINUP-K9.

Q. Are evaluation copies of Cisco Secure ACS for Windows available?

A. Yes. You can download a 90-day trial version of Cisco Secure ACS from <http://www.cisco.com/go/acs>. Customers are encouraged to work with a Cisco sales representative if they would like to order a copy of the evaluation.

Q. When I move from the 90-day trial version to the full, commercial version of Cisco Secure ACS for Windows, do I have to uninstall the trial version?

A. No. You can easily upgrade to the full, commercial version from the trial version without uninstalling the trial version. All configuration settings, user data, and device data entered into the trial database will be maintained.

Q. Is training available for Cisco Secure ACS?

A. Yes. Information on instructor led training for ACS is available at <http://www.cisco.com/go/ndm>

For More Information

For more information about Cisco Secure ACS, contact your local account representative or visit <http://www.cisco.com/go/acs>.



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, CCVP, Cisco Eos, 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, 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, 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. (0801R)