

Cisco Secure Access Control Server 4.2

Cisco® Secure Access Control Server (ACS) provides a comprehensive, identity-based access policy system for Cisco intelligent information networks. It is the integration and control platform for managing access policy for network resources.

Cisco Secure ACS provides central management of access policies for both network access and device administration and supports a wide range of access scenarios including wireless LAN, 802.1x wired, and remote access. Cisco Secure ACS is the leading authentication, authorization, and accounting (AAA) platform in the market and is deployed by 90 percent of the top 500 Cisco customers. Cisco Secure ACS is available as a rack-mountable, dedicated appliance—Cisco Secure ACS Solution Engine—or as software that runs on Windows platforms, Cisco Secure ACS for Windows.

Product Overview

With the ever-increasing number of methods and opportunities for accessing networks today, security breaches and uncontrolled user access are of primary concern among enterprises. While the wide deployment of wireless LANs and remote access have increased security challenges at the perimeter, security risks inside the enterprise exist as well. Identity networking technologies such as 802.1x that can mitigate both internal and external security vulnerabilities have become of prime interest to customers worldwide. Network security officers and administrators need solutions that support flexible authentication and authorization policies that are tied to the user identity as well as context such as the network access type and the security of the machine used to access the network. Further, there is a need to audit network use and monitor corporate compliance.

Cisco Secure ACS is a highly scalable, high-performance access policy system that centralizes authentication, user access, and administrator access policy and reduces the administrative and management burden. Cisco Secure ACS is a central point for administering security policy for users and devices accessing the network. Cisco Secure ACS supports multiple and concurrent access scenarios including:

- **Device administration:** Cisco Secure ACS authenticates network administrators, authorizes commands, and provides an audit trail.
- **Remote Access:** Cisco Secure ACS works with VPN and other remote network access devices to enforce access policies.
- **Wireless:** Cisco Secure ACS authenticates and authorizes wireless users and hosts and enforces wireless-specific policies.
- **802.1x LAN:** Cisco Secure ACS supports dynamic provisioning of VLANs and access control lists (ACLs) on a per user basis and 802.1x with port-based security.
- **Network admission control:** Cisco Secure ACS communicates with posture and audit servers to enforce admission control policies.

Features and Benefits

Cisco Secure ACS is a powerful access policy system with management and scalability features for the growing organization. Table 1 lists the key features and benefits of Cisco Secure ACS 4.2.

Table 1. Key Features and Benefits of Cisco Secure ACS 4.2

Feature	Benefit
AAA protocols	Cisco Secure ACS supports two distinct protocols for authentication, authorization, and accounting (AAA). Cisco Secure ACS supports both RADIUS and TACACS+ for the concurrent support of network access and network device access control. Cisco Secure ACS is a single system for enforcing access policy.
Database options	Cisco Secure ACS provides an onboard database while supporting Windows Active Directory, Lightweight Directory Access Protocol (LDAP), and Open Database Connectivity (ODBC) for integration with existing user databases. Support for RSA SecurID Authentication Manager and RADIUS-enabled token servers allows integration with strong authentication systems. Multiple databases can be used concurrently for maximum flexibility in enforcing access policy.
Authentication protocols	Cisco Secure ACS supports a wide range of authentication protocols including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, EAP-Generic Token Card (GTC), Cisco LEAP, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), and EAP-Transport Layer Security (TLS) to support all your authentication requirements.
Network access policies	Cisco Secure ACS allows the configuration of complex network access policies that may include authentication protocol requirements, device restrictions, time of day restrictions, posture validation, and other access requirements. Cisco Secure ACS may apply downloadable access control lists (dACLs), VLAN assignments, and other authorization parameters.
Centralized configuration management	Cisco Secure ACS replication allows administrator-defined configuration items to be replicated across ACS servers in the network, providing both flexibility and ease of administration for large networks. Provisioning is facilitated through a secure, web-based GUI, command-line interface (CLI), and relational database management system (RDBMS) synchronization to allow Cisco Secure ACS to fit in your workflow.
Logging	Cisco Secure ACS logs are viewable and exportable for use in other systems. Cisco Secure ACS logs support troubleshooting and diagnostics, compliance and auditing, and other reporting and billing activities.
Platform options	Cisco Secure ACS is available as a closed and hardened appliance or as Windows Server software for customers with existing practices for server/OS management. Cisco Secure ACS for Windows may be used with VMWare ESX Server for customers deploying virtual servers.

System Requirements

Cisco Secure ACS is available as Cisco Secure ACS for Windows and as the Cisco Secure ACS Solution Engine—a one-rack-unit (1RU), security-hardened appliance with a preinstalled Cisco Secure ACS license. Table 2 lists the specifications of Cisco Secure ACS Solution Engine 4.2.

Table 2. Cisco Secure ACS Solution Engine 4.2 Specifications

Component	Specifications
CPU	3.4 GHz Intel Pentium 4, 800 MHz FSB, 2 MB cache
System memory	1GB
Hard disk drive	160 GB SATA
Media	CD/DVD combo
I/O ports	RS232 Serial Port, 3 USB 2.0 (1 front, 2 rear)
Physical dimensions (1RU)	<ul style="list-style-type: none"> • 429 (W) x 508 (D) x 42 (H) mm • 16.9 (W) x 20 (D) x 1.67 (H) in.
Rated input power	345W

Table 3. Minimum Server Specifications for Cisco Secure ACS 4.2 for Windows

Specification	Minimum Requirement
Processor speed	Pentium IV processor, 1.8 GHz or faster
Memory	Minimum 1 GB RAM
Virtual memory	Minimum 1 GB
Hard drive	At least 1 GB of free hard drive space

Specification	Minimum Requirement
Operating system	<ul style="list-style-type: none"> • Windows Server 2008, Enterprise Edition or Standard Edition (English Version only) • Windows Server 2003 Service Pack 1, Enterprise Edition or Standard Edition (English Version only) • Japanese Windows Server 2003, Service Pack 1 • Windows Server 2003, R2, Standard Edition • Windows Server 2003, Service Pack 2 • Windows Server 2003, R2, Service Pack 2
Resolution	Minimum of 800 x 600 (256 colors)

Ordering Information

Cisco Secure ACS products are available for purchase through regular Cisco sales and distribution channels worldwide. Please refer to the Cisco Secure ACS 4.2 product bulletins for Cisco Secure ACS product numbers at http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_bulletins_list.html.

To place an order, visit the [Cisco Ordering Home Page](#).

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, see [Cisco Technical Support Services](#).

For More Information

For more information about Cisco Secure ACS products please visit <http://www.cisco.com/go/acs> or email the product marketing team at acs-mkt@cisco.com

For questions about product ordering and availability and for support contract information, please contact your local 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, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; 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, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, 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. (0907R)