# Cisco Secure Access Control Server 4.1

Cisco® Secure Access Control Server (ACS) provides a comprehensive, identity-based access control solution for Cisco intelligent information networks. It is the integration and control layer for managing enterprise network users, administrators, and the resources of the network infrastructure.

Cisco Secure ACS is available as a rack-mountable, dedicated appliance—Cisco Secure ACS Solution Engine—or as software that runs on Windows 2000 and 2003 platforms, Cisco Secure ACS for Windows. Both products provide secure, industry-leading authentication, authorization, and accounting (AAA) services to enterprises.

## Product Overview

With an ever-increasing number of methods for accessing networks today, security breaches and uncontrolled user access are of primary concern among enterprises. With the wide adoption of IEEE 802.11 wireless LANs and ubiquitous broadband Internet connections, security challenges exist not only at the perimeter, but also inside a network. Identity networking technologies that can mitigate these security vulnerabilities have become of prime interest to customers worldwide.

Stronger forms of authentication, such as public key infrastructure (PKI) and one-time passwords (OTPs), are increasingly used to control user access to corporate resources from public networks. Network administrators look for solutions that provide flexible authorization policies that are tied to the user identity, as well as to the network access type and the security of the machine used to access the network. Lastly, the ability to centrally track and monitor the connectivity of network users is of primary importance in isolating unwanted and excessive use of valuable network resources.

Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized RADIUS and TACACS+ server. It extends access security by combining authentication, user access, and administrator access with policy control within a centralized identity networking solution, allowing greater flexibility and mobility, increased security, and user-productivity gains. It enforces a uniform security policy for all users regardless of how they access the network. It reduces the administrative and management burden involved in scaling user and network administrator access to the network. By using a central database for all user accounts, Cisco Secure ACS centralizes the control of all user privileges and distributes them to hundreds or thousands of access points throughout the network. As an accounting service, Cisco Secure ACS provides detailed reporting and monitoring capabilities of network users' behavior and keeps a record of every access connection and device configuration change across the entire network. This feature has become extremely important for organizations in complying with Sarbanes-Oxley Act regulations. Cisco Secure ACS supports a broad variety of access connections, including wired and wireless LAN, dialup, broadband, content, storage, voice over IP (VoIP), firewalls, and VPNs.

Cisco Secure ACS is an important component of the Cisco Identity-Based Networking Services (IBNS) architecture. Cisco IBNS is based on port-security standards such as 802.1x (an IEEE standard for port-based network access control) and Extensible Authentication Protocol (EAP),

and extends security authentication, authorization, and accounting (AAA) from the perimeter of the network to every connection point inside the LAN. New policy controls (such as per-user quotas, VLAN assignments, and access-control lists [ACLs]) can be deployed within this new architecture, because of the extended capabilities of Cisco switches and wireless access points to query Cisco Secure ACS over the RADIUS protocol.

Cisco Secure ACS is also an important component of Cisco Network Admission Control (NAC). Cisco NAC is an industry initiative sponsored by Cisco that uses the network infrastructure to enforce security-policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms. With NAC, customers can choose to allow network access only to compliant and trusted endpoint devices (for instance, PCs, servers, and personal digital assistants) and can restrict the access of noncompliant devices. Cisco NAC is part of the Cisco Self-Defending Network initiative and is the foundation for enabling network admission control on Layer 2 and Layer 3 networks. Future phases extend endpoint and network security interoperation to include dynamic incident-containment capabilities. This innovation enables compliant system elements to report misuse emanating from rogue or infected systems during an attack. Thus, infected systems can be dynamically quarantined from the rest of the network to significantly reduce virus, worm, and blended threat propagation.

Cisco Secure ACS is a powerful access control server with many high-performance and scalability features for any organization growing its WAN or LAN. Table 1 lists the main benefits of Cisco Secure ACS.

**Table 1.** Main Cisco Secure ACS Benefits

| Benefit | Description |
|---|---|
| **Ease of Use** | A Web-based user interface simplifies and distributes configuration for user profiles, group profiles, and Cisco Secure ACS configuration. |
| **Scalability** | Cisco Secure ACS is built to support large networked environments with support for redundant servers, remote databases, and database replication and backup services. |
| **Extensibility** | Lightweight Directory Access Protocol (LDAP) authentication forwarding supports the authentication of user profiles stored in directories from leading directory vendors, including Sun, Novell, and Microsoft. |
| **Management** | Windows Active Directory support consolidates Windows user name and password management and uses the Windows Performance Monitor for real-time statistics viewing. |
| **Administration** | Different access levels for each Cisco Secure ACS administrator-and the ability to group network devices-enable easier control and maximum flexibility to facilitate enforcement and changes of security policy administration over all the devices in a network. |
| **Product Flexibility** | Because Cisco IOS® Software has embedded support for AAA, Cisco Secure ACS can be used across virtually any network access server that Cisco sells (the Cisco IOS Software release must support RADIUS or TACACS+).<br>Cisco Secure ACS is available in two options: Cisco Secure ACS Solution Engine, a rack-mountable, security-hardened appliance and Cisco Secure ACS for Windows, a scalable and feature-rich software that runs on Windows platform |
| **Integration** | Tight coupling with Cisco IOS routers and VPN solutions provides features such as Multichassis Multilink Point-to-Point Protocol (PPP) and Cisco IOS Software command authorization. |
| **Third-Party Support** | Cisco Secure ACS offers token server support for any OTP vendor that provides an RFC-compliant RADIUS interface (such as RSA, PassGo, Secure Computing, ActiveCard, Vasco, or CryptoCard). |
| **Control** | Cisco Secure ACS provides dynamic quotas for time-of-day, network use, number of logged sessions, and day-of-week access restrictions. |

## Features and Benefits

Cisco Secure ACS 4.1 provides the following new features and benefits:

- Regulatory compliance support—Cisco Secure ACS 4.1 addresses the increased concern about compliance with the Sarbanes-Oxley Act. Release 4.1 supports compliance features

associated with Cisco Secure ACS administrator permission and audit reports. The features include:

- Administrative constraints on log settings— Restricts administrators from disabling certain types of logging.
- Forced administrator password change at logon—Prompts the administrators to change the password at configurable time intervals.
- Administrator password policy—Provides a mechanism to enforce a configurable minimum password length and mix of characters (upper/lower case, numeric, punctuation).
- Forced administrator password change for stale account—Enforces password change when the administrator has not logged on in a specified number of days.
- Generation of entitlement reports—Provides a report that will show all administrator privileges.
- Password history for administrators—Prevents administrators from reusing passwords.

- Syslog support—Provides the native syslog support to log data out of Cisco Secure ACS. Supports standard Cisco syslog format and will integrate with Cisco Security Monitoring, Analysis, and Monitoring System (MARS).
- External database MAC authentication bypass—Supports the use of external LDAP database for authentication based on MAC address. This functionality is an enhancement from current internal database MAC authentication bypass support.
- Protected Extensible Authentication Protocol (PEAP) with Extensible Authentication Protocol Transport Layer Security (EAP-TLS)—Enables certificate-based authentication to occur within a secure tunnel.
- Support for Japanese version of Windows—The Cisco Technical Assistance Center (TAC) will officially support Cisco Secure ACS on Japanese Windows.

## System Requirements

Cisco Secure ACS is available as Cisco Secure ACS for Windows and the Cisco Secure ACS Solution Engine—a 1-rack-unit (RU), security-hardened appliance with a preinstalled Cisco Secure ACS license. Table 2 lists the specifications of Cisco Secure ACS Solution Engine 4.1.

**Table 2.** Cisco Secure ACS Solution Engine 4.1 Specifications

| CPU | 3.4 GHz Intel Pentium 4, 800 MHz FSB, 2 MB cache |
|---|---|
| **System Memory** | 1GB |
| **HDD** | 80 GB SATA |
| **Media** | CD/DVD combo |
| **I/O Ports** | RS232 Serial Port, 3 USB 2.0 (1 front, 2 rear) |
| **Physical Dimensions (1RU)** | • 429 (W) x 508 (D) x 42 (H) mm<br>• 16.9 (W) x 20 (D) x 1.67 (H) in. |
| **Rated Input Power** | 345W |

For implementation of Cisco Secure ACS 4.1 for Windows, your Windows server must meet the minimum hardware requirements listed in Table 3.

**Table 3.** Minimum Server Specifications for Cisco Secure ACS 4.1 for Windows

| Specification | Minimum Requirement |
|---|---|
| **Processor Speed** | Pentium IV processor, 1.8 GHz or faster |
| **Memory** | Minimum 1 GB RAM |
| **Hard Drive** | Minimum 250 MB free disk space |
| **Operating System** | • Windows 2000 Server<br>• Windows 2000 Advanced Server without features specific to Windows 2000 Advanced Server enabled or without Microsoft clustering service installed<br>• Windows Server 2003, Enterprise Edition or Standard Edition |
| **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 4.1 product bulletins for Cisco Secure ACS product numbers.

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, including the user guide and release notes, please visit http://www.cisco.com/go/acs.

For questions about product ordering, availability, and support contract information please contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.**



Printed in USA

C78-378331-00 12/06