

Cisco Secure Access Control System 5.2

Cisco® Secure Access Control System (ACS) ties together an enterprise's network access policy and identity strategy. Cisco Secure ACS is the world's most trusted enterprise access and policy platform, deployed by 80 percent of Fortune 500 companies.

A core component of the Cisco TrustSec solution, Cisco Secure ACS 5.2 is a next-generation policy platform providing RADIUS and TACACS+ services. It supports the increasingly complex policies needed to meet today's new demands for access control management and compliance. Cisco Secure ACS provides central management of access policies for device administration and wireless and wired 802.1x network access scenarios.

Figure 1. Cisco 1121 Secure Access Control System



Product Overview

With the ever-increasing reliance on enterprise networks to perform daily job routines and the increasing number of methods and opportunities to access today's networks, security breaches and uncontrolled user access are of primary concern among enterprises. Network security officers and administrators need solutions that support flexible authentication and authorization policies that are tied to a user's identity as well as to context such as the network access type, time of day, and the security of the machine used to access the network. Further, there is a need to effectively audit network use, monitor corporate compliance, and get broad visibility into policies and activities across the network.

Cisco Secure ACS provides the policy control for the Cisco Self Defending Network architecture, an architecture that protects your business by identifying, preventing, and adapting to threats from inside and outside the company. Cisco Secure ACS is a highly scalable, high-performance access policy system that centralizes device administration, authentication, and user access policy and reduces the management and support burden for these functions.

Features and Benefits

Cisco Secure ACS 5.2 is the third release of this next-generation network identity and access solution. This release establishes Cisco Secure ACS as a Policy Administration Point (PAP) and Policy Decision Point (PDP) for policy-based access control. Release 5.2 offers additional capabilities, including:

- A powerful, attribute-driven rules-based policy model that addresses complex policy needs in a flexible manner
- A lightweight, web-based graphical user interface (GUI) with intuitive navigation and workflow

- Industry unique, flexible and granular device administration with full auditing and reporting capabilities as required for standards compliance
- Integrated advanced monitoring, reporting, and troubleshooting capabilities for maximum control and visibility
- Improved integration with external identity and policy databases, including Windows Active Directory and Lightweight Directory Access Protocol (LDAP)-accessible databases, simplifying policy configuration and maintenance
- A distributed deployment model that enables large-scale deployments and provides a highly available solution

The Cisco Secure ACS 5.2 rules-based policy model supports the application of different authorization rules under different conditions, and thus policy is contextual and not limited to authorization determined by a single group membership. New integration capabilities allow information in external databases to be directly referenced in access policy rules, and attributes can be used both in policy conditions and authorization rules.

Cisco Secure ACS 5.2 features centralized collection and reporting for activity and system health information for full manageability of distributed deployments. It supports proactive operations such as monitoring and diagnostics, and reactive operations such as reporting and troubleshooting. Advanced features include a deploymentwide session monitor, threshold-based notifications, entitlement reports, and diagnostic tools.

Table 1 lists the key features and benefits of Cisco Secure ACS 5.2.

Table 1. Key Features and Benefits of Cisco Secure ACS 5.2

Feature	Benefit
Complete Access Control and Confidentiality Solution	Can be deployed with other Cisco TrustSec components - including policy components, infrastructure enforcement components, endpoint components, and professional services - for a comprehensive access control and confidentiality solution.
AAA protocols	Cisco Secure ACS 5.2 supports two distinct protocols for authentication, authorization, and accounting (AAA). Cisco Secure ACS 5.2 supports RADIUS for network access control and TACACS+ for network device access control. Cisco Secure ACS is a single system for enforcing access policy across the network as well as network device configuration and change management as required for standards compliance such as PCI compliance.
Database options	Cisco Secure ACS 5.2 supports an integrated user repository in addition to supporting integration with existing external identity repositories such as Windows Active Directory and LDAP. Multiple databases can be used concurrently for maximum flexibility in enforcing access policy.
Authentication protocols	Cisco Secure ACS 5.2 supports a wide range of authentication protocols including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), and EAP-Transport Layer Security (TLS) to support your authentication requirements.
Access policies	Cisco Secure ACS 5.2 supports a rules-based, attribute-driven policy model that provides greatly increased power and flexibility for access control 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 management	Cisco Secure ACS 5.2 supports a completely redesigned lightweight, web-based GUI that is easy to use. An efficient, incremental replication scheme quickly propagates changes from primary to secondary systems providing centralized control over distributed deployments. Software upgrades are also managed through the GUI and can be distributed by the primary system to secondary instances.
Monitoring and troubleshooting	Cisco Secure ACS 5.2 includes an integrated monitoring, reporting, and troubleshooting component that is accessible through the web-based GUI. This tool provides maximum visibility into configured policies and authentication and authorization activities across the network. Logs are viewable and exportable for use in other systems as well.
Platform options	Cisco Secure ACS 5.2 is available as a closed and hardened Linux-based appliance or as a software operating system image for VMware ESX.
FIPS 140-2 certified	Meets deployment requirements for federal customers and agencies.

System Requirements

Cisco Secure ACS 5.2 is available as a one rack-unit (1-RU), security-hardened, Linux-based appliance with preinstalled Cisco Secure ACS software or as a software operating system image for installation in a virtual machine on VMware ESX 3.5 or ESX 4.0. Table 2 lists the system specifications for the Cisco 1121 Secure ACS 5.2 Appliance. For VMware ESX system requirements, please review Table 3.

Table 2. Cisco 1121 Secure ACS 5.2 Appliance Specifications

Component	Specifications
CPU	Intel Xeon 2.66-GHz Q9400 (Quad Core)
System memory	4 GB DDR II ECC
Hard disk drive	2 x 250 GB 7.2K RPM 3.5" SATA
Optical storage	DVD-ROM
Network connectivity	4 10/100/1000, RJ-45 interfaces
I/O ports	1 serial port, 4 USB 2.0 (2 front, 2 rear), SVGA Video
Rack-mounting	4-post (kit included)
Physical dimensions (1RU)	<ul style="list-style-type: none"> • 44.0 (W) x 55.9 (D) x 4.45 (H) cm • 17.3 (W) x 22.0 (D) x 1.75 (H) in.
Weight	24.25 (minimum) to 28.0 lb (maximum); 11.0-12.7 kg

Power	Specifications
Number of Power Supplies	1
Power Supply Size	351W universal, autoswitching

Environmental	Specifications
Operating temperature range	50 to 95°F; 10 to 35°C (up to 3000 ft/914.4m)
Heat emitted	341 (minimum) to 1024 (maximum) BTUs; 100-300W
Maximum altitude	7000 ft; 2133 m

Table 3. Cisco Secure ACS 5.2 VMware Requirements

Component	Specifications
VMware Version	ESX 3.5 or ESX 4.0
CPU	Intel Core 2 (2.13 GHz)
System memory	4 GB
Hard disk requirement	Minimum 512 GB

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 5.2 product bulletin for Cisco Secure ACS 5.2 product numbers and ordering information.

To place an order, contact your account representative or 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

Please check the Cisco Secure ACS homepage at <http://www.cisco.com/go/acs> for the latest information about Cisco Secure ACS.

For more information about Cisco Secure ACS products and the Cisco TrustSec solution, visit <http://www.cisco.com/en/US/netsol/ns1051/index.html> or 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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)