

## Cisco Secure Access Control System 5.0

Cisco® Secure Access Control System (ACS), the Cisco flagship network access control solution, 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 the Fortune 500 companies and almost 70 percent of Russell 1000 companies.

Cisco Secure ACS 5.0 is a next-generation platform that 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 LAN and wired 802.1x network access scenarios.

**Figure 1.** Cisco 1120 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 the networks today, 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 the user identity as well as 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 supports the Cisco Self-Defending Network 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 administrative and management burden.

### Features and Benefits

Cisco Secure ACS 5.0 is the initial release of Cisco's next-generation network identity and access solution. It is a Policy Administration Point (PAP) and Policy Decision Point (PDP) for policy-based access control. This release delivers major new functionality 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

- 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 simplifies policy configuration and maintenance
- A distributed deployment model that enables large scale deployments

The Cisco Secure ACS 5.0 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 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 5.0 features centralized collection and reporting for activity and system health information for full manageability of distributed deployments. It supports proactive operations like monitoring and diagnostics and reactive operations like 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 5.0.

**Table 1.** Key Features and Benefits of Cisco Secure ACS 5.0

Feature	Benefit
<b>AAA protocols</b>	Cisco Secure ACS 5.0 supports two distinct protocols for authentication, authorization, and accounting (AAA). Cisco Secure ACS 5.0 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.
<b>Database options</b>	Cisco Secure ACS 5.0 supports an integrated user repository in addition to supporting integration with existing external identity repositories like Windows Active Directory and LDAP. Multiple databases can be used concurrently for maximum flexibility in enforcing access policy.
<b>Authentication protocols</b>	Cisco Secure ACS 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.
<b>Access policies</b>	Cisco Secure ACS 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.
<b>Centralized management</b>	Cisco Secure ACS 5.0 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.
<b>Monitoring and troubleshooting</b>	Cisco Secure ACS 5.0 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.
<b>Platform options</b>	Cisco Secure ACS is available as a closed and hardened Linux-based appliance or as a software-only application and operating system image for VMWare ESX.

## System Requirements

Cisco Secure ACS 5.0 is available as a one rack-unit (1RU), security-hardened, Linux-based appliance with preinstalled Cisco Secure ACS software or as a software application and operating system image for installation on VMWare ESX 3.5. Table 2 lists the system specifications for the Cisco 1120 Secure ACS 5.0 appliance. For VMWare ESX system requirements, consult the product documentation.

**Table 2.** Cisco 1120 Secure ACS 5.0 Appliance Specifications

Component	Specifications
<b>CPU</b>	Intel E6400 Core2 Duo @ 2.13GHz; 2MB Level 2 cache
<b>Frontside bus</b>	1066 MHz
<b>System memory</b>	4GB, PC2-5300 DDR2 SDRAM, ECC
<b>Hard disk drive</b>	2 x 250GB SATA
<b>Optical storage</b>	DVD-ROM
<b>Network connectivity</b>	2 onboard 10/100/1000, RJ-45 connectors
<b>I/O ports</b>	1 Serial Port, 3 USB 2.0 (1 front, 2 rear), keyboard (PS/2), mouse (PS/2)
<b>Rack-mounting</b>	4 post (kit included)
<b>Physical dimensions (1RU)</b>	<ul style="list-style-type: none"> <li>• 4.3 (W) x 50.8 (D) x 43.2 (H) cm</li> <li>• 17.0 (W) x 20 (D) x 1.7 (H) in.</li> </ul>

Power	Specifications
<b>Maximum power consumption</b>	350W (maximum output, power supply rating) 540W (maximum input, power supply rating)
<b>Input low range</b>	90 to 127 (nominal) VAC; 47–63 Hz
<b>Input high range</b>	180 to 264 (nominal) VAC; 47–63 Hz

Environmental	Specifications
<b>Air temperature – Server on</b>	50 to 95°F (10 to 35°C)
<b>Air temperature – Server off</b>	–104 to 158°F (–40 to 70°C)
<b>Altitude</b>	2000m at 40C
<b>Humidity (nonoperating)</b>	95 percent, noncondensing at +35°C
<b>Cooling system</b>	2 blowers, 1 40mm fan, 1 air shroud

## Ordering Information

Cisco Secure ACS 5.0 does not replace ACS 4.2. Cisco Secure ACS 5.0 is the next-generation platform for centralized identity and access policy management. Some of the key areas of functionality differences include protocol support, external database support, and provisioning interfaces. Customers that choose to deploy ACS 4.2 will have future upgrade paths to the next-generation ACS 5.x platform.

Please see the Cisco Secure ACS 5.0 User Guide at [http://www.cisco.com/en/US/products/ps9911/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html) for a more detailed comparison of ACS 4.0 and ACS 5.0.

Cisco Secure ACS products are available for purchase through regular Cisco sales and distribution channels worldwide. Please refer to the Cisco Secure ACS 5.0 product bulletin for Cisco Secure ACS 5.0 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

For more information about Cisco Secure ACS products please contact your account representative or send your questions to [acs-mkt@cisco.com](mailto:acs-mkt@cisco.com).



**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](http://www.cisco.com/go/offices).

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store 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. (0809R)