# Cisco Secure Access Control System 5.6

## Product Overview

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 policy-based enterprise access and network device administration control platform, deployed by about 80 percent of Fortune 500 companies.

Cisco Secure ACS, a core component of the Cisco TrustSec® solution, is a highly sophisticated policy platform providing RADIUS and TACACS+ services. It supports the increasingly complex policies needed to meet today's demands for access control management and compliance. Cisco Secure ACS provides central management of access policies for device administration and for wireless, wired IEEE 802.1x, and remote (VPN) network access scenarios. Figure 1 shows the Cisco Secure Network Server (SNS) 3415 appliance, based on the Cisco UCS® C220 M3 Rack Server platform.

Cisco Secure ACS 5.6 software can run on the Cisco SNS 3415 and 3495 appliances as well as on existing Cisco 1121 for Cisco Secure ACS Engine appliances, which have reached their end-of-sale dates.

**Figure 1.** Cisco Secure Network Server 3415 Appliance for Cisco Secure Access Control System 5.6 Software

With the ever-increasing reliance on enterprise networks to perform daily job routines and the increasing number of methods available to access today's networks, security breaches and uncontrolled user access are primary concerns for enterprises. Network security officers and administrators need solutions that support flexible authentication and authorization policies that are tied not only to a user's identity but also to context such as the network access type, time of day the access is requested, and the security of the machine used to access the network. Further, there is a stronger need to effectively audit the use of network devices, monitor the activities of device administrators for corporate compliance, and provide broader visibility and control over device access policies across the network.

Cisco Secure ACS is a highly scalable, high-performance access policy system that centralizes device administration, authentication, and user access policy while reducing the management and support burden for these functions.

## Features and Benefits

Cisco Secure ACS 5.6 serves as a policy administration point (PAP) and policy decision point (PDP) for policy-based network device access control, offering a large set of identity management capabilities, including:

- Unique, flexible, and detailed device administration in IPv4 and IPv6 networks, with full auditing and reporting capabilities as required for standards compliance
- A powerful, attribute-guided and rules-based policy model that flexibly addresses complex policy needs
- A lightweight, web-based GUI with intuitive navigation and workflow accessible from both IPv4 and IPv6 clients
- Integrated advanced monitoring, reporting, and troubleshooting capabilities for excellent control and visibility
- Integration with external identity and policy databases, including Microsoft 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 5.6 rules-based policy model supports the application of different authorization rules under different conditions; thus, policy is contextual and not limited to authorization determined by a single group membership. 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 in authorization rules.

Cisco Secure ACS 5.6 features the centralized collection and reporting of 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 deployment wide session monitor, threshold-based notifications, entitlement reports, and diagnostic tools.

Table 1 lists the main features and benefits of Cisco Secure ACS 5.6.

**Table 1.** Main Features and Benefits of Cisco Secure ACS 5.6

| Feature | Benefit |
|---|---|
| **Complete access control and confidentiality solution** | Cisco Secure ACS 5.6 can be deployed with other Cisco TrustSec components, including policy components, infrastructure enforcement components, endpoint components, and professional services. |
| **Authentication, authorization, and accounting (AAA) protocols** | Cisco Secure ACS 5.6 supports two distinct AAA protocols: 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 Payment Card Industry (PCI) compliance. Cisco Secure ACS 5.6 supports AAA features for TACACS+-based device administration on both IPv4 and IPv6 networks. |
| **Database options** | Cisco Secure ACS 5.6 supports an integrated user repository in addition to integration with existing external identity repositories such as Microsoft Active Directory servers, LDAP servers, and RSA token servers. This capability enables the use of multiple LDAP servers for a Cisco Secure ACS cluster and primary and backup LDAP servers per Cisco Secure ACS node (instance). In addition, each Cisco Secure ACS instance can be connected to a different Microsoft Active Directory domain. In Cisco Secure ACS 5.6, you can define multivalue attributes for Microsoft Active Directory and LDAP servers, use Boolean Microsoft Active Directory values, and enter substitutions for Microsoft Active Directory IPv4 address attributes. Multiple databases can be used concurrently for excellent flexibility in enforcing access policy with identity store sequences. You also can add Cisco Secure ACS administrators stored in external Microsoft Active Directory and LDAP databases and authenticate them using those identity stores. |
| **Authentication protocols** | Cisco Secure ACS 5.6 supports a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication through Secure Tunneling (FAST), EAP-Transport Layer Security (TLS), and PEAP-TLS. It also supports TACACS+ authentication with CHAP/MSCHAP protocols and PAP-based password change when using TACACS+ and EAP-GTC with LDAP servers. |

| Feature | Benefit |
|---|---|
| **Access policies** | Cisco Secure ACS 5.6 supports a rules-based, attribute-guided policy model that provides greatly increased power and flexibility for access control policies, which can include authentication protocol requirements, device restrictions, time-of- day restrictions, and other access requirements. Cisco Secure ACS can apply downloadable access control lists (dACLs), VLAN assignments, and other authorization parameters. Furthermore, it allows comparison between the values of any two attributes that are available to Cisco Secure ACS to be used in identity, group-mapping, and authorization policy rules. |
| **Centralized management** | Cisco Secure ACS 5.6 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. |
| **Support for high availability in larger Cisco Secure ACS deployments** | Cisco Secure ACS 5.6 supports up to 22 instances in a single Cisco ACS cluster: 1 primary and 21 secondary. One of these instances can function as a hot (active) standby system, which can be manually promoted to the primary system in the event that the original primary system fails. |
| **Programmatic interface** | Cisco Secure ACS 5.6 supports a programmatic interface for create, read, update, and delete operations on users and identity groups, network devices, and hosts (endpoints) within the internal database. It also adds the capability to export the list of Cisco Secure ACS administrators and their roles through the same web services API. |
| **Monitoring, reporting, and troubleshooting** | Cisco Secure ACS 5.6 includes an integrated monitoring, reporting, and troubleshooting component that is accessible through the web-based GUI. This tool provides excellent visibility into configured policies and authentication and authorization activities across the network. Logs are viewable and exportable for use in other systems as well. A new report generation mechanism in Cisco Secure ACS 5.6 provides significantly better performance and improved ease of use. However, it does not have report customization capabilities under the “Interactive Viewer” option for reports that were available in Cisco UCS ACS 5.5 and earlier releases. A subset of those options such as “Show/Hide columns” and “Sort columns” will be added in a subsequent Cisco Secure ACS release or patch. |
| **Proxy services** | Cisco Secure ACS 5.6 can function as a RADIUS or TACACS+ proxy for an external AAA server by forwarding incoming AAA requests from a network access device (NAD) to the external server and forwarding responses from that server back to the NAD initiating such requests. Cisco Secure ACS 5.6 also has the capability to add and to overwrite RADIUS attributes in proxied AAA requests sent to the external AAA server as well as those in the responses sent back from the external AAA server. |
| **Platform options** | Cisco Secure ACS 5.6 is available as a closed and hardened Linux-based Cisco SNS 3415 or 3495 appliance or as a software operating system image for VMware ESX or ESXi 5.1 or 5.5. It is also supported on the older Cisco 1121 for Cisco Secure ACS Engine appliance, which has reached end-of-sale. |

## System Requirements

Cisco Secure ACS 5.6 is available as a one-rack-unit (1 RU), security-hardened, Linux-based appliance with preinstalled Cisco Secure ACS software on the Cisco SNS 3415 and 3495 appliances as well as the older Cisco 1121 for Cisco Secure ACS Engine appliances. It is also available as a software operating system image for installation in a virtual machine on VMware ESX and ESXi 5.1 and 5.5. Table 2 and Table 3 list the system specifications for the Cisco SNS 3415 and 3495 appliances, respectively. For VMware ESXi system requirements, please see Table 4.

**Table 2.** Cisco SNS 3415 Appliance Specifications

| Component | Specifications |
|---|---|
| **CPU** | 2.4-GHz Intel E5-2609, 80 watts (W), 4 cores, 10-MB cache, DDR3, and 1600 MHz |
| **System memory** | 16 GB total: 4 x 4-GB DDR3 1600-MHz RDIMMs |
| **Hard disk drive (HDD)** | 600-GB 6-Gbps SAS 10,000-rpm HDD |
| **Software RAID controller** | Not used by Cisco Secure ACS application software |
| **Optical storage** | None |
| **Network connectivity** | 4 x 1-GB network interface card (NIC) interfaces<br>**Note:** Only Ethernet0 can be used for management functions; all interfaces listen to AAA requests. |
| **I/O ports** | • Rear panel: 1 DB9 serial port, 2 USB 2.0 ports, 1 DB15 VGA port, and NIC connectors<br>• Front panel: Keyboard, video, and mouse (KVM) console connector, which supplies 2 USB ports, 1 VGA port, and 1 serial port |
| **Trusted Platform Module** | Yes |
| **SSL acceleration card** | No |
| **Rack mount** | 4-post mount |

| Component | Specifications |
|---|---|
| **Physical dimensions (1RU) (H x W x D)** | 1.7 x 16.92 x 28.5 in. (4.32 x 43.0 x 72.4 x cm) |
| **Weight** | 27.1 lb (12.2 kg) |

| Power | Specifications |
|---|---|
| **Number of power supplies** | 1 |
| **Power supply size** | 650W universal (input voltage: 90 to 260V; 47 to 63 Hz) |

| Environmental | Specifications |
|---|---|
| **Operating temperature range** | 41 to 104°F (5 to 40°C); decrease maximum temperature by 1°C per every 1000 ft (305m) of altitude above sea level) |
| **Operating altitude** | 0 to 10,000 ft (0 to 3000m) |

**Table 3.** Cisco SNS 3495 Appliance Specifications

| Component | Specifications |
|---|---|
| **CPU** | 2 x 2.4-GHz Intel E5-2609, 80W, 4 cores, 10-MB cache, DDR3, and 1600 MHz |
| **System memory** | 32 GB total: 8 x 4-GB DDR3 1600-MHz RDIMMs |
| **Hard disk drive** | 2 x 600-GB 6-Gbps SAS 10,000-rpm HDDs |
| **Hardware RAID controller** | Levels 0 and 1<br>LSI 2008 SAS RAID mezzanine card |
| **Optical storage** | None |
| **Network connectivity** | 4 x 1-GB NIC interfaces<br>**Note:** Only Ethernet0 can be used for management functions; all interfaces listen to AAA requests. |
| **I/O ports** | • Rear panel: 1 DB9 serial port, 2 USB 2.0 ports, 1 DB15 VGA port, and NIC connectors<br>• Front panel: KVM console connector, which supplies 2 USB ports, 1 VGA port, and 1 serial port |
| **Trusted Platform Module** | Yes |
| **SSL acceleration card** | Yes |
| **Rack mount** | 4-post mount |
| **Physical dimensions (1RU) (H x W x D)** | 1.7 x 16.92 x 28.5 in. (4. 32 x 43.0 x 72.4 cm) |
| **Weight** | 27.1 lb (12.2 kg) |

| Power | Specifications |
|---|---|
| **Number of power supplies** | 2 |
| **Power supply size** | 650W universal (input voltage: 90 to 260V; 47 to 63 Hz) |

| Environmental | Specifications |
|---|---|
| **Operating temperature range** | 41 to 104°F (5 to 40°C); decrease maximum temperature by 1°C per every 1000 ft (305m) of altitude above sea level) |
| **Operating altitude** | 0 to 10,000 ft (0 to 3000m) |

**Table 4.** Cisco Secure ACS 5.6 VMware Requirements

| Component | Specifications |
|---|---|
| **VMware version** | VMware ESX and ESXi 5.1 and 5.5 |
| **CPU** | 2 CPUs (dual CPUs, Intel Xeon processors, Core 2 Duo or 2 single CPUs) |
| **System memory** | 4 GB or RAM |
| **Hard disk requirements** | User-configurable between 60 and 750 GB (minimum of 150 GB is recommended) |
| **NIC** | Network NIC (1 Gbps) available for Cisco Secure ACS application use |

## 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 5.6 product bulletin for Cisco Secure ACS 5.6 part numbers and ordering information.

To place an order, contact your account representative or visit the Cisco Ordering homepage.

## Service and Support

Cisco offers a wide range of service 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 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.

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.



Printed in USA C78-732914-01 12/14