Cisco Secure Control Access System 5.8

Cisco® Secure Access Control System ties together an enterprise's network access policy and identity strategy. It is the world's most trusted policy-based platform for enterprise access and network device administration control, deployed by about 80 percent of Fortune 500 companies.

Product Overview

Secure Access Control System, 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. It manages 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 3515/3595 appliances which are based on the Cisco UCS® C220 M4 Rack Server platform.

Release 5.8 of the Secure Access Control System software can run on the Secure Network Server 3515 and 3595 appliances as well as on existing Secure Network Server 3415 and 3495, which have reached their end-of-sale dates.

Figure 1. Secure Network Server 3515/3595 Appliances for Secure Access Control System 5.8

Organizations rely on enterprise networks to perform daily job routines. With the increasing number of methods available to access those networks, security breaches and uncontrolled user access are primary concerns. 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.

Secure Access Control System 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

Secure Access Control System 5.8 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 supports large-scale deployments and provides a highly available solution

The 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. Information in external databases can be directly referenced in access policy rules. Attributes can be used both in policy conditions and in authorization rules.

Secure Access Control System 5.8 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 solution's main features and benefits.

Table 1. Main Features and Benefits

Feature	Benefit
Complete access control and confidentiality solution	The solution 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	Two distinct AAA protocols are supported: RADIUS for network access control and TACACS+ for network device access control. Secure Access Control System 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. It supports AAA features for TACACS+-based device administration on both IPv4 and IPv6 networks.
Database options	Secure Access Control System 5.8 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. You can use multiple LDAP servers for a Secure Access Control System cluster and primary and backup LDAP servers for Secure Access Control System nodes (instances). In addition, each instance can be connected to a different Microsoft Active Directory domain. You can define multivalue attributes for Active Directory and LDAP servers, use Boolean Active Directory values, and enter substitutions for Active Directory IPv4 address attributes. Multiple databases can be used concurrently for exceptional flexibility in enforcing access policy with identity store sequences. You also can add Secure Access Control System administrators stored in external Active Directory and LDAP databases and authenticate them using those identity stores.
Authentication protocols	A wide range of authentication protocols are supported, 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. The solution also supports TACACS+ authentication with CHAP and MSCHAP protocols and PAP-based password change when using TACACS+ and EAP-GTC with LDAP servers.

Feature	Benefit
Access policies	The rules-based, attribute-guided policy model 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. Secure Access Control System can apply downloadable access control lists (dACLs), VLAN assignments, and other authorization parameters. Furthermore, it allows a comparison between the values of any two attributes that are available to Secure Access Control System to be used in identity, group-mapping, and authorization policy rules.
Centralized management	The lightweight, web-based GUI 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 deployments	Secure Access Control System 5.8 supports up to 22 instances in a single 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	A programmatic interface is used for create, read, update, and delete operations on users and identity groups, network devices, and hosts (endpoints) within the internal database. The list of administrators and their roles can be exported through the same web services API.
Monitoring, reporting, and troubleshooting	An integrated monitoring, reporting, and troubleshooting component 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.
Proxy services	The solution can function as a RADIUS or TACACS+ proxy for an external AAA server. It forwards incoming AAA requests from a network access device (NAD) to the external server and forwards responses from that server back to the NAD initiating such requests. It can also add and 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.
FIPS 140-2 Level 1	Secure Access Control System 5.8 is compliant with Federal Information Processing Standard (FIPS) 140-2 Level 1. The solution's embedded FIPS 140-2 Level 1 implementation uses validated Cisco Common Cryptographic Module (C3M) and Network Security Services (NSS) modules, adhering to FIPS 140-2 Implementation Guidance section G.5 guidelines. The key size of Certificate Authority certificates and server certificates that are used in Secure Access Control System should be at least 2048 bits. The key size of client certificates should be at least 1024 bits.
	Release 5.8 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 5.1,5.5 and 6.0. It is also supported on the older Secure Access Control System 1121 appliance, which has reached its end-of-sale date.

Release 5.8 adds the following new features on top of the features available in Release 5.7:

- PowerBroker Identity Services (PBIS) library support for Active Directory integration
- Capability to authenticate administrators against RSA identity and RADIUS SecurID servers
- Capability to export policies from the web interface
- Capability to change internal user passwords using representational state transfer (REST) API
- Internal administrator password hashing
- FIPS 140-2 Level 1 compliance

System Requirements

Secure Access Control System 5.8 is available as a one-rack-unit (1RU), security-hardened, Linux-based appliance with preinstalled system software on the Cisco SNS 3415 and 3495 appliances as well as the older Cisco 1121 for Secure Access Control System Engine appliances. It is also available as a software operating system image for installation in a virtual machine on VMware ESX and ESXi 5, 5.0 update 2, 5.1, 5.1 update 2, 5.5, 5.5 update 1, and 6.0. Table 2 and Table 3 list the system specifications for the Cisco SNS 3515 and 3595 appliances, respectively. For VMware ESXi system requirements, please see Table 4.

Table 2. SNS 3515 Appliance Specifications

Component	Specifications
CPU	1 – Intel Xenon 2.40 GHz E5-2620 (6 cores)
System memory	16 GB (2 x 8 GB)

Component	Specifications
Hard disk drive (HDD)	1 - 2.5-in. 600-GB 6Gb SAS 10K RPM
Caching RAID controller	Caching only, RAID not supported on SNS-3515
Network connectivity	6 x 1-GB network interface card (NIC) interfaces **Note:** Only Ethernet0 can be used for management functions; all interfaces listen to AAA requests.
Rack mount	4-post mount
Physical dimensions (1RU) (H x W x D)	1.7 x 16.9 x 29.8 in. (4.32 x 43 x 75.6 cm)

Power	Specifications
Number of power supplies	1
Power supply size	770W universal (input voltage: 90 to 260V; 47 to 63 Hz)

Environmental	Specifications
Operating temperature range	41 to 95°F (5 to 35°C) (operating, sea level, no fan fail, no CPU throttling, turbo mode)
Operating altitude	0 to 10,000 ft (0 to 3000m)

Table 3. SNS 3595 Appliance Specifications

Component	Specifications
CPU	1 – Intel Xenon 2.60 GHz E5-2640 (8 cores)
System memory	64 GB (4 x 16 GB)
Hard disk drive	4 - 2.5-in. 600-GB 6Gb SAS 10K RPM
Caching RAID controller	Level 10 Cisco 12G SAS Modular RAID Controller
Network connectivity	6 x 1-GB NIC interfaces **Note:** Only Ethernet0 can be used for management functions; all interfaces listen to AAA requests.
Rack mount	4-post mount
Physical dimensions (1RU) (H x W x D)	1.7 x 16.9 x 29.8 in. (4.32 x 43 x 75.6 cm)

Power	Specifications
Number of power supplies	2
Power supply size	770W universal (input voltage: 90 to 260V; 47 to 63 Hz)

Environmental	Specifications
Operating temperature range	41 to 95°F (5 to 35°C) (operating, sea level, no fan fail, no CPU throttling, turbo mode)
Operating altitude	0 to 10,000 ft (0 to 3000m)

Table 4. VMware Requirements

Component	Specifications
VMware version	VMware ESX and ESXi 5.1, 5.5 and 6.0.
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 Access Control System products are available for purchase through regular Cisco sales and distribution channels worldwide. Please refer to the Cisco Secure Access Control System 5.8 product bulletin for 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.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For More Information

Please check the Cisco Secure Access Control System homepage at http://www.cisco.com/go/acs for the latest solution information.

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 C78-735913-01 02/17