# Cisco Secure Access Control System 5.5

## Product Overview

**Q.** What is the Cisco® Secure Access Control System?

**A.** The Cisco Secure Access Control System (ACS) is a centralized identity and access policy solution that ties together an enterprise's network access policy and identity strategy. Cisco Secure ACS operates as a RADIUS and TACACS+ server, combining user authentication, user and administrator device access control, and policy control in a centralized identity networking solution.

**Q.** Why do I need Cisco Secure ACS?

**A.** Changing business dynamics, IT transformations, regulatory requirements, and increasing security threats have created new challenges in access control management. Technologies such as IEEE 802.1X have become more pervasive, and the demand for robust access policy and visibility is growing. New solutions are needed that integrate access policy and identity in the network. Cisco Secure ACS allows you to implement advanced enterprise policies by defining powerful and flexible policy rules through an easy-to-use, lightweight GUI. The system's integrated management and advanced monitoring, reporting, and troubleshooting capabilities provide a high level of control and visibility into access control and device administration policies and activities across the network.

## New Features

**Q.** What is new in Cisco Secure ACS 5.x?

**A.** Cisco Secure ACS 5.x serves as a Cisco Policy Administration Point (PAP) and Policy Decision Point (PDP) for policy-based network device access control. It offers a large set of identity management capabilities, including:

- Unique, flexible, and precise device administration in IPv4 and IPv6 networks with full auditing and reporting capabilities as required for standards compliance
- A powerful attribute-driven rules-based policy model that addresses complex policy needs in a flexible manner
- 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 control and visibility
- Streamlined integration with external identity and policy databases, including those accessible through Windows Active Directory and Lightweight Directory Access Protocol (LDAP), for simpler policy configuration and maintenance
- A distributed deployment model that enables large-scale deployments and supports a highly available solution

For more information about Cisco Secure ACS 5.x features, and for ordering and deployment guides and all other relevant documentation, visit http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html.

**Q.** What new features became available in Cisco Secure ACS 5.3?

**A.** Cisco Secure ACS 5.3 added support for the following features:

- Enhanced upgrade from versions 5.1 and 5.2 without the need to reimage, back up, or restore policy configuration
- Programmatic interface for create, read, update, and delete (CRUD) operations on user objects
- Use of dynamic attributes (attribute substitution) in TACACS+ shell profiles
- Capability to limit the number of concurrent sessions for all users or per user group based on each Cisco Secure ACS instance
- Capability to retrieve and verify internal users' passwords from an external ID store
- Capability to disable a user account based on the number of failed attempts or its expiration on a fixed date or in a specific number of days
- ID Store Sequence option to proceed to the next ID store when access to the current ID store fails for any reason
- Capability to function as TACACS+ proxy server
- Support for wildcards for host MAC addresses
- Capability to add network devices using IP address ranges
- Capability to look up devices by IP address
- TACACS+ authentication using CHAP/MSCHAP
- Capability to compare values of any two attributes in identity and authorization policies
- Support for checking the dial-in attributes in users' Active Directory accounts
- Capability to display RSA Secured® node missing secret
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS) support
- Recovery of logs after local servers are reconnected to the remote log collector Cisco Secure ACS device

**Q.** What the new features became available in Cisco Secure ACS 5.4?

**A.** The following features are supported in Cisco Secure ACS 5.4:

- Support of the new Cisco UCS® C220 M3 hardware platform (the Cisco Secure Network Server SNS-3415-K9 appliance for Cisco Secure ACS, Cisco Identify Services Engine, and Cisco Network Admission Control)
- TACACS+-based device administration and HTTP- and SSH-based access for the Cisco Secure ACS administrator in IPv6 networks.
- Support for Cisco Secure ACS on VMware with less than 500 GB hard disk space
- Support for multiple Ethernet interfaces
- Capability to connect different nodes (instances) in a Cisco Secure ACS cluster to a different AD domain
- Administrator authentication through Active Directory and LDAP
- API for CRUD operations on devices and hosts
- Online Certificate Status Protocol (OCSP) support
- Display of configurable copyright banner before and after administrator's login
- Support for VMware tools
- Support of up to 20 instances in a single Cisco Secure ACS cluster

- Capability to inject RADIUS attributes into proxied authentication, authorization, and accounting (AAA) requests
- Synchronization of the machine access restriction (MAR) cache among all Cisco Secure ACS instances in a cluster
- Capability to add Common Name (CN) as a new member attribute for LDAP users in addition to Distinguished Name (DN)
- Support for PAP change password for TACACS+ and Extensible Authentication Protocol-Generic Token Card (EAP-GTC) for LDAP
- Support for account expiry date per user for internal users
- Capability to add a Certificate Issuer field into the Certificate Dictionary for use in Cisco Secure ACS policy rules
- Authenticated NTP support

**Q.** What are the new features available in Cisco Secure ACS 5.5?

**A.** Many new features and capabilities are supported Sin Cisco Secure ACS 5.5 These include a resiliency platform with the Cisco Secure Network Server SNS-3495,* which offers redundant power supplies and hard drives with RAID.

Enhancements in monitoring, reporting and troubleshooting include:

- Support for report generation covering events for longer periods of time (with more than 100 pages)
- Scheduled (automated) reports sent by email
- Support for Simple Network Management Protocol (SNMP) traps for Cisco Secure ACS health status
- Logs and alarms for replication failures
- Reports for policy configuration changes between two specified times

Enhancements in usability include:

- Capability to import vendor-specific attributes from comma-separated values (CSV) files
- Option to autorefresh at user-defined intervals (for pages that have a refresh button)
- NIC bonding (a virtual IP address shared by all enabled Ethernet interfaces)
- Support for the reuse of the current RSA Secured token cached by Cisco Secure ACS
- Capability to allow any Cisco Secure ACS administrator to be disabled or deleted, including predefined “acsadmin” account
- Capability for the Base license to be reinstalled from the Cisco Secure ACS GUI without having to reset Cisco Secure ACS

Enhancements for standards-ready security include:

- Encrypted (highly secure) syslogs
- Protection against Cisco Secure ACS administrator management spoofing
- Option to protect the Cisco Secure ACS backup with a custom password provided by the Cisco Secure ACS administrator
- Support for downloading certificate revocation lists (CRLs) over HTTPS in addition to HTTP

Note that Cisco Secure ACS Release 5.5 will be certified for Federal Information Processing Standards (FIPS) 140-2 Level 1 for use by federal customers.

**Q.** Does Cisco Secure ACS 5.5 have full feature parity with Cisco Secure ACS 4.2?

**A.** No. Cisco Secure ACS 5.5 supports most of the features in Release 4.2 and is well-suited for many deployments today that require policy-based device administration or wired, wireless, or remote access control. Release 4.2 features that are not available in Release 5.5 include authentication via Open Database Connectivity (ODBC), synchronization with relational database management system (RDBMS) databases, and integration with CiscoWorks Common Services for role-based access control (RBAC) support. Since the last two features have acceptable workarounds, such as using the Representational State Transfer (REST) API to add, delete, or modify users, hosts, and network devices, support for those features is not planned for future Cisco Secure ACS releases.

**Q.** Is Cisco Secure ACS 5.5 a software or a hardware product?

**A.** Cisco Secure ACS 5.5 is offered both as a hardware appliance and as software. You can order it as:

- A one rack-unit (1RU) dedicated, security-hardened Linux appliance (CSACS-1121-K9 or CSACS-3415-K9 or CSACS-3495-K9[*]) with the base Cisco Secure ACS software preinstalled
- A software-only image (application and operating system) for installation on VMware ESX/ESXi hypervisor

For complete specifications, please refer to the Cisco Secure ACS data sheets at http://www.cisco.com/en/US/products/ps9911/products_data_sheets_list.html.

**Q.** How is the new Cisco Secure ACS 5.5 policy model different from that of earlier releases?

**A.** Cisco Secure ACS 5.5 introduced a rules-based policy model that is different from the group-based policy model supported in earlier releases. The new model delivers the power and flexibility needed for complex security policies that require the evaluation of many different attributes and conditions, in addition to the user's identity, in order to grant access privileges.

Following are some of the main enhancements with the new policy model:

- Policy logic is decoupled from users and groups. The assignment of privileges and permissions is not directly defined in Cisco Secure ACS users and user groups. It is defined through authorization rules.
- In Cisco Secure ACS authorization rules, multiple authorization profiles may be specified as an authorization decision result (with a precedence order to resolve conflicts). This reduces the overall number of authorization profiles needed and simplifies policy modification.
- Network devices may be categorized in multiple groups, such as those based on geography or organization. This capability allows rules to be created based on hierarchical groups.
- Release 5.5 offers more powerful and flexible rules-based mapping of users or hosts to identity groups from the information available in external directories or in identity repositories (such as group memberships or identity attributes).
- Release 5.5 includes highly flexible access control policies that address authentication protocol requirements, device restrictions, time-of-day restrictions, posture validation, downloadable access control lists (dACLs), VLAN assignments, and other authorization parameters.

**Q.** What are the capabilities of the Cisco Secure ACS GUI?

**A.** Release 5.5 has a lightweight, web-based GUI that is highly secure, intuitive, and easy to use. It does not require the installation of additional client software for GUI access. In addition to policy management and provisioning, the Cisco Secure ACS Release 5.5 GUI also has integrated monitoring and reporting capabilities that provide a high level of control and visibility into the network.

**Q.** What are the monitoring and reporting capabilities that the new GUI offers?

**A.** Cisco Secure ACS 5.5 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. Cisco Secure ACS 5.5 supports the generation of at least five times the number of records-enabling reports, for longer periods of time, than Cisco Secure ACS 5.4. In addition, Cisco Secure ACS 5.5 also supports autogenerated scheduled reports.

**Q.** How does Cisco Secure ACS 5.5 integrate with external databases?

**A.** Release 5.5 provides a great deal of flexibility for integrating with external identity and policy databases such as those accessible through Active Directory and LDAP. Information in external databases can be referenced directly in policy rules. User and group attributes can be retrieved and then referenced when configuring either policy conditions or authorization results. This capability allows the definition of much more sophisticated policies than authorization through group mapping. Cisco Secure ACS 5.5 also supports multivalue attributes for Active Directory and LDAP servers.

**Q.** Do I need to run a remote agent to use the Cisco Secure ACS 5.5 appliance?

**A.** No. Although earlier versions of Cisco Secure ACS appliances and software required that the Cisco Secure ACS Remote Agent for Windows software be installed on a member of a trusted domain for Microsoft Windows authentication, all ACS 5.x appliance and software Releases, including 5.5, support native integration with Active Directory and do not need a remote agent.

## Scalability

**Q.** How does Cisco Secure ACS 5.5 scale for large deployments?

**A.** Cisco Secure ACS 5.5 supports distributed deployment to provide high availability and scalability. A deployment can be composed of multiple Cisco Secure ACS instances that are managed together in a single distributed deployment. One system is designated as primary, and that system accepts configuration changes and propagates them to the secondary instances. For the smallest deployments, one primary and one secondary instance are recommended for redundancy. Larger deployments can add additional secondary servers as dictated by network design. Release 5.5 officially supports up to 22 instances: one primary and 21 secondaries (one of which can work as a hot, or active, standby that can be manually promoted to primary in case of primary failure), including a log collector, in a single cluster. All the Cisco Secure ACS instances are identical in the sense that a full Cisco Secure ACS software version is installed on each of them. Yet part of the functionality (AAA, management interface, or monitoring and reporting) can be disabled on these instances, allowing each Cisco Secure ACS instance to play a specific role or roles in the deployment.

Cisco Secure ACS 5.5 has an efficient replication mechanism that makes the system easy to configure. Within the distributed deployment, the primary Cisco Secure ACS server is the single point of configuration, and all configuration changes made on the primary server are automatically replicated in the deployment by propagating incremental changes to all the secondary servers. The primary server has a GUI where all the associated secondary servers can be monitored, together with their replication status.

**Q.** How are software updates handled in Cisco Secure ACS 5.5?

**A.** Cisco Secure ACS 5.5 features improved, centralized management of software updates (upgrades and patches); this process is controlled through the GUI of the primary Cisco Secure ACS server. Updates can be applied on selected Cisco Secure ACS servers in a deployment, or on all of them, and software update files can reside in remote repositories or be uploaded to the primary server. Releases 5.3, 5.4, and 5.5 support

direct upgrades from earlier releases via CLI and do not need to be reimaged with the new software image. In addition, there is no need to back up and restore the database.

## Ordering Information

**Q.** What is the licensing model for Cisco Secure ACS 5.5?

**A.** Each Cisco Secure ACS 5.5 appliance or software package is delivered with a Base license, and each Cisco Secure ACS instance requires a Base license to operate. Add-on licenses are available to support deployments with more than 500 network devices and to support advanced Cisco Security Group Access (SGA) features. For available part numbers and detailed descriptions, refer to the Cisco Secure ACS 5.5 Ordering Guide at http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps5698/ps6767/ps9911/product_bulletin_c25-689829.html.

**Q.** I currently use Cisco Secure ACS View 4.0 for monitoring and reporting. Do I still need that product with Cisco Secure ACS 5.5?

**A.** No. Cisco Secure ACS 5.5's integrated monitoring and reporting component replaces the Cisco Secure ACS View 4.0 product in Cisco Secure ACS 5.5 deployments. Customers may still require a separate Cisco Secure ACS 5.5 instance for monitoring and reporting to minimize any impact on run-time performance.

**Q.** Are evaluation copies of Cisco Secure ACS available?

**A.** Yes. You can download a 90-day trial version of the Cisco Secure ACS Base license from https://tools.cisco.com/SWIFT/LicensingUI/loadDemoLicensee?FormId=310. You can download the Cisco Secure ACS 5.5 software image from Cisco.com if you have a valid SAS contract for an earlier release. Otherwise, please contact your local Cisco representative to obtain a copy of the software image or order the free product (product identification number R-CSACS-EVAL-K9=) to do your evaluation.

* Estimated availability is early December 2013.

## For More Information

For more information about Cisco Secure ACS, contact your local account representative or send your questions to 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.



Printed in USA C67-730034-00 10/13