Cisco Secure Access Control System 5.4

Cisco Secure Access Control System Overview

Q. What is Cisco® Secure Access Control System?

A. 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, regulatory requirements, and increased security threats have created new demands in access control management. As technologies such as IEEE 802.1x become more pervasive and the need for robust access policy and visibility grows, new solutions are needed that integrate access policy and identity into 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 the maximum 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 5.4?

A. Cisco Secure ACS 5.4 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 granular 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 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

For more information about Cisco Secure ACS 5.4 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 new features and capabilities:

- Enhanced upgrade from versions 5.1 and 5.2 without the need to re-image, back up, or restore policy configuration
- Programmatic interface for Create, Read, Update, and Delete (CRUD) operations on user objects
- Ability to use dynamic attributes (attribute substitution) in TACACS+ shell profiles
- Maximum 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
- User accounts can be disabled based on the number of failed attempts and/or their expiration (on a fixed date or in a specific number of days)
- When using ID Store Sequence, option to proceed to the next ID store when access to the current ID store fails for any reason
- Ability to function as TACACS+ proxy server
- Support for wildcards for host MAC addresses
- Network devices can be added using IP address ranges
- Ability to look up devices by IP address
- TACACS+ authentication using CHAP/MSCHAP
- Ability to compare values of any two attributes in identity and authorization policies
- Support for checking the dial-in attributes in users' Active Directory accounts
- Ability to display RSA node missing secret
- PEAP-TLS protocol support
- Recovery of logs after reconnection of local servers to the remote log collector Secure ACS device

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

A. The following new features and capabilities are supported in Cisco Secure ACS 5.4:

- Support new Cisco UCS C220 M3 hardware platform (SNS-3415-K9 appliance for ACS/ISE/NAC application)
- TACACS+ based device admin and HTTPS/SSH based ACS admin access in IPv6 networks
- Support ACS on VMware with less than 500 GB hard disk
- Support multiple Ethernet interfaces
- Capability to connect different nodes (instances) in an ACS cluster to a different AD domain
- Admin authentication via Active Directory/LDAP
- API for CRUD operations on devices and hosts
- Online Certificate Status Protocol (OCSP) support
- Display configurable copyright banner before and after admin login
- Support VMware tools
- Support up to 20 instances in a single ACS cluster
- Capability to inject RADIUS attributes into proxied AAA requests
- Synchronization of MAR cache among all ACS instances in a cluster

- Add Common Name (CN) as a new member attribute for LDAP users in addition to Distinguished Name (DN)
- Support PAP change password (for T+ and EAP-GTC) for LDAP
- Support account expiry date per user for internal users
- Add Certificate Issuer field into Certificate Dictionary for use in ACS policy rules
- Authenticated NTP support

Q. Does Cisco Secure ACS 5.4 have full feature parity with Cisco Secure ACS 4.2?

A. No. Cisco Secure ACS 5.4 supports most of the features in Release 4.2 and is well-suited for many deployments today that require policy-based device administration and/or wired, wireless, or remote access control. Release 4.2 features that are not available in Release 5.4 include authentication via ODBC, synchronization with RDBMS databases, and integration with CiscoWorks Common Services for RBAC support. Since the last two features have acceptable workarounds, such as using REST API to add, delete, or modify users, hosts, and network devices, support is not planned for them in future Cisco Secure ACS releases.

Q. Is Cisco Secure ACS 5.4 a software or a hardware product?

A. Cisco Secure ACS 5.4 is offered both as a hardware appliance and as software:

- A one rack-unit (1-RU), dedicated, security-hardened Linux appliance (CSACS-1121-K9 or CSACS-3415-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 5.4 policy model different from that of earlier releases?

A. Cisco Secure ACS 5.4 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 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. Assignment of privileges and permissions is not directly defined in Cisco Secure ACS users and user groups, but 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 device groups, such as those based on geography or organization. This allows rules to be defined based on hierarchical groups.
- Release 5.4 offers more powerful and flexible rules-based mapping of users or hosts to identity groups based on information available in external directories or identity repositories (such as group memberships or identity attributes).
- Release 5.4 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 new capabilities of the Cisco Secure ACS GUI?

A. Release 5.4 features a lightweight, web-based GUI that is secure, intuitive, and easy to use, and does not require the installation of additional client software for GUI access. In addition to policy management and provisioning, the Release 5.4 GUI also has integrated monitoring and reporting capabilities that provide a high level of granular control and visibility into the network.

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

A. Cisco Secure ACS 5.4 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.

Q. How does Cisco Secure ACS 5.4 integrate with external databases?

A. Release 5.4 provides a great deal of flexibility for integrating with external identity and policy databases such as Microsoft Active Directory and LDAP-accessible databases. 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 allows the definition of much more sophisticated policies than authorization through group mapping.

Q. Do I need to run a remote agent to use the Cisco Secure ACS 5.4 appliance?

A. No. While previous Cisco Secure ACS appliances required that Cisco Secure ACS Remote Agent for Windows software be installed on a member of a trusted domain for Microsoft Windows authentication, the Release 5.4 appliance supports native integration with Active Directory and does not need a remote agent.

Scalability

Q. How does Cisco Secure ACS 5.4 scale for large deployments?

A. Cisco Secure ACS 5.4 supports distributed deployment to provide high availability and scalability. A deployment can be composed of multiple 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 secondary instance are recommended for redundancy. Larger deployments can add additional secondary servers as dictated by network design. Release 5.4 officially supports up to 21 instances (1 primary and 20 secondary, 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 (authentication, authorization, and accounting [AAA], management interface, and monitoring and reporting) could be disabled on these instances, allowing for each Cisco Secure ACS instance to play a specific role or roles in the deployment.

Cisco Secure ACS 5.4 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 provides 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 5.4?

A. Cisco Secure ACS 5.4 features improved, centralized management of software updates (upgrades and patches); this process is controlled through the GUI of the primary ACS server. Updates can be applied on selected or all ACS servers in a deployment, and software update files can reside in remote repositories or be uploaded to the primary server. Releases 5.3 and 5.4 support direct upgrade from earlier releases via CLI and do not need to be re-imaged with the new software image (in addition, there is no need for database backup and restore).

Ordering Information

Q. What is the licensing model for Cisco Secure ACS 5.4?

A. Each Cisco Secure ACS 5.4 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 Security Group Access (SGA) features. For available part numbers and detailed descriptions, refer to the Cisco Secure ACS 5.4 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 5.4?

A. No. Cisco Secure ACS 5.4's integrated monitoring and reporting component replaces the Cisco Secure ACS View 4.0 product in Cisco Secure ACS 5.4 deployments. Customers may still require a separate Cisco Secure ACS 5.4 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 5.4 software image from Cisco.com if you have a valid SAS contract for an earlier ACS release. Otherwise, please contact your local Cisco representative to obtain a copy of the software image to do your evaluation.

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 C67-718298-00 01/13