Cisco Secure Access Control Server Express 5.0

Overview

Q. What is Cisco® Secure Access Control Server Express 5.0 (Cisco Secure ACS Express)?

A. Cisco Secure ACS Express is an entry-level RADIUS and TACACS+ authentication, authorization, and accounting (AAA) server for retail branch, enterprise branch office deployments and small-medium-sized businesses (SMBs) with fewer than 350 users and 50 devices.

Cisco Secure ACS Express controls user and machine access to various networks including wireless, wired, and virtual private networks. Cisco Secure ACS Express also controls administrative access to network devices using RADIUS and TACACS+.

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

A. Cisco Secure ACS Express is available on a Cisco hardware appliance that is preloaded with Cisco Secure ACS Express 5.0. For more details on the hardware specifications, please refer to the data sheet at http://www.cisco.com/go/acsexp.

Q. How is Cisco Secure ACS Express positioned in comparison to Cisco Secure ACS for Windows (ACS Windows) and Cisco Secure ACS Solution Engine (ACS SE)?

A. ACS Windows and ACS SE are for customers who need a highly scalable access control solution that spans multiple sites. The feature set is catered to the enterprise deployments and includes but is not limited to support for Network Admission Control (NAC), device command authorization, command-line interface (CLI) views, integration with CiscoWorks management applications, and support for Cisco Security Monitoring, Analysis, and Response System (MARS).

For a detailed feature set, please refer to the ACS Windows and ACS SE data sheets at http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_data_sheets_list.html.

Cisco Secure ACS Express is well suited for deployments that need an access control solution for fewer than 350 users and 50 devices. This product is intended to serve small to medium-sized businesses, retail sites and enterprise branch offices where customers need an easy-to-use GUI yet require a comprehensive but simple feature set and a lower price point to address their specific deployment needs.

For a detailed feature set, please refer to the Cisco Secure ACS Express data sheet at http://www.cisco.com/go/acsexp.

In summary, ACS Windows and ACS SE cater to enterprise-class deployments that need a highly scalable AAA server. Cisco Secure ACS Express is positioned to cater to smaller deployments that need AAA services.

Q. What deployments is Cisco Secure ACS Express best suited for?

A. Cisco Secure ACS Express can be deployed at the following:

- Enterprise branch
- Retail sites
- Small and medium-sized businesses

Enterprise Branch

Large enterprises are likely to have a centralized AAA deployment that manages the various regions within a corporate network. User and machine identities within the enterprise may be stored in centralized user databases, such as Active Directory.

Such large enterprises might have several branch sites that need to mitigate adverse impacts of a WAN outage by having a local AAA server present at that site. For that purpose, a single or a pair of Cisco Secure ACS Express servers may be deployed that are configured to authenticate users and machines against the centralized user database. Alternatively, the branch site may deploy a user database, such as Active Directory, at a local site to work around any dependency on a central site for user management.

Retail Branch

Cisco Secure ACS Express can be deployed within retail organizations that require a local AAA server in each of their retail branches for various reasons including but not limited to WAN independence, localized access policies, and decentralized user repositories.

Small and Medium-Sized Businesses

Cisco Secure ACS Express can be deployed at businesses that have a few hundred users across one or multiple sites. In this instance, Cisco Secure ACS Express could be used to control access for wireless, wired, remote access, and device administration deployments, similar to what an enterprise-class AAA server would do in larger deployments but customized from a usability, feature, deployment size, and price point of view.

Q. Can I migrate to Cisco Secure ACS Express from ACS Windows or ACS SE?

A. No. Migration from ACS Windows or ACS SE is not supported.

Q. Can I upgrade to ACS Windows or ACS SE from Cisco Secure ACS Express?

A. No. This upgrade is currently not supported.

Q. Does Cisco Secure ACS Express require any licensing?

A. Cisco Secure ACS Express supports 50 network devices and 350 unique logins in a 24-hour period. No additional licensing is available or required.

For more details on this, please refer to the product guide at http://www.cisco.com/go/acsexp.

Features and Protocol Support

Q. What network access gateways does Cisco Secure ACS Express support?

A. Cisco Secure ACS Express supports a broad set of networking access products, including Cisco IOS® routers, VPN and firewall access products such as VPN concentrators and the ASA, voice-over-IP (VoIP) solutions, Cisco Wireless LAN controllers and access points, storage networks, and 802.1x-enabled Cisco Catalyst® switches.

For more details, refer to the product guide at http://www.cisco.com/go/acsexp.

Q. What protocols does Cisco Secure ACS Express support?

A. Cisco Secure ACS Express supports the protocols listed in Table 1.

Table 1. Protocols Supported by Cisco Secure ACS Express

Protocol	Description
RADIUS	Cisco Secure ACS Express conforms to RFC 2138, 2284, 2865, 2866, 2867, and 2869. Cisco Secure ACS Express supports the following: • Authentication on old and new RADIUS ports • Vendor-specific attributes (VSAs) from Cisco IOS Software/PIX® devices, VPN concentrators, Cisco WLAN controllers, Aironet® access points, and other IETF RADIUS-compliant Network Access Servers (NAS) • The definition of custom VSAs
TACACS+	Cisco Secure ACS Express supports privilege-level authorization and time of day (TOD) and day of week (DOW) policies for TACACS+ users. Additionally, there is support for external databases such as Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, one-time password (OTP) servers (RADIUS and RSA native access) for TACACS+ requests.
EAP	Cisco Secure ACS Express supports the following Extensible Authentication Protocol (EAP) methods with a configurable order of negotiation: • EAP Transport Layer Security (EAP TLS) • Protected EAP (PEAP) v0, v1 • EAP-Flexible Authentication through Secure Tunneling (EAP-FAST) v0 • Cisco LEAP • Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) Additionally, Cisco Secure ACS Express supports Password Authentication Protocol (PAP) and CHAP.

Q. What ports does Cisco Secure ACS Express use?

A. Cisco Secure ACS Express responds to the following incoming ports/services when it is operational:

- RADIUS: User Datagram Protocol (UDP)/1645, UDP/1812, UDP/1646, UDP/1813 (in)
- Replication: UDP/1645 (in-out)
- TACACS+: TCP/49 (in)
- HTTPS/443 (in)
- Secure Shell (SSH) Protocol/22 (in)
- Internet Control Message Protocol (ICMP) (in-out)
- Simple Network Management Protocol (SNMP)/161 (in-out)
- Secure FTP (SFTP)/22 (out)
- Simple Network Time Protocol (SNTP)/123 (out)
- Lightweight Directory Access Protocol (LDAP)/389 (out)
- Active Directory: LDAP/389, Kerberos/88, Kerberos password change/464, Global Catalog/3268 (out)
- RSA OTP Software Development Kit (SDK): 5500 (out)
- FTP/21 (out)
- Syslog UDP/514 (out)
- Simple Mail Transfer Protocol (SMTP)/465 (out)

Q. How does Cisco Secure ACS Express handle authentication?

A. Cisco Secure ACS Express uses authentication to verify an individual's identity during a login attempt. Cisco Secure ACS Express uses the following authentication methods:

- Credential source
- Machine authentication

Credential Source

Cisco Secure ACS Express supports the use of a local database, an external token server, LDAP, and Active Directory as credential sources based on network access profiles. Cisco Secure ACS Express also supports the use of token server using proxy RADIUS.

Machine Authentication

Machine authentication enables a client machine to authenticate itself using the identity and credentials of the computer to Cisco Secure ACS Express. Cisco Secure ACS Express supports only Windows Machine Authentication against Active Directory.

Cisco Secure ACS Express supports machine authentication configuration for the protocols listed in Table 2.

You configure the outer and inner EAP methods using the GUI.

Table 2. Supported Machine Authentication Protocols

Outer Method	Inner Method
PEAP	EAP-MSCHAPv2
PEAP	EAP-TLS
EAP-TLS	

As part of the certificate setup, you have to install the server certificate for Cisco Secure ACS Express and enable autoenrollment on Active Directory for the client machine to obtain a machine certificate. Server certificates can be requested using either the Windows Certification Authority or OPENSSL[1] utilities.

Q. What authorization policies does Cisco Secure ACS Express make available?

A. Cisco Secure ACS Express supports the authorization policies listed in Table 3.

Table 3. Cisco Secure ACS Express Authorization Policies

Feature	Description
Group mapping	Supports the mapping of external groups to determine entitlements for users or machines
Time based	Supports access based on time of day and day of week
RADIUS	Supports the returning of RADIUS attributes/values in an authentication response based on group mapping and time-based conditions
Machine access restrictions	Supports machine address restriction to require machine authentication as a prerequisite for successful user authentication
Service profile	Supports definition and application of a service profile, also known as a network access profile (NAP)

[1] This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more details please visit the following website: http://www.openssl.org/

Q. What password policies does Cisco Secure ACS Express provide for internal users?

A. Cisco Secure ACS Express supports the password policies for internal users listed in Table 4.

Table 4. Cisco Secure ACS Express Password Policies for Internal Users

Password Policy	Description
Minimum Length	Specifies the minimum acceptable password length.
Uppercase Required	Specifies whether an uppercase character is required in a user password. Default is true.
Lowercase Required	Specifies whether a lowercase character is required in a user password. Default is true.
Number Required	Specifies whether a number is required in a user password. Default is true.
Disallow Username	Indicates whether you can use your username for a user password. Default is true, disallowing username as password.
Cannot Reuse Last Password	Indicates whether you can use your most recent password. Default is true, meaning that you cannot reuse your last password after it has expired.
Enable Password Lockout after N Attempts	Specifies whether there is a maximum number of failed password attempts. Default is true.
Number of Failed Attempts	Specifies the number of failed attempts before user is locked out of the system; defaults to 8. After a user has been locked out due to exceeding the specified number of failed attempts, an administrator must reactivate the user account before it can be used again.

Q. Can I use Cisco Secure ACS Express for high availability?

A. Yes, Cisco Secure ACS Express supports high availability between a Cisco Secure ACS Express pair.

This allows customers to achieve redundancy if one Cisco Secure ACS Express server is unavailable from a network device point of view.

Q. If I need to deploy Cisco Secure ACS Express across more than two sites, how would I distribute my configuration?

A. Cisco Secure ACS Express provides a mechanism to export configurations that can be modified and imported back to the same Cisco Secure ACS Express or another Cisco Secure ACS Express in the network. Customers can use the CLI to export a configuration file, make changes as desired per site, and import the configuration into the destination Cisco Secure ACS Express server.

Q. We have an existing back-end database where our user repository resides. Would I be able to integrate with it?

A. Yes, Cisco Secure ACS Express supports Microsoft Active Directory, LDAP, and OTP servers.

For more details, please refer to the users guide at http://www.cisco.com/go/acsexp.

Q. Does Cisco Secure ACS Express support Active Directory natively or is integration required?

A. Cisco Secure ACS Express allows users to authenticate against Active Directory seamlessly. There is no need to install or configure any agent on either the Cisco Secure ACS Express appliance or any other server to interact with Active Directory.

Administration

Q. What administrative features are available within Cisco Secure ACS Express?

A. Table 5 lists the administrative features in Cisco Secure ACS Express.

Table 5. Cisco Secure ACS Express Administrative Features

Feature	Description
Web and CLI	Cisco Secure ACS Express can be securely administrated from the Web GUI (HTTPS) or through the scriptable CLI. These administrative interfaces provide flexibility in remotely managing individual Cisco Secure ACS Express appliances directly or in bulk through automated scripts.
Administrator access control	Provides two-level access: administrators and operators; restricts operators to read-only access to specific pages.
Password policies	Supports password expiration, forced change, and lockout. Password policy applies to administrator authentication to Cisco Secure ACS Express.
Logging	Supports RADIUS accounting logs, debug logs, and backup of the logs off the machine.
Reporting	Provides usage reports.

Q. What password policies are available for ACS view administrators?

A. Cisco Secure ACS Express provides a password policy applicable to ACS administrators. The policy is made up of rules that define the password complexity and password lockout.

Table 6 highlights that policy.

Table 6. Cisco Secure ACS Express Password Policy for ACS Administrators

Feature	Description
Password Complexity	
Lowercase Characters	Check to require lowercase characters in passwords.
Uppercase Characters	Check to require uppercase characters in passwords.
Numbers	Check to require numbers in passwords.
Minimum Password Length	Number (1–999) specifies the minimum password length.
Disallow Username in Password	Check to disallow passwords that contain the user's username.
Disallow Reuse of Previous Password	Check to disallow a user to use his or her previous password.
Password Expiration Enabled	Check box; enables password expiration and password lockout.
Expiration Days	Number of days until a password expires.
Password Lockout Policy	
Password Never Locked Out	Check box; when checked, this eliminates password lockout and allows an unlimited number of unsuccessful login attempts.
Number of Invalid Logins	Number (1–999) of invalid login attempts before password lockout occurs.

Q. Can ACS Express be upgraded remotely?

A. Cisco Secure ACS Express can be upgraded and patched remotely. This helps enable administrators to remotely manage Cisco Secure ACS Express deployments.

Q. What reports are available within the product?

A. Cisco Secure ACS Express provides the following reports:

- Usage Summary Report
- Authentication Report
- Device Commands Report
- Accounting Logs

For more details on each of these reports, please refer to the user guide at http://www.cisco.com/go/acsexp.

Ordering Information

Q. How do I order Cisco Secure Access Control Server Express 5.0?

A. You can order Cisco Secure ACS Express 5.0 through your regular purchasing channels by ordering part number CSACS-5.0-EXP-K9.

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 C67-432903-01 02/08