



PRODUCT BULLETIN 3022

CISCO SECURE ACCESS CONTROL SERVER (ACS) FOR WINDOWS AND CISCO SECURE ACS SOLUTION ENGINE 3.3

PRODUCT OVERVIEW

Cisco® Secure Access Control Server (ACS) is a highly scalable, high-performance access control server that provides a comprehensive identity networking solution and secure user experience for Cisco intelligent information networks. As an important component of the [Cisco Identity-Based Networking Services \(IBNS\)](#) architecture, Cisco Secure ACS extends access security by combining authentication, user or administrator access, and policy control from a centralized identity networking framework, allowing for greater flexibility and mobility, increased security, and user productivity gains. Cisco Secure ACS supports a wide array of access connection types, including wired and wireless LAN, dialup, broadband, content, storage, voice over IP (VoIP), firewalls, and VPNs.

The Cisco Secure ACS is also an important component of [Cisco Network Admission Control](#). Cisco Network Admission Control (NAC) is a multiple-vendor program led by Cisco Systems® that focuses on limiting damage from emerging security threats such as viruses and worms. With NAC, customers can allow network access only to compliant and trusted endpoint devices (such as PCs, servers, and personal digital assistants [PDAs]) and can restrict the access of noncompliant devices. This innovation will help enable compliant endpoints or other system elements to report misuse emanating from rogue or infected systems during an attack. Cisco expects to use this intelligence to dynamically quarantine infected systems from the rest of the network and significantly reduce virus, worm, and blended threat propagation.

Cisco Secure ACS is available in two options: Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine—a one-rack-unit (1-RU), security-hardened appliance with a preinstalled Cisco Secure ACS license. The Cisco Secure ACS Solution Engine is a highly secure, OS-independent, and dedicated platform that offers a highly manageable access-control solution with an increasingly reduced setup and troubleshooting time. The Cisco Secure ACS Solution Engine is a highly reliable, ready-to-deploy authentication, authorization, and accounting (AAA) solution that increases total cost of ownership (TCO) protection through the high availability and simplified day-to-day operation and management of the Cisco Secure ACS service.

NEW FEATURES

Cisco Secure ACS Version 3.3 offers the following new features:

- Cisco Network Admission Control (NAC) support
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) support for wireless authentication
- Downloadable IP access-control lists (ACLs)
- Certification Revocation List (CRL) comparison for EAP-Transport Layer Security (EAP-TLS) authentication
- Machine Access Restriction (MAR) complementing 802.1X machine authentication
- Network Access Filtering (NAF) as a new shared-profile component
- Cisco Security Agent integration in Cisco Secure ACS Solution Engine
- Replication enhancements for allowing more granular user and group components selections

For more detailed information on these new capabilities, please refer to the Cisco Secure ACS for Windows data sheet at http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_literature.html.

UPGRADE PATHS

The Cisco Secure ACS 3.3 for Windows software kit will be available to existing Cisco Secure ACS for Windows 2.x and 3.x customers on July 6, 2004. Customers interested in purchasing these products can place orders through their normal sales channels beginning June 23, 2004.

Cisco Secure ACS 3.x customers with Cisco Software Application Support (SAS) can go to the Product Upgrade Tool at <http://www.cisco.com/upgrade> and request the service release kit for Cisco Secure ACS 3.3 beginning June 25, 2004.

Cisco Secure ACS 3.x customers who do not have Cisco SAS support can purchase the minor release update kit with part number CSACS-3.3-WINMR-K9 through normal Cisco Direct, Partner, and Reseller sales channels.

The Cisco Secure ACS Solution Engine 3.3 ships on a new appliance platform, the Cisco 1112 for Cisco Secure ACS Solution Engine. For more information about the availability of the Cisco 1111 platform, please refer to the end-of-sale bulletin at http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_alerts_troubleshooting.html. The Cisco Secure ACS Solution Engine 3.3 will be available on August 10, 2004 to existing Cisco Secure ACS Solution Engine customers and to Cisco Secure ACS for Windows 2.x and 3.x customers who want to migrate to the new solution engine. Customers interested in purchasing these products can place orders through their normal sales channels beginning July 27, 2004. Cisco Secure ACS Solution Engine 3.2 customers with Cisco SAS can go to the Product Upgrade Tool at <http://www.cisco.com/upgrade> and request the service release kit for their Cisco Secure ACS Solution Engine on the Cisco 1111 platform beginning June 25, 2004.

Cisco Secure ACS Solution Engine 3.2 customers on a Cisco 1111 platform who do not have Cisco SAS can purchase the minor release update kit with part number CSACSE-3.3-SWMR-K9 through normal Cisco Direct, Partner, and Reseller sales channels.

AVAILABILITY

The Cisco Secure ACS 3.3 for Windows will be available beginning July 2, 2004. Customers interested in purchasing these products can place orders through their normal sales channels beginning June 23, 2004.

The Cisco Secure ACS Solution Engine 3.3 will be available beginning August 10, 2004. Customers interested in purchasing these products can place orders through their normal sales channels beginning July 27, 2004.

ORDERING INFORMATION

Table 1 lists the ordering information for the Cisco Secure ACS 3.3 for Windows and Cisco Secure ACS Solution Engine 3.3.

Table 1. Ordering Information

Part Number	Description
CSACS-3.3WIN-K9	Cisco Secure ACS 3.3 for Windows
CSACS-3.3-WINUP-K9	Upgrade to Cisco Secure ACS 3.3 for Windows from versions 1.x, 2.x, 3.x, and Cisco Secure ACS for UNIX 2.x
CSACS-WNAPR05MR-K9	Minor release update to Cisco Secure ACS 3.3 for Windows software for existing Cisco Secure ACS 3.x customers—available May 2005
CSACSE-1112-K9	Cisco Secure ACS Solution Engine 3.3; includes Cisco 1112 hardware platform and Cisco Secure ACS Software 3.3
CSACSE-1112-UP-K9	Upgrade for customers using Cisco Secure ACS 3.x for Windows, Cisco Secure ACS for UNIX, or Cisco 1111 platform to the Cisco Secure ACS Solution Engine 3.3; includes Cisco 1112 hardware platform and Cisco Secure ACS Software 3.3
CSACSE-APR05MR-K9	Minor release update to Cisco Secure ACS Solution Engine 3.3. software for existing Cisco Secure ACS Solution Engine 3.2 and 3.3 customers—available May 2005

FOR MORE INFORMATION

For more information about the Cisco Secure Access Control Server, visit <http://www.cisco.com/go/acs>. For more information about Cisco Secure Access Control Server Solution Engine, visit <http://www.cisco.com/en/US/products/sw/secursw/ps5338/index.html> or contact your local account representative or send an e-mail to ACS-MKT@cisco.com.



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R) 205379.BB_ETMG_KW_7.05

