



Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine Version 3.3

June 28, 2007

Full Build Number: 3.3.3.11

Introduction

Because the number of devices that Cisco Secure ACS Solution Engine Version 3.3 interoperates with runs into the hundreds, this “supported devices” list differs significantly from those of other Cisco products with which you may be familiar. The relation of hardware to software Cisco Secure ACS Solution Engine Version 3.3 products is specified in [Supported Versions, page 2](#).

This document lists supported devices and software, that is, those that we have tested against. Finally, this document also lists devices and software programs that are, to the best of our knowledge, interoperable. Of the hundreds of devices and software programs that Cisco Secure ACS Solution Engine Version 3.3 interoperates with, Cisco officially supports only those that have been tested.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003. Cisco Systems, Inc. All rights reserved.

For details regarding other limitations and known problems see *Release Notes for CiscoSecure Access Control Server Appliance Version 3.3*. You can find the most recent version of all documentation at:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacsapp/csapp33/index.htm

This document contains the following sections:

- [Supported Versions, page 2](#)
- [Upgrades and Patches, page 3](#)
- [Third-party RADIUS and TACACS+ Clients, page 6](#)
- [Supported and Interoperable Devices and Software, page 7](#)

Supported Versions

[Table 1](#) details the Cisco Secure ACS software versions supported by each Cisco Secure ACS Solution Engine platform.

Table 1 *Supported Versions*

Cisco Secure ACS Solution Engine Platform	Cisco Secure ACS version 3.3	Cisco Secure ACS version 3.2
Cisco 1111	Yes ¹	Yes
Cisco 1112	Yes	No

1. To upgrade an existing Cisco 1111 platform to Cisco Secure ACS version 3.3, see [Upgrades and Patches, page 3](#).

Supported Migration Versions

We support migrating to Cisco Secure ACS Solution Engine version 3.3 from many versions of Cisco Secure ACS for Windows Server; however, migration requires upgrading Cisco Secure ACS for Windows Server to version 3.3.

For detailed steps for performing a migration from Cisco Secure ACS for Windows Server to Cisco Secure ACS Solution Engine, see either of the following two documents:

- *Installation Guide for Cisco Secure ACS for Windows Server*, version 3.3
- *Installation and Configuration Guide for Cisco Secure ACS Solution Engine*, version 3.3

Upgrades and Patches

Upgrading to Cisco Secure ACS Version 3.3

See [Release Notes for Cisco Secure ACS Solution Engine Version 3.3](#) for the procedure to upgrade your Cisco Secure ACS software to version 3.3.

Security Patch Process

For information about our process for evaluating and releasing Microsoft security patches for Cisco Secure ACS Solution Engine, see *Cisco Secure ACS Solution Engine Security Patch Process*, available in the Product Literature section for Cisco Secure ACS Solution Engine on cisco.com.

Remote Agent Support

Cisco Secure ACS 3.3 supports Cisco Secure ACS Remote Agent on Microsoft Windows 2000 and Solaris operating systems, as specified in the following two sections.

- [Windows Support for Remote Agent, page 4](#)
- [Solaris Support for Remote Agent, page 6](#)

The list of tested patches will be updated as additional patches are identified and tested.

Windows Support for Remote Agent

The computer running Cisco Secure ACS Remote Agent for Windows must use an English-language version of one of the following operating systems:

- Windows 2000 Server, with Service Pack 4 installed
- Windows 2000 Advanced Server, with the following conditions:
 - with Service Pack 4 installed
 - without features specific to Windows 2000 Advanced Server enabled
- Windows Server 2003, Enterprise Edition with Service Pack 1 installed
- Windows Server 2003, Standard Edition with Service Pack 1 installed

The following restrictions apply to support for Microsoft Windows operating systems:

- We have not tested and cannot support the multi-processor feature of any supported operating system.
- We cannot support Microsoft clustering service on any supported operating system.
- Windows 2000 Datacenter Server is not a supported operating system.

Tested Windows Security Patches



Note

For information about remote agent support for Microsoft patches issued after the release of Cisco Secure ACS Solution Engine version 3.3, see *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine*, version 3.3.

We tested Cisco Secure ACS Remote Agent for Windows with the Windows Server 2003 patches documented in the following Microsoft Knowledge Base Articles:

- [819696](#)
- [823182](#)
- [823559](#)
- [824105](#)

- [824141](#)
- [824146](#)
- [825119](#)
- [828028](#)
- [828035](#)
- [828741](#)
- [832894](#)
- [835732](#)
- [837001](#)
- [837009](#)
- [839643](#)
- [840374](#)

We tested Cisco Secure ACS Remote Agent for Windows with the Windows 2000 Server patches documented in the following Microsoft Knowledge Base Articles:

- [329115](#)
- [823182](#)
- [823559](#)
- [823980](#)
- [824105](#)
- [824141](#)
- [824146](#)
- [825119](#)
- [826232](#)
- [828035](#)
- [828741](#)
- [828749](#)
- [835732](#)
- [837001](#)
- [839643](#)

Solaris Support for Remote Agent

The computer running Cisco Secure ACS Remote Agent for Solaris must use Solaris 2.8.

Third-party RADIUS and TACACS+ Clients

With regard to third-party RADIUS and TACACS+ clients, Cisco Secure ACS Solution Engine fully interoperates with devices that adhere to the governing protocols. Also, support for RADIUS and TACACS+ functions depends on device-specific implementation. On a given device, TACACS+ may not be available for user authentication and authorization. Likewise, RADIUS may not be available for administrative authentication and authorization.

For RADIUS these include the following RFCs:

- [RFC 2138 - Remote Authentication Dial In User Service \(RADIUS\)](#)
- [RFC 2139 - RADIUS Accounting](#)
- [RFC 2865 - Remote Authentication Dial In User Service \(RADIUS\)](#)
- [RFC 2866 - RADIUS Accounting](#)
- [RFC 2867 - RADIUS Accounting for Tunnel Protocol Support](#)
- [RFC 2868 - RADIUS Attributes for Tunnel Protocol Support](#)
- [RFC 2869 - RADIUS Extensions](#)

For details regarding the implementation of vendor-specific attributes (VSAs), see *User Guide for Cisco Secure ACS Solution Engine Version 3.3*.

Cisco Secure ACS Solution Engine conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.77.

Supported and Interoperable Devices and Software

The following tables show the devices and software that Cisco Secure ACS Solution Engine supports or with which it interoperates:

- [Table 2, Web Browsers](#)
- [Table 3, Device Operating Systems](#)
- [Table 4, Routers](#)
- [Table 5, Access Devices/Universal Gateways](#)
- [Table 6, Cable Devices](#)
- [Table 7, Content Networking Devices](#)
- [Table 8, Security and VPN Devices](#)
- [Table 9, Storage Networking Devices](#)
- [Table 10, Switches](#)
- [Table 11, Cisco Aironet Software \(Access Points for Wireless LAN\)](#)
- [Table 12, CiscoWorks VMS](#)
- [Table 13, PKI/Certificate Servers](#)
- [Table 14, Token Servers](#)
- [Table 15, LDAP Servers](#)
- [Table 16, User Databases](#)
- [Table 17, Proxy Support](#)

You can find information about new device support at Cisco.com, <http://www.cisco.com>.

To ensure full capabilities, the clients you deploy to interoperate with Cisco Secure ACS Solution Engine should use the most recent operating systems available. Nonetheless, [Table 3](#) provides details on the minimum acceptable client operating system versions.

Table 2 *Web Browsers¹*

Program	Versions	Notes
Microsoft Internet Explorer	Version 6.0 with Service Pack 1 for Microsoft Windows—English Language version Microsoft Java Virtual Machine	Tested
Microsoft Internet Explorer	Version 6.0 with Service Pack 1 for Microsoft Windows—English Language version Sun Java Plug-in 1.4.2_04	Tested
Netscape Communicator for Microsoft Windows	Version 7.1 for Microsoft Windows - English Language version Sun Java Plug-in 1.4.2_04	Tested
Netscape Communicator for Solaris 2.8	Version 7.0 English Language version Mozilla 5.0 Sun Java Plug-in 1.4.0_01	Tested

1. To use a web browser to access the Cisco Secure ACS HTML interface, you must enable both Java and JavaScript in the browser. Also, you must disable HTTP proxy in the browser.

Table 3 *Device Operating Systems*

Operating System	Minimum Version	Notes
IOS	11.2	For full RADIUS support
CAT OS	7.2	Cisco products—and other third-party products that are RFC compliant—will work with Cisco Secure ACS even when running earlier versions of CAT OS. However, full functionality, including the 802.1x VLAN assignment, is supported only when the listed version is used.

Table 4 Routers

Series	Notes
Cisco 1400	End of life (EOL) status
Cisco 1600	RADIUS and TACACS+ interoperability
Cisco 1700	Tested with IOS 12.2(8) RADIUS and TACACS+ interoperability
Cisco 2500	EOL status
Cisco 2600	RADIUS and TACACS+ interoperability
Cisco 3600	RADIUS and TACACS+ interoperability
Cisco 3700	Tested with IOS 12.2 RADIUS and TACACS+ interoperability
Cisco 7100	RADIUS and TACACS+ interoperability
Cisco 7200	Tested with IOS 12.2 RADIUS and TACACS+ interoperability
Cisco 7300	RADIUS and TACACS+ interoperability
Cisco 7400	RADIUS and TACACS+ interoperability
Cisco 7500	RADIUS and TACACS+ interoperability
Cisco 10000	RADIUS interoperability
Cisco 10720	RADIUS and TACACS+ interoperability

Table 5 Access Devices/Universal Gateways

Series	Notes
6400 Series	RADIUS and TACACS+ interoperability
AS2600 Series	RADIUS and TACACS+ interoperability
AS5350 Series	RADIUS and TACACS+ interoperability
AS5300 Series	Tested on version 3.3. RADIUS and TACACS+ interoperability

Table 5 *Access Devices/Universal Gateways (continued)*

Series	Notes
AS5400 Series ¹	Tested with IOS12.2(7c) RADIUS and TACACS+ interoperability
AS5850 Series	RADIUS and TACACS+ interoperability
DSL Series / 6015, 6100, 6130, 6160, 6260	RADIUS and TACACS+ interoperability
MGX Series / 8220, 8250, 8800, 8950	TACACS+ interoperability

1. This series, tested on version 3.2, not retested on version 3.3.

Table 6 *Cable Devices*

Devices	Notes
uBR7100 ¹	Tested with IOS 12.2BC RADIUS and TACACS+ interoperability

1. Tested on version 3.2, not retested on version 3.3.

Table 7 *Content Networking Devices¹*

Series / Devices	Notes
CE7300 / CE 7320	Tested with ACNS 4.2 RADIUS and TACACS+ interoperability
CDM4600 / CDM4630, CDM4650	RADIUS and TACACS+ interoperability
4400 Content Routers/ CR4430	Tested with ACNS 4.2 RADIUS and TACACS+ interoperability

1. Tested on version 3.2, not retested on version 3.3.

Table 8 Security and VPN Devices

Series / Devices	Notes
3000 Series Concentrator / 3005, 3015, 3030, 3060, 3080	Tested with 3015 RADIUS and TACACS+ interoperability
PIX 500 Series Firewall / 501, 506E, 515, 515E, 525, 535	Tested with 515 and PIX OS v6.3 RADIUS and TACACS+ interoperability
5000 Series Concentrator	EOL status

Table 9 Storage Networking Devices

Series	Devices Supported	Notes
MDS 9000	MDS 9216, MDS9509	RADIUS interoperability (TACACS+ support in future release)

Table 10 Switches

Series / Devices	Notes
Catalyst 2950/3550	Tested with 3550 and IOS 12.1(12)EA1 RADIUS and TACACS+ interoperability
Catalyst 4000/4500	Tested with Cat4503, CatOS 7.5, and IOS 12.1 RADIUS and TACACS+ interoperability
Catalyst 5000	EOL status
Catalyst 6500	Tested with CatOS 7.5, and IOS 12.1 RADIUS and TACACS+ interoperability

Table 11 Cisco Aironet Software (Access Points for Wireless LAN)

Series	Notes
AP1100	RADIUS interoperability with IOS v12.2(15)JA
AP1200	RADIUS interoperability with IOS v12.2(15)JA

Table 12 CiscoWorks VMS

Series	Devices Supported	Notes
IOS/Router MC	Version 1.3	TACACS+ interoperability
Firewall MC	Version 1.1	Tested with VMS2.1 TACACS+ interoperability
IDS MC	Version 1.1	TACACS+ interoperability
LMS	—	TACACS+ interoperability (future release)
HSE	Version 1.7	TACACS+ interoperability
WLSE	—	TACACS+ interoperability (future release)

Table 13 PKI/Certificate Servers

Platform	Versions	Notes
Microsoft CA Certificate Server	Windows 2000 Windows 2000 with SP3	Tested
Entrust PKI	Version 6.0	—
Verisign Onsite	Version 5.0	—

Table 14 Token Servers¹

Platform	Versions	Client Requirement	Notes
ActivCard Server	Version 3.1	—	—

Table 14 Token Servers¹ (continued)

CRYPTOCard CRYPTOAdmin	Version 5.16	—	—
PassGo Defender	Version 4.1.3	—	—
RSA ACE/Server	Version 5.1 and 5.2	—	Tested
Safeword Premier Access	Version 3.1	—	—
Vasco Vacman Server	Version 6.0.2	—	—

1. Cisco Secure ACS Solution Engine uses a RADIUS interface to support all token servers.

Table 15 LDAP Servers

Platform	Versions	Notes
SunONE Identity Server (Formerly iPlanet Directory)	Version 5.2	Tested with Windows 2000 Active Directory with Windows Service Pack 3
Novell NetWare Directory Services (NDS)	Version 6.0	Tested
Novell eDirectory	Version 8.6	Tested

Table 16 User Databases¹

Platform	Version	Requirement
AD on Windows 2003	—	Tested with Service Pack 1
AD on Windows 2000	—	Tested with Service Pack 3
SAM on Windows 2000	—	Tested with Service Pack 3
SAM on Windows NT 4.0	—	—
LDAP	Generic	—

Table 16 *User Databases¹ (continued)*

Novell NetWare Directory Services (NDS)	Version 6.0	Tested with eDirectory v.8.6 and Novell Client 4.83 SP2 for Windows NT 4.0, Windows 2000, and Windows XP
LEAP Proxy RADIUS servers	—	Tested

1. See also [Table 14](#).

Table 17 *Proxy Support*

Platform	Versions	Notes
Cisco Secure ACS		Tested with version 3.3
Funk Steel Belted Radius	Enterprise Edition	—