



Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Release 4.1

Revised: December 2006, OL-9973-01

Introduction

The Cisco Secure Access Control Server Release 4.1, hereafter referred to as ACS, works with hundreds of devices. Given the number of devices, this device list might significantly differ from the device lists associated with other Cisco products.

Use this list to find:

- Tested devices and software that we support.
- Interoperable devices and software.



Note

Cisco officially supports only tested devices and software.

For information on ACS SE hardware platforms and supported ACS software versions, see [Supported ACS Software Versions on the ACS SE](#), page 4. For details regarding limitations and known problems, see the *Release Notes for Cisco Secure ACS Release 4.1*.

This document contains the following sections:

- [Tested Network Elements and Software](#), page 2
- [Supported ACS Software Versions on the ACS SE](#), page 4
- [Supported Operating Systems](#), page 4
- [Remote Agent Support](#), page 5
- [Supported Upgrades for ACS for Windows](#), page 5
- [Supported Upgrades for ACS SE](#), page 5
- [Supported Migrations for ACS SE](#), page 5



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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Tested Windows Security Patches, page 6](#)
- [Third-Party RADIUS and TACACS+ Clients, page 7](#)
- [Supported and Interoperable Devices and Software, page 8](#)

Tested Network Elements and Software

This section lists the network elements and software that were tested with ACS 4.1.

Tested Network Elements

Cisco has tested the following network elements:

- Routers
 - Cisco 800
 - Cisco 1600
 - Cisco 1700
 - Cisco 2600
 - Cisco 3600
 - Cisco 3810
 - Cisco 7100
 - Cisco 7200
 - Cisco uBR7114E
 - Cisco AS5300
- Switches
 - Catalyst 3550
 - Catalyst 4500
 - Catalyst 6500/Cisco 7600
- Security Appliances
 - PIX 500 Series Firewall
 - VPN 3000
- Wireless Access Points
 - AP350
 - AP1100
 - AP1200
 - Airespace controller

Tested Software

Cisco has tested the following Cisco and third-party software:

- Cisco Trust Agent (CTA), v.2.x
- Microsoft IIS 5.0
- Microsoft IIS 6.0
- Microsoft Internet Explorer, v.6.0 (SP1)
- Microsoft OS (Windows 2000 Server SP4, Windows 2003 Standard Edition, Windows 2003 Enterprise Edition)
- Microsoft SQL server v.7.5
- Microsoft SQL server v8.0
- NAI VirusScan Enterprise, v.8.0
- Netscape Communicator for Microsoft Windows, v.8.0
- Oracle 9i Database
- Red Hat Linux Enterprise, v.3.0 WS
- RSA ACE/Server, v.6.0
- Safeword Premier Access, v.3.1
- Secure RSA agent for Windows, v.5.6
- Secure RSA Server (OTP), v.5.2
- Solaris 8 for SPARC
- SunONE Identity Server (Formerly iPlanet Directory), v.5.2
- Supplicants for supported protocols (1 for each)
- Third-party Auditing Servers (tested with QualysGuard Appliance by Qualys and Wholesecurity by Symantec)
- Trend Micro Antibody Server Corporate Edition, v.6.5
- Trend Micro OfficeScan Server Corporate Edition, v.6.5
- VMware ESX Server
- Win XP(SP2) and a Hotfix for the MS PEAP fast reconnect defect, for dialup clients used as 802.1x supplicants

Supported ACS Software Versions on the ACS SE

Table 1 indicates the Cisco Secure ACS software versions that each Cisco Secure ACS SE platform supports.

Table 1 *Supported Versions*

Cisco Secure ACS Solution Engine Platform	Cisco Secure ACS version 4.0 and 4.1	Cisco Secure ACS version 3.3	Cisco Secure ACS version 3.2
Cisco 1111	Yes	Yes ¹	Yes
Cisco 1112	Yes ²	Yes	No
Cisco 1113	Yes	No	No

1. To upgrade an existing Cisco 1111 platform to Cisco Secure ACS version 3.3, see [Supported Upgrades for ACS SE, page 5](#)
2. To upgrade an existing Cisco 1112 or 1113 platform to Cisco Secure ACS version 4.x, see [Supported Upgrades for ACS SE, page 5](#).

Supported Operating Systems

ACS supports the following Windows operating systems. The operating system and the service pack must be English-language versions.

- Windows 2000 Server, with Service Pack 4 installed
- Windows 2000 Advanced Server
 - 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



Note

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

- We have not tested and cannot support the multiprocessor feature of any supported operating system. However, we did test ACS with dual-processor computers.
- We cannot support the Microsoft clustering service on any supported operating system.
- We do not support Windows 2000 Datacenter Server.

When running ACS on Windows Server 2003, you might encounter event messages that falsely indicate that ACS services have failed. Bug CSCea91690 documents this issue. For details, see the *Release Notes for Cisco Secure ACS Release 4.1*.

Remote Agent Support

Cisco Secure ACS 4.1 supports Cisco Secure ACS Remote Agent on the Microsoft Windows and Solaris operating systems. The following sections describe ACS Remote Agent support.

Windows Support for the Remote Agent

The Remote Agent runs on following English-language versions of the Windows operating system and service pack:



Note

You must use only English-language versions of the operating system and the service pack.

Supported Upgrades for ACS for Windows

We tested upgrades to Cisco Secure ACS for Windows Server 4.1 from releases 3.3.3, 3.3.2, 3.3.1*, 3.2.3, 3.2.2*, 3.2.1*, 3.1.2*, and 3.04*.

*First upgrade to Cisco Secure ACS for Windows Server, release 3.3.3, then upgrade to release or 4.1.

Supported Upgrades for ACS SE

We tested upgrades of the Solution Engine from releases 3.2.3 and 3.3.3 to release 4.0, 4.01, and 4.1. To upgrade the Solution Engine from an earlier release (3.2.1, 3.2.2, 3.3.1, and 3.3.2), you must first upgrade to release 3.3.3 and then upgrade to release 4.0, 4.0.1, or 4.1. For more information, see *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.

Supported Migrations for ACS SE

We support migration from ACS for Windows releases 3.0.4, 3.1.2, 3.2.3, 3.3.3, and 4.0 to release 4.0, 4.0.1, or 4.1 of the ACS Solution Engine. To migrate from an earlier release of ACS for Windows (3.3.1, 3.3.2, 3.2.2, 3.2.1, 3.1.2, and 3.0.4), you must first upgrade to release 3.3.3 and then upgrade to release 4.0, 4.0.1, or 4.1. For more information, see *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.

Solaris Support for the Remote Agent

The Cisco Secure ACS Remote Agent for Solaris runs on Solaris 2.8.



Note

The Solaris Remote Agent requires the *libstdc++.so* library (C++ runtime). Without this library, the Remote Agent is not operational. The default path is set in the environment variable *LD_LIBRARY_PATH* and the directory */router/lib*.

Tested Windows Security Patches

**Note**

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

Security Patch Process

Cisco Systems officially supports and encourages the installation of all Microsoft security patches for Windows 2000 Server and Windows Server 2003 when they are used with Cisco Secure ACS.

Cisco experience has shown that these patches do not cause problems with the operation of Cisco Secure ACS. If the installation of security patches does cause a problem with Cisco Secure ACS, contact the Cisco TAC and we will resolve the problem as quickly as possible.

For information about our process for evaluating and releasing Microsoft security patches for Cisco Secure ACS, see the Cisco Secure ACS Q&A area in the Product Literature area for the Cisco Secure Access Control Server Solution Engine at <http://www.cisco.com>.

Windows Server 2003 Patches

We tested ACS with the following Windows Server 2003 patches:

- 819696
- 823182
- 823559
- 824105
- 824141
- 824146
- 825119
- 828028
- 828035
- 828741
- 832894
- 835732
- 837001
- 837009
- 839643
- 840374

Windows 2000 Server Patches

We tested ACS with the following Windows 2000 Server patches:

- 329115
- 823182
- 823559
- 823980
- 824105
- 824141
- 824146
- 825119
- 826232
- 828035
- 828741
- 828749
- 835732
- 837001
- 839643

Third-Party RADIUS and TACACS+ Clients

ACS fully interoperates with third-party RADIUS and TACACS+ client devices that adhere to the governing protocols. Support for RADIUS and TACACS+ functions depends on the device-specific implementation. For example, on a specific device:

- TACACS+ might not be available for user authentication and authorization.
- RADIUS might not be available for administrative authentication and authorization.

For TACACS+ devices, ACS conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.78, which is available at <http://www.cisco.com>.

For RADIUS, ACS conforms to 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



Note

For details regarding the implementation of vendor-specific attributes (VSAs), see the *User Guide for Cisco Secure ACS 4.1*.

For TACACS+ devices, ACS conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.78, which is available at <http://www.cisco.com>.

Supported and Interoperable Devices and Software

This section contains the following tables and sections:

- [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 17, User Databases](#)
- [Table 18, Proxy Support](#)
- [VMWare ESX Server Support, page 14](#)

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



Note

To ensure full ACS capabilities, you must use the most recent operating system release on the clients that you deploy. See [Table 3, Device Operating Systems](#), for the minimum acceptable client operating system versions.

Table 2 **Web Browsers¹**

Program	Versions	Notes
Microsoft Internet Explorer	Version 6.0 • Service Pack 1 for Microsoft Windows (English and Japanese Language versions) • Sun Java Plug-in, v.1.4.2_04	Tested

Table 2 *Web Browsers¹ (continued)*

Microsoft Internet Explorer	Version 5.5 • Service Pack 1 for Microsoft Windows • Japanese Language version • Sun Java Plug-in, v.1.4.2_04	Not Tested
Netscape Communicator	Version 8.0 for Microsoft Windows • English Language version • Sun Java Plug-in, v.1.4.2_04 Version 7.1 for Microsoft Windows • Japanese Language version • Sun Java Plug-in, v.1.4.2_04	Tested
Netscape Communicator	Versions 7.0, 7.1, and 7.2 for Microsoft Windows • English and Japanese Language versions • Sun Java Plug-in, v.1.4.2_04	Not Tested

1. To use a web browser to access the ACS web interface, you must enable Java and JavaScript in the browser. You must also disable the HTTP proxy in the browser.

Table 3 *Device Operating Systems*

Operating System	Minimum Version	Notes
PIX	515E	PixOS 7.0(3)
IOS	11.2	For full RADIUS support.
CatOS	7.2	Cisco products—and other third-party products that are RFC compliant—will work with ACS when running earlier versions of CatOS. However, full functionality, including the 802.1x VLAN assignment, is supported only when using the listed version.

Table 4 *Routers*

Series	Notes
Cisco 1400	End-Of-Life (EOL) Status
Cisco 1600	RADIUS and TACACS+ interoperability
Cisco 1700	RADIUS and TACACS+ interoperability
Cisco 2500	EOL
Cisco 2600	RADIUS and TACACS+ interoperability
Cisco 3600	RADIUS and TACACS+ interoperability
Cisco 3700	RADIUS and TACACS+ interoperability

Table 4 **Routers (continued)**

Cisco 7100	RADIUS and TACACS+ interoperability
Cisco 7200	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	RADIUS and TACACS+ interoperability
AS5400 Series ¹	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. Tested on version 3.2, not retested on version 3.3.

Table 6 **Cable Devices**

Devices	Notes
uBR7100 ¹	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	RADIUS and TACACS+ interoperability
CDM4600/CDM4630, CDM4650	RADIUS and TACACS+ interoperability
4400 Content Routers/CR4430	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 v6.5 RADIUS and TACACS+ interoperability
5000 Series Concentrator	EOL Status

Table 9 **Storage Networking Devices**

Series	Devices Supported	Notes
MDS 9000	MDS 9216, MDS9509	RADIUS and TACACS+ interoperability

Table 10 **Switches**

Series/Devices	Notes
Catalyst 3550	Tested with IOS 12.1(13)EA1a RADIUS and TACACS+ interoperability
Catalyst 4500	Tested with IOS 12.2(25)SG(1.93) RADIUS and TACACS+ interoperability
Catalyst 5000	EOL status
Catalyst 6500	Tested with CatOS 8.5.0(114)JAC RADIUS and TACACS+ interoperability
Catalyst 7600	Tested with CatOS 8.5.0(114)JAC  Note You can run CatOS on the supervisor engine installed in a 7600-series chassis. Cisco does not market the 7600 series with the CatOS. RADIUS and TACACS+ interoperability

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

Series	Notes
AP1100	RADIUS interoperability with IOS v12.3(4)JA
AP1200	RADIUS interoperability with IOS v12.3(4)JA

Table 12 *CiscoWorks VMS*

Series	Version	Notes
IOS/Router MC	1.3.1	Tested with VMS 2.3 TACACS+ interoperability
Firewall MC	1.3	Tested with VMS2.3 TACACS+ interoperability
IDS MC	1.1	TACACS+ interoperability
HSE	1.7	TACACS+ interoperability

Table 13 *PKI/Certificate Servers*

Platform	Versions	Notes
Microsoft CA Certificate Server	Windows 2000 Windows 2000 with Service Pack 4 Windows 2003 Enterprise and Standard editions	Tested
Entrust PKI	6.0	Not Tested
Verisign Onsite	5.0	Not Tested

Table 14 *Token Servers¹*

Platform	Version	Client Requirement	Notes
ActivCard Server	3.1	—	Not Tested
CRYPTOCARD CRYPTOAdmin	5.16	—	Not Tested
PassGo Defender	4.1.3	—	Not Tested
RSA ACE/Server	6.0	—	Tested
RSA ACE/Server	5.2	—	Tested
Safeword Premier Access	3.1	—	Not Tested
Vasco Vacman Server	6.0.2	—	Not Tested

1. Cisco Secure ACS uses a RADIUS interface to support all token servers, with the exception of the RSA ACE/Server. For more information, see [Changes to Token Server Support](#).

Table 15 *LDAP Servers*

Platform	Version	Notes
SunONE Identity Server	5.2	Tested with Windows 2003, Enterprise Edition Tested with Solaris 8
Microsoft Active Directory		Tested with Windows 2003, Enterprise Edition
Open-LDAP	2.2.23	Tested with RedHat Enterprise Linux AS, Release 3 Tested with Open-SSL 0.9.7e

Table 15 *LDAP Servers (continued)*

Novell NetWare Directory Services (NDS)	6.5	Not tested with ACS 4.1
Novell eDirectory	8.7.1	Not tested with ACS 4.1

Table 16 *User Databases¹*

Platform	Version	Requirement
AD on Windows 2003	—	Tested with Service Pack 1
AD on Windows 2000	—	Tested with Service Pack 4
SAM on Windows 2000	—	Tested with Service Pack 4
SAM on Windows NT 4.0	—	Not Tested
LDAP	Generic	See Table 15 .
Novell NetWare	Version 6.5	Not Tested
Open Database Connectivity (ODBC)-compliant relational databases	—	In addition to the Windows ODBC interface, the third-party ODBC driver must be installed on the ACS server.
LEAP Proxy RADIUS servers	—	Tested

1. See also [Table 14, Token Servers](#).

Table 17 *User Databases¹*

Platform	Version	Requirement
AD on Windows 2003	—	Tested with Service Pack 1
AD on Windows 2000	—	Tested with Service Pack 4
SAM on Windows 2000	—	Tested with Service Pack 4
SAM on Windows NT 4.0	—	Not Tested
LDAP	Generic	See Table 15
Novell NetWare	6.5	Not Tested
LEAP Proxy RADIUS servers	—	Tested

1. See also [Table 14, Token Servers](#).

Table 18 *Proxy Support*

Platform	Version	Notes
Cisco Secure ACS	—	Tested with version 4.1
Funk Steel Belted Radius	Enterprise Edition	Not Tested

VMWare ESX Server Support

ACS 4.1 has been tested on the VMWare ESX server with the following configuration:

- VMWare ESX Server 3.0.0
- 16 GB of RAM
- AMD Opteron Dual Core processor
- 300 GB hard drive
- Four virtual machines
- Windows 2000 3.0 Standard Edition
- 3 GB of RAM for the guest operating system

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, 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, 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, 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. (0601R)