



Supported and Interoperable Devices and Software Tables for Cisco Secure Access Control Server for Windows Version 4.0

Revised: June 26, 2007, OL-7466-03

Introduction

Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, works with hundreds of devices. Given the number of devices, this device list might significantly differ from other Cisco products.

You 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. However, Cisco also supports any standard TACACS+ or RADIUS client.

For details regarding other limitations and known problems, see the [Release Notes for Cisco Secure Access Control Server for Windows](#).

This document contains the following sections:

- [Supported Network Elements and Software, page 2](#)
- [Supported Operating Systems, page 3](#)
- [Supported Upgrades, page 4](#)
- [Tested Windows Security Patches, page 4](#)
- [Third-party RADIUS and TACACS+ Clients, page 5](#)
- [Supported and Interoperable Devices and Software, page 6](#)



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

© 2005 Cisco Systems, Inc. All rights reserved.

Supported Network Elements and Software

This section lists the network elements and software that have been tested with ACS 4.0.

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

Cisco has not tested the following network elements:

- Routers:
 - Cisco 1800
 - Cisco 2800
 - Cisco 3800
- Switches:
 - Catalyst 3560
 - Catalyst 3750

Software

Cisco has tested the following third-party software:

- Cisco Trust Agent (CTA) v.2.x
- Microsoft IIS 5.0
- Microsoft IIS 6.0
- Microsoft Internet Explorer Version 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 8.0
- Netscape Communicator for Microsoft Windows v.8.0
- Novell Directory Netware 6.5
- Novell NDS eDirectory - Version 8.6
- Oracle 9i Database
- Red Hat Linux Enterprise v3.0 WS
- RSA ACE/Server v6.0
- Safeword Premier Access - Version 3.1, 3.2
- Secure RSA agent for Windows v.5.6
- Secure RSA Server (OTP) v.5.2
- Solaris 8 for SPARC
- Sun Java Plug-in 1_5_0_02
- SunONE Identity Server (Formerly iPlanet Directory) - Version 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 6.5
- Trend Micro OfficeScan Server Corporate Edition 6.5
- Win XP(SP2) and a Hotfix for the MS PEAP fast reconnect defect, for dialup client and used as 802.1x supplicants

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.
- Windows 2000 Datacenter Server is not a supported operating system.

When running ACS on Windows Server 2003, you may encounter event messages that falsely indicate that ACS services have failed. This issue is documented in bug CSCea91690. For details, see the [Release Notes for Cisco Secure Access Control Server for Windows](#).

Supported Upgrades

We tested upgrades to Cisco Secure ACS for Windows Server, 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 4.0.

Tested Windows Security Patches

**Note**

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

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

Cisco experience has shown that these patches do not cause any problems with the operation of Cisco Secure ACS for Windows. If the installation of one of these security patches does cause a problem with Cisco Secure ACS, please contact Cisco TAC and Cisco 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 ACS at <http://www.cisco.com>.

We tested ACS 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 ACS 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](#)

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 Access Control Server for Windows*.

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

The following tables show the supported and interoperable devices and software:

- [Table 1, Web Browsers](#)
- [Table 2, Device Operating Systems](#)
- [Table 3, Routers](#)
- [Table 4, Access Devices/Universal Gateways](#)
- [Table 5, Cable Devices](#)
- [Table 6, Content Networking Devices](#)
- [Table 7, Security and VPN Devices](#)
- [Table 8, Storage Networking Devices](#)
- [Table 9, Switches](#)
- [Table 10, Cisco Aironet Software \(Access Points for Wireless LAN\)](#)
- [Table 11, CiscoWorks VMS](#)
- [Table 12, PKI/Certificate Servers](#)
- [Table 13, Token Servers](#)
- [Table 14, LDAP Servers](#)
- [Table 15, User Databases](#)
- [Table 16, Proxy Support](#)

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 2, Device Operating Systems](#), for the minimum acceptable client operating system versions.

Table 1 **Web Browsers¹**

Program	Versions	Notes
Microsoft Internet Explorer	Version 6.0 <ul style="list-style-type: none"> • Service Pack 1 for Microsoft Windows (English and Japanese Language versions) • Microsoft Java Virtual Machine (JVM, version 5.00.3810) • Sun Java Plug-in, version 1.5 	Tested
Microsoft Internet Explorer	Version 5.5 <ul style="list-style-type: none"> • Service Pack 1 for Microsoft Windows • Japanese Language version • Sun Java Plug-in, version 1.4.2_04 	Not Tested
Netscape Communicator	Version 8.0 for Microsoft Windows <ul style="list-style-type: none"> • English Language version • Sun Java Plug-in, version 1.5 Version 7.1 for Microsoft Windows <ul style="list-style-type: none"> • Japanese Language version • Sun Java Plug-in, version 1.5 	Tested
Netscape Communicator	Versions 7.0, 7.1, and 7.2 for Microsoft Windows <ul style="list-style-type: none"> • English and Japanese Language versions • Sun Java Plug-in, version 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. Also, you must disable HTTP proxy in the browser.

Table 2 **Device Operating Systems**

Operating System	Minimum Version	Notes
PIX	Version 515E	PixOS 7.0(3)
IOS	Version 11.2	For full RADIUS support.
CatOS	Version 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 3 **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
Cisco 7100	RADIUS and TACACS+ interoperability
Cisco 7200	RADIUS and TACACS+ interoperability
Cisco 7300	RADIUS and TACACS+ interoperability
Cisco7400	RADIUS and TACACS+ interoperability
Cisco 7500	RADIUS and TACACS+ interoperability
Cisco 10000	RADIUS interoperability
Cisco 10720	RADIUS and TACACS+ interoperability

Table 4 **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 4.0.

Table 5 **Cable Devices**

Devices	Notes
uBR7100 ¹	RADIUS and TACACS+ interoperability

1. Tested on version 3.2, not retested on version 4.0.

Table 6 *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 4.0.

Table 7 *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 v6.3.5 RADIUS and TACACS+ interoperability
5000 Series Concentrator	EOL Status

Table 8 *Storage Networking Devices*

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

Table 9 *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 <div style="text-align: center;">  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. </div> RADIUS and TACACS+ interoperability

Table 10 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 11 CiscoWorks VMS

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

Table 12 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	Version 6.0	Not Tested
Verisign Onsite	Version 5.0	Not Tested

Table 13 Token Servers¹

Platform	Versions	Client Requirement	Notes
ActivCard Server	Version 3.1	—	Not Tested
CRYPTOCARD CRYPTOAdmin	Version 5.16	—	Not Tested
PassGo Defender	Version 4.1.3	—	Not Tested
RSA ACE/Server	Version 6.0	RSA ACE Agent version 6.0.1 for Windows 2000 Server, Service Pack 4	Tested
RSA ACE/Server	Versions 5.2	RSA ACE Agent version 5.6 for Windows 2000 Server, Service Pack 4	Tested
Safeword Premier Access	Version 3.1, 3.2	—	Tested
Vasco Vacman Server	Version 6.0.2	—	Not Tested

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

Table 14 LDAP Servers

Platform	Versions	Notes
SunONE Identity Server	Version 5.2	Tested with Windows 2003, Enterprise Edition Tested with Solaris 8
Microsoft Active Directory		Tested with Windows 2003, Enterprise Edition
Open-LDAP	Version 2.2.23	Tested with RedHat Enterprise Linux AS, Release 3 Tested with Open-SSL 0.9.7e
Novell NetWare Directory Services (NDS)	Version 6.5	Tested
Novell eDirectory	Version 8.7.1	Tested

Table 15 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 14 .
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 13, Token Servers](#).

Table 16 Proxy Support

Platform	Versions	Notes
Cisco Secure ACS	—	Tested with version 4.0.1
Funk Steel Belted Radius	Enterprise Edition	Not Tested

This document is to be used in conjunction with the documents listed in the *Documentation Guide for Cisco Secure ACS for Windows* document.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0705R)

© 2005 Cisco Systems, Inc. All rights reserved.