



# Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows Server Version 3.3

---

June 28, 2007

Full Build Number: 3.3.3.11

## Introduction

Because the number of devices that Cisco Secure ACS for Windows Server Version 3.3 interoperates with runs into the hundreds, this device list differs significantly from those of other Cisco products with which you may be familiar. This document lists supported devices and software, that is, those that we have tested against. However, 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 for Windows Server Version 3.3 interoperates with, Cisco only officially supports those that have been tested.

For details regarding other limitations and known problems see [Release Notes for Cisco Secure Access Control Server for Windows Server Version 3.3](#).



---

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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

This document contains the following sections:

- [Supported Operating System, page 2](#)
- [Supported Upgrade Versions, page 3](#)
- [Tested Windows Security Patches, page 3](#)
- [Third-party RADIUS and TACACS+ Clients, page 4](#)
- [Supported and Interoperable Devices and Software, page 5](#)

## Supported Operating System

Cisco Secure ACS for Windows Servers 3.3 supports the Windows operating systems listed below. Both 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 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



### Note

---

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.
- 

When running Cisco Secure ACS on Windows Server 2003, you may encounter event messages that falsely indicate that Cisco Secure ACS services have failed. This issue is documented in bug CSCe91690.

# Supported Upgrade Versions

We tested upgrading to Cisco Secure ACS for Windows Server, version 3.3, from the following previous versions:

- Cisco Secure ACS for Windows Server, version 3.2.3
- Cisco Secure ACS for Windows Server, version 3.2.2
- Cisco Secure ACS for Windows Server, version 3.2.1
- Cisco Secure ACS for Windows Server, version 3.1.2

# Tested Windows Security Patches

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

We tested Cisco Secure ACS for Windows Server 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 for Windows Server 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

With regard to third-party RADIUS and TACACS+ clients, Cisco Secure ACS fully interoperates with devices that adhere to the governing protocols. 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 your Cisco Secure ACS user guide.

Cisco Secure ACS 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 supports or with which it interoperates:

- [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 Cisco.com, <http://www.cisco.com>.

To ensure full capabilities, the clients you deploy to interoperate with Cisco Secure ACS should use the most recent operating systems available. Nonetheless, [Table 2, Device Operating Systems](#) provides details on the minimum acceptable client operating system versions.

**Table 1** *Web Browsers<sup>1</sup>*

Program	Versions	Notes
Microsoft Internet Explorer	Version 6.0 <ul style="list-style-type: none"> <li>• Service Pack 1 for Microsoft Windows</li> <li>• English Language version</li> <li>• Microsoft Java Virtual Machine</li> </ul>	Tested
Microsoft Internet Explorer	Version 6.0 <ul style="list-style-type: none"> <li>• Service Pack 1 for Microsoft Windows</li> <li>• English Language version</li> <li>• Sun Java Plug-in 1.4.2_04</li> </ul>	Tested
Netscape Communicator	Version 7.1 for Microsoft Windows <ul style="list-style-type: none"> <li>• English Language version</li> <li>• Sun Java Plug-in 1.4.2_04</li> </ul>	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 2** *Device Operating Systems*

<b>Operating System</b>	<b>Minimum Version</b>	<b>Notes</b>
IOS	Version 11.2	For full RADIUS support
CAT OS	Version 7.2	Cisco products—and other third-party products that are RFC compliant—will work with 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 3** *Routers*

<b>Series</b>	<b>Notes</b>
Cisco 800	RADIUS and TACACS+ interoperability
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
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

**Table 3 Routers (continued)**

Cisco 10000	RADIUS interoperability
Cisco 10720	RADIUS and TACACS+ interoperability

**Table 4 Access Devices/Universal Gateways**

<b>Series</b>	<b>Notes</b>
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
AS5400 Series <sup>1</sup>	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 5 Cable Devices**

<b>Devices</b>	<b>Notes</b>
uBR7100 <sup>1</sup>	Tested with IOS 12.2BC RADIUS and TACACS+ interoperability

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

**Table 6** *Content Networking Devices<sup>1</sup>*

<b>Series / Devices</b>	<b>Notes</b>
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 7** *Security and VPN Devices*

<b>Series / Devices</b>	<b>Notes</b>
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 8** *Storage Networking Devices*

<b>Series</b>	<b>Devices Supported</b>	<b>Notes</b>
MDS 9000	MDS 9216, MDS9509	RADIUS and TACACS+ interoperability

**Table 9** *Switches*

<b>Series / Devices</b>	<b>Notes</b>
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 10** *Cisco Aironet Software (Access Points for Wireless LAN)*

<b>Series</b>	<b>Notes</b>
AP1100	RADIUS interoperability with IOS v12.2(15)JA
AP1200	RADIUS interoperability with IOS v12.2(15)JA

**Table 11** *CiscoWorks VMS*

<b>Series</b>	<b>Devices Supported</b>	<b>Notes</b>
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 12 PKI/Certificate Servers**

Platform	Versions	Notes
Microsoft CA Certificate Server	Windows 2000 Windows 2000 with SP4 Windows 2003 Enterprise and Standard editions	Tested
Entrust PKI	Version 6.0	—
Verisign Onsite	Version 5.0	—

**Table 13 Token Servers<sup>1</sup>**

Platform	Versions	Client Requirement	Notes
ActivCard Server	Version 3.1	—	—
CRYPTOCARD CRYPTOAdmin	Version 5.16	—	—
PassGo Defender	Version 4.1.3	—	—
RSA ACE/Server	Version 5.1 and 5.2	RSA ACE Agent version 5.5 for Windows 2000	Tested
Safeword Premier Access	Version 3.1	—	—
Vasco Vacman Server	Version 6.0.2	—	—

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 2000 Active Directory with Windows Service Pack 3

**Table 14 LDAP Servers (continued)**

Novell NetWare Directory Services (NDS)	Version 6.0	Tested
Novell eDirectory	Version 8.6	Tested

**Table 15 User Databases<sup>1</sup>**

Platform	Version	Requirement
AD on Windows 2003	—	Tested
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	—
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.  Novell Client must be installed on the same Windows server as Cisco Secure ACS.
Open Database Connectivity (ODBC)-compliant relational databases	—	In addition to the Windows ODBC interface, the third-party ODBC driver must be installed on the Cisco Secure ACS Windows 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 3.3
Funk Steel Belted Radius	Enterprise Edition	—