Supported and Interoperable Devices and Software Tables for Cisco Secure ACS 4.2

OL-14389-01
Revised: February 2008

Introduction

The Cisco Secure Access Control Server Release 4.2, 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 Solution Engine (SE) hardware platforms and supported ACS software versions, see Supported ACS Software Versions on the ACS SE. For details regarding limitations and known problems, see the *Release Notes for Cisco Secure ACS Release 4.2*.

This document contains:

- Tested Network Elements and Software
- Supported ACS Software Versions on the ACS SE
- Supported Operating Systems
- Remote Agent Support
- SNMP Support
- Tested Windows Security Patches
- Tested Windows Security Patches
- Third-Party RADIUS and TACACS+ Clients

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

- Supported and Interoperable Devices and Software
- Open Source License Acknowledgements
- Obtaining Documentation and Submitting a Service Request

Tested Network Elements and Software

This section lists the network elements and software that were tested with ACS 4.2.

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.7 (SP2)
- Microsoft Internet Explorer, v.6.0 (SP1)
- Microsoft OS (Windows 2000 Server SP4, Windows 2003 Standard Edition, Windows 2003 Enterprise Edition, Windows Server 2003 SP2, Windows Server 2003 R2 Standard Edition, Windows Server 2003 R2 SP2)
- Microsoft SQL server v.7.5
- Microsoft SQL server v8.0
- Mozilla Firefox 2.0.0.6
- 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, 3.2
- Secure RSA agent for Windows, v.5.6
- Secure RSA Server (OTP), v.5.2
- Solaris 8 for SPARC
- Solaris 9
- 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 ACS software versions that each Cisco Secure ACS SE platform supports.

Table 1 Supported Versions

Cisco Secure ACS SE Platform	Cisco Secure ACS versions 3.3.4	Cisco Secure ACS version 4.2	Cisco Secure ACS version 4.0 and 4.1
Cisco 1111	Yes	No	Yes
Cisco 1112	Yes	Yes	Yes
Cisco 1113	Yes	Yes	Yes

Supported Operating Systems

ACS supports the following Windows operating systems for ACS for Windows:

- Windows Server 2000 (English version only)
- Windows 2000 Advanced Server, Service Pack 4, without features specific to Windows 2000 Advanced Server enabled or without Microsoft clustering service installed (English version only)
- Windows Server 2003, Service Pack 1, Enterprise Edition or Standard Edition (English version only)
- Japanese Windows Server 2003, Service Pack 1
- Japanese Windows Server 2003, Service Pack 2, Enterprise Edition (or higher, if available 90 days prior to FCS)
- Japanese Windows Server 2003, Service Pack 2, R2, Enterprise Edition (or higher, if available 90 days prior to FCS)
- Japanese Windows Server 2003, Service Pack 2, Standard Edition (or higher, if available 90 days prior to FCS)
- Japanese Windows Server 2003, Service Pack 2, R2, Standard Edition (or higher if available 90 days prior to FCS)
- Windows Server 2003, R2, Standard Edition
- Windows Server 2003, Service Pack 2
- Windows Server 2003, R2, Service Pack 2

Note ACS supports the multi-processor feature on dual processor computers.

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 4.2.

Remote Agent Support

Cisco Secure ACS 4.2 supports Cisco Secure ACS Remote Agent on the Microsoft Windows and Solaris operating systems.

Windows Support for the Remote Agent

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

SNMP Support

ACS provides Simple Network Management Protocol (SNMP) support for the appliance only. The SNMP agent provides read-only SNMP v1 and SNMP v2c support. The supported Management Information Bases (MIBs) include:

- Structure and Identification of Management Information for TCP/IP-based Internets (1155)
- SNMP (1157)
- MIB for Network Management of TCP/IP-based internets: MIB-II (1213)
- MIB-II and LAN Manager MIB-II for Windows
- Host Resources MIB (RFC 1514/2790)

Note Support for the Host Resources MIB (RFC 1514/2790) does not include support for releases:

- 1.3.6.1.2.1.25, which is related to Microsoft hostmib.*dll*.
- 1.3.6.1.4.1, which is related to WinTrust.dll.

The SNMP agent is configurable on the appliance configuration page.

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 SE 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

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 Cisco Systems defined in draft 1.78, which is available a http://www.cisco.com

For RADIUS, ACS conforms to the following Request For Comments (RFC):

- **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 4.2*.

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

Supported and Interoperable Devices and Software

This section contains:

- 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, Public Key Infrastructure (PKI)/Certificate Servers
- Table 14, Token Servers
- Table 15, LDAP Servers
- Table 16, User Databases
- Table 17, User Databases
- Table 18, Proxy Support
- VMWare ESX Server Support, page 13

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 Browsers[1]

Program	Versions	Notes
Microsoft Internet Explorer	Version 7 • Service Pack 1 for Microsoft Windows 2003 Server (English Language Version) • Service Pack 2 for Microsoft Windows XP (English Language Version)	Tested
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 • Service Pack 1 for Microsoft Windows 2003 Server (English and Japanese Language versions) – Sun Java Plug-in, v.1.4.2_16 – Sun Java Plug-in, v.5.0 Update 13 – Sun Java Plug-in, v.6.0 Update 3	Tested
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
Mozilla Firefox	Version 2.0.0.6 • Sun Java Plug-in, v.1.4.2_16 • Sun Java Plug-in, v.5.0 Update 13 • Sun Java Plug-in, v.6.0 Update 3	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
PIXOS	7.0(3)	For full RADIUS support.
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, when the listed CatOS version is used, it supports full functionality, including the 802.1x VLAN assignment.

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
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 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	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

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 Devices[1]

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 v6.3.5 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

Table 10 Switches (continued)

Series/Devices	Notes
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 Public Key Infrastructure (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 Servers[1]

Platform	Version	Client Requirement	Notes
ActivCard Server	3.1	—	Not Tested

Table 14 Token Servers[1] (continued)

CRYPTOCard CRYPTOAdmin	5.16	—	Not Tested
PassGo Defender	4.1.3	—	Not Tested
RSA ACE/Server	6.0	—	Tested
RSA ACE/Server	5.2	—	Not Tested
Safeword Premier Access	3.1, 3.2	—	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
Novell NetWare Directory Services (NDS)	6.5	Not tested with ACS 4.2
Novell eDirectory	8.7.1	Not tested with ACS 4.2

Table 16 User Databases[1]

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.
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 Databases[1]

Platform	Version	Requirement
AD on Windows 2003	—	Tested with Service Pack 1
AD on Windows 2000	—	Tested with Service Pack 4

Table 17 User Databases[1] (continued)

SAM on Windows 2000	—	Tested with Service Pack 4
SAM on Windows NT 4.0	—	Not Tested
LDAP	Generic	See Table 15
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 4.2
Funk Steel Belted Radius	Enterprise Edition	Not Tested

VMWare ESX Server Support

ACS 4.2 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 2003 Standard Edition
- 3 GB of RAM for the guest operating system

The following versions of VMWare ESX are supported:

- ESX 3.0.x (tested)
- ESX 3.5.x (not tested)
- ESX 3.5i (not tested)

Open Source License Acknowledgements

The following acknowledgements pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

© 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Supported and Interoperable Devices and Software Tables for Cisco Secure ACS 4.2