Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.5

Revised: September 26, 2014

The Cisco Secure Access Control System Release 5.5, hereafter referred to as ACS, works with hundreds of devices. You can use this document to find devices and software that ACS 5.5 supports.

For details regarding limitations and known problems, see the Release Notes for Cisco Secure Access Control System 5.5.

This document contains:

- Supported Devices, page 2
- Supported User Repositories, page 3
- Supported 802.1X Clients, page 4
- Supported Browsers, page 5
- Supported Authentication Protocols, page 6
- FIPS support, page 6
- SNMP Support, page 7
- Syslog Support, page 7
- ACS View 5.5 Database Support, page 7
- Supported VMware Versions, page 7
- Documentation Updates, page 8
- Related Documentation, page 8
- Notices, page 9
- Obtaining Documentation and Submitting a Service Request, page 11
Supported Devices

ACS 5.5 supports all devices that implement the authentication, authorization, and accounting (AAA) mechanism similar to Cisco IOS 12.x.

RADIUS and TACACS+

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 at 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 Access Control System 5.5.

Note
If ACS is set to operate in FIPS mode, some protocols are not supported. For more information, see see the User Guide for Cisco Secure Access Control System 5.5.

Table 1 lists some of the tested network elements that ACS 5.5 supports.

Table 1  Tested Network Elements

<table>
<thead>
<tr>
<th>Network Elements</th>
<th>Operating System with Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 2610</td>
<td>IOS 12.3.17b</td>
</tr>
<tr>
<td>Cisco 3640</td>
<td>IOS 12.3.17b</td>
</tr>
<tr>
<td>Cisco 7200</td>
<td>IOS 12.3.17b</td>
</tr>
<tr>
<td>Cisco 3750</td>
<td>IOS 12.2(25r)</td>
</tr>
<tr>
<td>Catalyst WS-3560-24TS Switch</td>
<td>IOS 12.2(25)-SEC2</td>
</tr>
<tr>
<td>Cisco 515E PIX</td>
<td>PIX OS 6.3.5</td>
</tr>
<tr>
<td>Cisco AP 1200</td>
<td>IOS 12.3(7)JA1</td>
</tr>
</tbody>
</table>
Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.5

**Supported User Repositories**

ACS 5.5 supports the following external user repositories:

- Windows Active Directory, page 4
- RSA Secure ID Server, page 4
- Radius Token OTP Server, page 4

---

**Table 1**  
**Tested Network Elements (continued)**

<table>
<thead>
<tr>
<th>Network Elements</th>
<th>Operating System with Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nexus 7000</td>
<td>4.2(1)</td>
</tr>
<tr>
<td>Catalyst 6000</td>
<td>12.2 (SIERRA_INTEG_080914)</td>
</tr>
<tr>
<td>IP Phone</td>
<td>Cisco IP Phone 7970</td>
</tr>
<tr>
<td>VPN Concentrator 3000</td>
<td>VPN 3000 4.7.2.1</td>
</tr>
<tr>
<td>ASA-5510</td>
<td>8.0(4)</td>
</tr>
<tr>
<td>Cisco Wireless Controller- WLC 4400</td>
<td>—</td>
</tr>
<tr>
<td>Load Balancer CSS11503-AC L0</td>
<td>08.10.1.06</td>
</tr>
<tr>
<td>Cisco VPN Client</td>
<td>5.0.04.3</td>
</tr>
<tr>
<td>Cisco AnyConnect VPN Client</td>
<td>2.3</td>
</tr>
<tr>
<td>Inherit Microsoft VPN Client</td>
<td>Microsoft XP</td>
</tr>
</tbody>
</table>

---

**CoA Support**

ACS supports Change of Authorization (CoA) on the Cisco IOS version 12.2(52)SE. Table 2 lists the devices and images that support CoA:

**Table 2**  
**Devices and Images that Support CoA**

<table>
<thead>
<tr>
<th>Devices</th>
<th>Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 2960</td>
<td>LANbase</td>
</tr>
<tr>
<td>Cisco 2975</td>
<td>LANbase</td>
</tr>
<tr>
<td>Cisco 3560/3560 version 2</td>
<td>IPbase</td>
</tr>
<tr>
<td>Cisco 3750/3750 version 2</td>
<td>IPbase</td>
</tr>
<tr>
<td>Cisco 3560E</td>
<td>IPbase</td>
</tr>
<tr>
<td>Cisco 3750E</td>
<td>IPbase</td>
</tr>
<tr>
<td>IE 3000</td>
<td>IPbase</td>
</tr>
<tr>
<td>CBS31xx</td>
<td>IPbase</td>
</tr>
<tr>
<td>CBS30xx</td>
<td>IPbase</td>
</tr>
</tbody>
</table>
Windows Active Directory

ACS 5.5 supports all editions of:
- Windows AD 2003
- Windows AD 2003 R2
- Windows AD 2008
- Windows AD 2008 R2
- Windows AD 2012
- Windows AD 2012 R2 is supported after ACS 5.5 patch 1.

Lightweight Directory Access Protocol Server

ACS 5.5 supports Lightweight Directory Access Protocol (LDAP) servers. The supported LDAP servers include, but are not limited to:
- SunONE LDAP Directory Server - Version 5.5
- Linux LDAP Directory Server - Version 4.1
- Open LDAP Directory Server

RSA Secure ID Server

ACS 5.5 supports:
- RSA ACE/Server 6.x Series
- RSA Authentication Manager 7.x Series
- RSA 8.x

Radius Token OTP Server

ACS 5.5 supports:
- Any RADIUS RFC 2865-compliant token server
- SafeWord Server

Supported 802.1X Clients

ACS 5.5 supports all 802.1X clients. These include, but are not limited to:
- Cisco AnyConnect 3.0
- Cisco AnyConnect 3.1
- Microsoft Built-In Windows XP 802.1X Client
- Microsoft Built-In Windows Vista 802.1X Client
- Microsoft Built-In Windows 7 802.1X Client
• Microsoft Built-In Windows 8 802.1X Client
• CSSC version 4.x
• CSSC version 5.x
• Juniper Odyssey 4.x
• Intel Wireless WiFi Link with AMT support
• CSSC SDK for Vista

Supported Browsers

ACS 5.5 supports the following browser platforms:

• MAC OS
  – Mozilla Firefox version 24.4 ESR
  – Mozilla Firefox version 28.x
  – Mozilla Firefox version 29.x

• Windows 7 32-bit
  – Internet Explorer version 11.x
  – Mozilla Firefox version 24.4 ESR
  – Mozilla Firefox version 28.x
  – Mozilla Firefox version 29.x

• Windows 7 64-bit
  – Internet Explorer version 10.x
  – Internet Explorer version 11.x
  – Mozilla Firefox version 17.x
  – Mozilla Firefox version 17.0.6 ESR
  – Mozilla Firefox version 21.x
  – Mozilla Firefox version 22.x
  – Mozilla Firefox version 24.1.1 ESR
  – Mozilla Firefox version 24.4 ESR
  – Mozilla Firefox version 24.5 ESR
  – Mozilla Firefox version 24.7.0 ESR
  – Mozilla Firefox version 25.x
  – Mozilla Firefox version 26.x
  – Mozilla Firefox version 28.x
  – Mozilla Firefox version 29.x
  – Mozilla Firefox version 31.x
  – Mozilla Firefox version 31.0 ESR
Supported Authentication Protocols

ACS 5.5 supports the following protocols:

- PAP/ASCII
- EAP-MD5
- EAP-TLS
- PEAP (with inner EAP-MSCHAPv2/EAP-GTC/EAP-TLS)
- EAP-FAST (with inner EAP-MSCHAPv2/EAP-GTC)
- TACACS+ (PAP/CHAP/MSCHAP)
- LEAP
- CHAP
- MSCHAP (v1)
- MSCHAP (v2)

FIPS support

ACS supports Federal Information Processing Standard (FIPS) 140-2 Level 1 certification. FIPS 140-2 is a United States government computer security standard that is used to accredit cryptographic modules.

ACS 5.5 in FIPS mode supports the following protocols:

- EAP-TLS
- PEAP and its inner methods
- EAP-FAST except the anonymous PAC provisioning

ACS 5.5 in FIPS mode supports the following supplicants:

- Wireless supplication with Any connect.

Notes:

1. You can launch the ACS web interface using IPv6 addresses only in Internet Explorer 7.x or later and Mozilla Firefox 3.x versions.

2. Disable the pop up blocker when you use Internet Explorer version 8.x on Windows XP.

3. You should install Windows XP SP3 to use SHA2 256-bit certificates as management certificates.

- MAC OS 10.5
  Mozilla Firefox version 3.x
- Linux RedHat (latest version)
  Mozilla Firefox version 3.x
- Oddysey (Oddysey does not support the Anonymous PAC Provisioning in EAP-FAST. Therefore, Oddysey with EAP-FAST is not supported in FIPS mode.)
- All Windows native supplicant.

For more information on FIPS, see the *User Guide for Cisco Secure Access Control System 5.5.*

### SNMP Support

ACS 5.5 supports Simple Network Management Protocol (SNMP) to provide logging services. The SNMP agent provides read-only SNMPv1 and SNMPv2c support. The supported MIBs include:

- SNMPv2-MIB
- RFC1213-MIB (MIB II)
- IF-MIB
- IP-MIB
- TCP-MIB
- UDP-MIB
- CISCO-CDP-MIB
- ENTITY-MIB


### Syslog Support

ACS 5.5 conforms to syslog standards (RFC 3164 and RFC 5424) and supports any generic syslog server. In addition, ACS supports the following:

- Syslog over TCP follows the standards of RFC 6587.
- Syslog over TLS (Secure TCP) follows the standards of RFC 5425.

### ACS View 5.5 Database Support

In ACS View 5.5, the following can be used as the remote database:

- Microsoft SQL Server 2008 R2
- Oracle Database 12c

### Supported VMware Versions

ACS 5.5 can be installed on the following VMware versions:

- VMware ESXi 5.0
- VMware ESXi 5.0 Update 2
• VMware ESXi 5.1
• VMware ESXi 5.5 Update 1 after you install patch 3 or a subsequent patch.

For information on the VMware machine requirements and installation procedures, refer to Installing ACS in a VMware Virtual Machine chapter in the Installation and Upgrade Guide for Cisco Secure Access Control System 5.5.

Documentation Updates

Table 3 Updates to the Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.5

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>

Related Documentation

Note

The printed and electronic documentation is sometimes updated after original publication. Therefore, you should also review the documentation on http://www.cisco.com for any updates.

Table 4 lists the product documentation that is available for ACS 5.5. To find end-user documentation for all the products on Cisco.com, go to: http://www.cisco.com/go/techdocs


Table 4 Product Documentation

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
</table>
The following notices pertain to this software license.

### OpenSSL/OpenSSL 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:**

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

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:

---

**Table 4: Product Documentation (continued)**

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
</table>
“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:
Copyright © 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, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What’s New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.5
Copyright © 2013 Cisco Systems, Inc. All rights reserved.