



Release Notes for Cisco Application eXtension Platform (AXP) 1.1.7

October 7, 2009

Revised: April 6, 2010, OL-14273-01

These release notes support the software for the Cisco Application eXtension Platform (AXP). To see if your software or hardware platforms are affected, view the field notices for Cisco IOS software version 12.4 (T) at http://www.cisco.com/warp/customer/tech_tips/index/cfn.html. (You need to have an account on cisco.com to view the field notices.)

Contents

- [System Requirements, page 1](#)
- [Limitations and Restrictions, page 8](#)
- [Basic Safeguards for Securing AXP Router/Blade, page 8](#)
- [Caveats for Cisco AXP, page 8](#)
- [Modified Commands in Cisco AXP 1.1.7, page 9](#)
- [Related Documentation, page 10](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 11](#)
- [Notices, page 11](#)

System Requirements

This section describes the system requirements for Cisco Application eXtension Platform Version 1.1.7 and includes the following sections:

- [Cisco IOS Software Release, page 2](#)
- [Supported Hardware, page 2](#)
- [Files in Cisco AXP 1.1.7, page 3](#)
- [Upgrading from Cisco AXP 1.1.5 to Cisco AXP 1.1.7, page 7](#)



Americas Headquarters:

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

- [Determining the Software Version, page 7](#)

Cisco IOS Software Release

Cisco AXP 1.1.7 supports routers with the following Cisco IOS releases.

- 12.4(15)T3 or higher: IP-based crypto images including the following image packs:
 - IP-Base
 - IP-Voice
 - Adv-Security
 - Adv-Enterprise

Download the image from:

<http://tools.cisco.com/support/downloads/go/Model.x?mdfid=282831883&mdfLevel=Model&treeName=Routers&modelName=Cisco%20Application%20Extension%20Platform%20Version%201.1&treeMdfId=268437899>

Supported Hardware

Cisco Platforms	Cisco AXP Service Module SKU	Processor/Memory	Hard Disk	Compact Flash
Cisco 1841 Cisco 2801 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3825 Cisco 3845	AIM-APPRE-102-K9	300 MHz/256 MB	—	1 GB
Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3825 Cisco 3845	NME-APPRE-302-K9	1.0 GHz/512 MB	80 GB	—
Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3825 Cisco 3845	NME-APPRE-502-K9	1.0 GHz/1.0 GB	120 GB	—
Cisco 3825 Cisco 3845	NME-APPRE-522-K9	1.4 GHz/2.0 GB	160 GB	—

Files in Cisco AXP 1.1.7

Download Cisco AXP files from the following location:

<http://www.cisco.com/kobayashi/sw-center/access/axp/117.shtml>

Files in Cisco AXP 1.1.7 are explained in the following sections:

- [Cisco AXP Product Files, page 3](#)
- [Cisco AXP Software Development Files, page 4](#)

Cisco AXP Product Files

Cisco AXP product files for AIM and NME service modules:

- [Cisco AXP Product Files for AIM Service Modules, page 3](#)
- [Cisco AXP Product Files for NME Service Modules, page 3](#)

Cisco AXP Product Files for AIM Service Modules

Compressed archive `axp-k9.aim.1.1.7.tar.gz` contains all package files associated with Cisco AXP on AIM service modules. The package files are shown in .

Table 1 *Cisco AXP 1.1.7 Product Files for AIM*

Filename	Purpose
<code>axp-helper-k9.aim.1.1.7</code>	Cisco AXP Rescue Helper image. Aids application installation on AIM service modules when necessary.
<code>axp-k9-aim.1.1.7.pkg</code>	Main package for installing Cisco AXP on AIM service modules.
<code>axp-k9-aim.1.1.7.prt1</code>	Package payload containing all data and executable files for the installer subsystem associated with Cisco AXP on AIM service modules.
<code>axp-installer-k9.aim.1.1.7.prt1</code>	Package payload containing all data and executable files for the installer subsystem associated with Cisco AXP on AIM service modules.

Cisco AXP Product Files for NME Service Modules

Compressed archive `axp-k9.nme.1.1.7.tar.gz` contains all package files associated with Cisco AXP on NME service module. The package files are shown in [Table 1](#).

Table 2 *Cisco AXP 1.1.7 Product Files for NME*

Filename	Purpose
<code>axp-helper-k9.nme.1.1.7</code>	Cisco AXP rescue helper image. Helps to install the application on Cisco NME service modules when necessary.
<code>axp-k9.nme.1.1.7.pkg</code>	Main package for installing the Cisco AXP on Cisco NME service modules.

Table 2 Cisco AXP 1.1.7 Product Files for NME

Filename	Purpose
axp-k9.nme.1.1.7.prt1	Package payload containing all data and executable files for a full installation of the Cisco AXP on Cisco NME service modules.
axp-installer-k9.nme.1.1.7.prt1	Package payload containing all data and executable files for the installer subsystem associated with the Cisco AXP on Cisco NME service modules.

Cisco AXP Software Development Files

Cisco AXP software development files:

- [Cisco AXP Software Development Kit \(SDK\), page 4](#)
- [Cisco AXP Software Development Files for VMware, page 4](#)
- [Cisco AXP Software Development Files for Add-ons on AIM Service Modules, page 4](#)
- [Cisco AXP Software Development Files for Add-ons on NME Service Modules, page 5](#)

Cisco AXP Software Development Kit (SDK)

Compressed archive axp-sdk.1.1.7.tar.gz contains the Cisco AXP Software Development Kit (SDK) for all service modules.

Cisco AXP Software Development Files for VMware

Compressed archive axp-k9.vmw.1.1.7.tar.gz contains the Cisco AXP Software Development Files for VMware.

The package files are shown in [Table 2](#).

Table 3 Cisco AXP 1.1.7 Software Development Files for VMware

Filename	Purpose
axp-k9.vmw.1.1.7.vmdk	Cisco AXP VMware disk image file.
axp-vm.1.1.7.vmx	Cisco AXP VMware virtual hardware configuration file.

Cisco AXP Software Development Files for Add-ons on AIM Service Modules

Compressed archive axp-k9.aim.addon.1.1.7.tar.gz contains Cisco AXP software development files for add-ons on AIM service modules. The package files are shown in [Table 3](#).

Table 4 Cisco AXP 1.1.7 Software Development Files for AIM Add-On Software

Filename	Purpose
axp-app-dev.aim.1.1.7.pkg	Package for installing the Application Development add-on associated with Cisco AXP on AIM service modules.
axp-app-dev.aim.1.1.7.prt1	Package payload containing all data and executable files for the Application Development add-on associated with Cisco AXP on AIM service modules.

Table 4 Cisco AXP 1.1.7 Software Development Files for AIM Add-On Software (continued)

Filename	Purpose
axp-cli-plugin.aim.1.1.7.pkg	Package for installing the Command Language Interpreter add-on associated with Cisco AXP on AIM service modules.
axp-cli-plugin.aim.1.1.7.prt1	Package payload containing all data and executable files for the Command Language Interpreter add-on associated with Cisco AXP on AIM service modules.
axp-eemapi.aim.1.1.7.pkg	Package for installing Cisco IOS Event Notification add-on associated with Cisco AXP on AIM service modules.
axp-eemapi.aim.1.1.7.prt1	Package payload containing all data and executable files for Cisco IOS Event Notification add-on associated with Cisco AXP on AIM service modules.
axp-iosapi.aim.1.1.7.pkg	Package for installing Cisco IOS Configuration add-on associated with Cisco AXP on AIM service modules.
axp-iosapi.aim.1.1.7.prt1	Package payload containing all data and executable files for Cisco IOS Configuration add-on associated with Cisco AXP on AIM service modules.
axp-vserial.aim.1.1.7.pkg	Package for installing the IOS Serial Device add-on associated with Cisco AXP on AIM service modules.
axp-vserial.aim.1.1.7.prt1	Package payload containing all data and executable files for the IOS Serial Device add-on associated with the Cisco AXP on AIM service modules.
axp-perl-5.8.8.aim.1.1.7.pkg	Package for installing a Perl Language Interpreter add-on associated with the Cisco AXP on AIM service modules.
axp-perl-5.8.8.aim.1.1.7.prt1	Package payload containing all data and executable files for a Perl Language Interpreter add-on associated with the Cisco AXP on AIM service modules.
axp-ssh-4.6p1-k9.aim.1.1.7.pkg	Package for installing a Secure Shell add-on associated with Cisco AXP on AIM service modules.
axp-ssh-4.6p1-k9.aim.1.1.7.prt1	Package payload containing all data and executable files for a Secure Shell add-on associated with the Cisco AXP on AIM service modules.
axp-tomcat5.aim.1.1.7.pkg	Package for installing a Tomcat java-based web server add-on associated with Cisco AXP on AIM service modules.
axp-tomcat5.aim.1.1.7.prt1	Package payload containing all data and executable files for a Tomcat java-based web server add-on associated with the Cisco AXP on AIM service modules.

Cisco AXP Software Development Files for Add-ons on NME Service Modules

Compressed archive axp-k9.nme.addon.1.1.7.tar.gz contains Cisco AXP software development files for add-ons on NME service modules. The package files are shown in [Table 4](#).

Table 5 Files included in Cisco AXP 1.1.7 Cisco NME Add-On Packages

Filename	Purpose
axp-app-dev.nme.1.1.7.pkg	Package for installing the Application Development add-on associated with the Cisco AXP on Cisco NME service modules.
axp-app-dev.nme.1.1.7.prt1	Package payload containing all data and executable files for the Application Development add-on associated with the Cisco AXP on Cisco NME service modules.
axp-cli-plugin.nme.1.1.7.pkg	Package for installing the Command Language Interpreter add-on associated with Cisco AXP on Cisco NME service modules.
axp-cli-plugin.nme.1.1.7.prt1	Package payload containing all data and executable files for the Command Language Interpreter add-on associated with Cisco AXP on Cisco NME service modules.
axp-eemapi.nme.1.1.7.pkg	Package for installing Cisco IOS Event Notification add-on associated with Cisco AXP on Cisco NME service modules.
axp-eemapi.nme.1.1.7.prt1	Package payload containing all data and executable files for the IOS Event Notification add-on associated with Cisco AXP on Cisco NME service modules.
axp-iosapi.nme.1.1.7.pkg	Package for installing Cisco IOS Configuration add-on associated with Cisco AXP on Cisco NME service modules.
axp-iosapi.nme.1.1.7.prt1	Package payload containing all data and executable files for the IOS Configuration add-on associated with Cisco AXP on Cisco NME service modules.
axp-vserial.nme.1.1.7.pkg	Package for installing Cisco IOS Serial Device add-on associated with the Cisco AXP on Cisco NME service modules.
axp-vserial.nme.1.1.7.prt1	Package payload containing all data and executable files for Cisco IOS Serial Device add-on associated with the Cisco AXP on Cisco NME service modules.
axp-perl-5.8.8.nme.1.1.7.pkg	Package for installing a Perl Language Interpreter add-on associated with Cisco AXP on Cisco NME service modules.
axp-perl-5.8.8.nme.1.1.7.prt1	Package payload containing all data and executable files for a Perl Language Interpreter add-on associated with Cisco AXP on Cisco NME service modules.
axp-ssh-4.6p1-k9.nme.1.1.7.pkg	Package for installing a Secure Shell add-on associated with Cisco AXP on Cisco NME service modules.
axp-ssh-4.6p1-k9.nme.1.1.7.prt1	Package payload containing all data and executable files for a Secure Shell add-on associated with Cisco AXP on Cisco NME service modules.
axp-tomcat5.nme.1.1.7.pkg	Package for installing a Tomcat Java-based Web Server add-on associated with Cisco AXP on Cisco NME service modules.
axp-tomcat5.nme.1.1.7.prt1	Package payload containing all data and executable files for a Tomcat Java-based Web Server add-on associated with Cisco AXP on Cisco NME service modules.

Upgrading and Downgrading to a New Software Release

Upgrading from Cisco AXP 1.1.5 to Cisco AXP 1.1.7

To upgrade from Cisco AXP 1.1.5 and higher versions to Cisco AXP 1.1.7 with applications packaged with the 1.1.5/1.1.7 SDK:

- a. Copy the installer payload file (**axp-installer.k9.nme.1.1.7.prt1** or **axp-installer.k9.aim.1.1.7.prt1**) to the same FTP directory as the Cisco AXP package. The FTP directory contains a package file such as (**axp-k9.nme.1.1.7.pkg** or **axp-installer.k9.aim.1.1.7.prt1**) and a corresponding payload file (**axp-k9.nme.1.1.7.prt1** or **axp-k9.aim.1.1.7.prt1**) with other add-on packages.
- b. Install the Cisco AXP package using the **software install upgrade** command.



Note

If you are using a URL to obtain a copy of the Cisco AXP package use an ftp or ftps server location. Do not use an sftp server location. Using an sftp server results in the error described in the caveat CSCsy53185 TypeError occurs during installation or upgrade of Cisco AXP.

For upgrading and downgrading various software versions on Cisco AXP, refer to the [Cisco Application eXtension Platform 1.1 Command Reference](#) and the [Cisco Application eXtension Platform 1.1 User Guide](#).

After upgrading to Cisco AXP 1.1.7, verify that the system is running on Cisco AXP 1.1.7.

Downgrading from Cisco AXP 1.1.7

To downgrade to Cisco AXP 1.1.5 with applications packaged with the 1.1.5 SDK:

- Use the **software install upgrade** command. The **software install downgrade** command is not currently supported. For more information, see the [Cisco Application eXtension Platform 1.1 Command Reference](#) and the [Cisco Application eXtension Platform 1.1 User Guide](#).



Note

If you downgrade the service module to Cisco AXP 1.1.5 and use applications packaged with the Cisco AXP 1.1.7 SDK, the applications may not work. To avoid this, first repackage the applications with the Cisco AXP 1.1.5 SDK, downgrade the service module to Cisco AXP 1.1.5, and run the applications packaged with the Cisco AXP 1.1.5 SDK.

Determining the Software Version

To determine the version of Cisco AXP software currently running on your Cisco AXP service module, log into the service module, and enter the **show software version EXEC** command.

The following sample output from the **show software version** command indicates the version number on the first output line.

```
Application eXtension Platform (AXP) version (1.1.7)
Technical Support: http://www.cisco.com/techsupport/ Copyright (c) 1986-2009 by Cisco
Systems, Inc.
```

Limitations and Restrictions

For Cisco AXP 1.1.7 and lower versions, issuing the **do** command through the Cisco AXP IOS Service API, always returns “OK”. If the **do** command works or fails, the return value is always the same—“OK”.

However, issuing the **do** command through a Cisco IOS CLI console session returns the correct error messages when the **do** command fails.

Basic Safeguards for Securing AXP Router/Blade

In order to improve the security of your system, we suggest the following actions:

- Telneting to router IP addresses must always be protected via username and password. Common pairs such as cisco, cisco should be avoided.
- Users that are allowed access to routers should be classified further by assigning privilege levels (0-15) that allow for limiting actions that can be performed. Privilege level 0 is most restrictive, and level 15 is least restrictive.

Following this safeguard ensures that users attempting a privileged CLI operation need to go through #enable mode and password authorization.

- Remote access to Service Modules via SSH is disabled by default. When enabling SSH access via the **ip ssh server** command ensure that the **username sysadmin password** command is also configured. There are provisions to encrypt this password as well.

Caveats for Cisco AXP

Caveats describe unexpected behavior or defects in Cisco software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.



Note

To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) and go to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

- [Resolved Caveats- Cisco AXP Version 1.1.7, page 8](#)

Resolved Caveats- Cisco AXP Version 1.1.7

- CSCsq89795 cyclades log file should have timestamps & needs improvement.
- CSCsx94365 bind serial <name> command allows duplicate entry
- CSCsy75257 vserial startup python script throws error and stops creating new process
- CSCsy80648 content of cyclades log file gets overwritten instead of appending
- CSCsy75576 Upgrading platform changes file permissions in guest environment

- CSCtb65413 Awk and More are Present in Restricted Shell after Upgrade from 1.1.1

This notice addresses vulnerability in the AXP **techsupport support shell** EXEC mode CLI. Specifically, “awk” and “more” utilities have been removed from the shell to plug mechanisms within those utilities that permit escaping from the “restricted” shell environment to “unrestricted” mode that may potentially allow full access to AXP guest/host file systems.

Future AXP releases may reinstate the removed “awk” and “more” utilities by disabling the mechanisms that permit escapes out of the restricted shell environment.

- CSCtc25607 disk resource is wrong after doing upgrade an app pkg in axp 1.1.7 image

Modified Commands in Cisco AXP 1.1.7

The following command has been modified in Cisco AXP 1.1.7.

techsupport support shell

To enter a restricted shell environment containing a limited set of diagnostic utilities used to troubleshoot the AXP system, use the **techsupport support shell** command in Cisco AXP EXEC mode.

techsupport support shell

Command Default

None

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release

1.1

1.1.7

Modification

This command was Introduced.

The **awk** and **more** keywords were removed.

Usage Guidelines

In Cisco AXP EXEC mode, use this command to enter a shell that provides a set of diagnostic utilities as well as read-only access to the /var/log directory. When in the shell, type “help” to list the utilities provided by this shell. Type “exit” to exit the shell. The **techsupport support shell** command does not allow the following diagnostic commands to be used: awk, more.

Examples

The following example shows the use of help to display the list of utilities and viewable directories.

```
se-192-1-1-137> techsupport support shell
```

```
Saving session script in: techshell_session.log
```

```
This is a restricted shell environment with a limited set of commands
```

useful to technical support personnel for diagnosing the system.
 Type "help" or ? to find out the list of TechSupport commands.
 Type "exit" or Cntrl-D to exit.

```
techsupport> help
```

TechSupport commands available:

```
df free head ls mpstat pidstat sort top vmstat
cat du grep iostat netstat ps tail traceroute wc
```

TechSupport directories viewable:

```
/var/log
```

```
techsupport>
```

The next example shows the use of grep to filter startup messages in messages.log.

```
techsupport> grep startup /var/log/messages.log
```

```
08/08/10 15:56:42 system_startup: rsrc_file:/etc/aim_rsrc_file
08/08/10 15:56:42 system_startup: Populating resource values from /etc/aim_rsrc_file
08/08/10 15:56:43 system_startup: rsrc_file:/etc/default_rsrc_file
08/08/10 15:56:43 system_startup: Populating resource values from /etc/default_rsrc_file
08/08/10 15:56:44 system_startup: rsrc_file:/etc/products/apphosting/aim_rsrc_file
```

For help using any of the given utilities, please type the name of the utility followed by --help.

Related Commands

Command

show tech-support

Description

Displays a summary of the diagnostic information for the application.

Related Documentation

The following sections describe the documentation available for the Cisco Application eXtension Platform and Cisco ISRs. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents for Cisco IOS Release.

Use these release notes with the documents listed in the following sections:

- [Software Documents, page 10](#)
- [Platform-Specific Documents, page 11](#)

Software Documents

The following documents are specific to Cisco Application eXtension Platform. They are also listed in the Support section at: <http://www.cisco.com/en/US/products/ps9701/index.html>.

- [Cisco Application eXtension Platform 1.1 Feature and Release History](#)

- [Cisco Application eXtension Platform 1.0 Quick Start Guide](#)
- [Cisco Application eXtension Platform 1.1 Developer Guide](#)
- [Cisco Application eXtension Platform 1.1 User Guide](#)
- [Cisco Application eXtension Platform 1.1 Command Reference](#)
- [Open Source Software Licenses for Cisco AXP 1.1](#)

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco ISR routers are available at:

[Cisco Integrated Service Routers](#)

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly [What's New in Cisco Product Documentation](#). This guide lists all new and revised Cisco technical documentation. You can also subscribe to the guide using an RSS feed.

Notices

The following notices 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:

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

Original SSLeay License:

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

This package is an SSL implementation written by Eric Young (ey@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].

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco 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. (1002R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008–2009, Cisco Systems, Inc. All rights reserved.

