Release Notes for Cisco Configuration Professional 2.6

December 5, 2011
OL-26292-01

These release notes support Cisco Configuration Professional (Cisco CP) version 2.6. They should be used with the documents listed in the "Related Documentation" section.

These release notes are updated as needed. To ensure that you have the latest version of these release notes, go to http://www.cisco.com/go/ciscocp. In the Support box, choose **Release and General Information** > **Release Notes**, and then find the latest release notes for your release.

Contents

This document contains the following sections:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 20
- Limitations and Restrictions, page 21
- Important Notes, page 22
- Caveats, page 26
- Related Documentation, page 36
- Glossary, page 37

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

Introduction

Cisco CP is a GUI-based device management tool for Integrated Service Routers. Cisco CP simplifies the router, Firewall, Intrusion Prevention System, VPN, Unified Communications, WAN, and basic LAN configurations through GUI-based, easy-to-use wizards. Cisco CP is installed on a PC.

Routers that are ordered with Cisco CP are shipped with Cisco CP Express installed in router flash memory. Cisco CP Express is a light-weight version of Cisco CP that you can use to configure LAN and WAN interfaces.

System Requirements

This sections describes PC and router system requirements. It contains the following parts:

- PC System Requirements, page 2
- Router System Requirements, page 3
- Cisco CP Ordering Options, page 19

PC System Requirements

Table 1 lists the system requirements for a PC running Cisco CP. Although the Cisco CP application requires Java Runtime Environment (JRE) to run, the Cisco CP Express application included with Cisco CP can run under the native Java Virtual Machine in the supported browsers and JRE.

Table 1 PC System Requirements

System Component	Requirement
Processor	2 GHz processor or faster
Random Access Memory	1 GB DRAM minimum; 2 GB recommended
Hard disk available memory	400 MB
Operating System	Any of the following: • Microsoft Windows 7-32 and 64 bit • Microsoft Windows Vista Business Edition • Microsoft Windows Vista Ultimate Edition • Microsoft Windows XP with Service Pack 3-32 bit • Mac OSX 10.5.6 running Windows XP using VMWare 2.0
Browser	Internet Explorer 6.0 or above
Screen Resolution	1024 X 768
Java Runtime Environment	JRE versions 1.6.0_11 up to 1.6.0_27 supported
Adobe Flash Player	Version 10.0 or later, with Debug set to “No”

Router System Requirements

Router System Requirements are described in the following parts:

- Supported Routers, page 3
- Supported Phones, page 11
- Supported Modules and Cards, page 12
- Connected Grid, page 17
- Determining the Cisco IOS Release, page 18
- Required IP Address Configuration Information, page 19
- Router Configuration Requirements, page 19

Supported Routers

Table 2 lists the routers that Cisco CP supports.

Table 2 Supported Routers

Supported Routers
Cisco 815 Series
CISCO815
CISCO815-VPN-K9
Cisco 819 Series
C819G-U-K9
C819G-V-K9
C819G-S-K9
C819G-B-K9
C819HG+7-K9
C819HG-U-K9
C819HG-V-K9
C819HG-S-K9
Cisco 851 Series
CISCO851-K9
CISCO851W-G-A-K9
CISCO851W-G-E-K9
CISCO851W-G-J-K9
Cisco 857 Series
CISCO857-K9
CISCO857W-G-A-K9
CISCO857W-G-E-K9
Cisco 861 Series

Table 2 Supported Routers (continued)

Supported Routers
CISCO861-K9
CISCO861W-GN-A-K9
CISCO861W-GN-E-K9
CISCO861W-GN-P-K9
Cisco 866 Series
CISCO866VAE
CISCO866VAE-K9
Cisco 867 Series
CISCO867-K9
CISCO867VA-K9
CISCO867VAE
CISCO867VAE-K9
CISCO867W-GN-A-K9
CISCO867W-GN-E-K9
Cisco 871 Series
CISCO871-K9
CISCO871W-G-A-K9
CISCO871W-G-E-K9
CISCO871W-G-J-K9
Cisco 876 Series
CISCO876-K9
CISCO876W-G-E-K9
Cisco 877 Series
CISCO877-K9
CISCO877-M-K9
CISCO877W-G-A-K9
CISCO877W-G-E-K9
CISCO877W-G-E-M-K9
Cisco 878 Series
CISCO878-K9
CISCO878W-G-A-K9
CISCO878W-G-E-K9
Cisco 881 Series

Table 2 Supported Routers (continued)

Supported Routers
C881W-A-K9
C881W-E-K9
CISCO881-K9
CISCO881W-GN-A-K9
CISCO881W-GN-E-K9
CISCO881W-GN-P-K9
CISCO881W-A-K9
CISCO881W-E-K9
CISCO881G-K9
CISCO881GW-GN-A-K9
CISCO881GW-GN-E-K9
CISCO881G-S-K9
CISCO881G-V-K9
CISCO881G-A-K9
C881G-U-K9
C881G-S-K9
C881G-V-K9
C881G-B-K9
C881G+7-K9
C881G+7-A-K9
C881SRST-K9
C881SRSTW-GN-A-K9
C881SRSTW-GN-E-K9
Cisco 886 Series
CISCO886-K9
CISCO886G-K9
CISCO886VA-K9
C886VA-W-E-K9
C886VAG+7-K9
CISCO886GW-GN-E-K9
Cisco 887 Series

Table 2 Supported Routers (continued)

Supported Routers
CISCO887-K9
CISCO887VA-K9
CISCO887VA-M-K9
C887VA-W-A-K9
C887VA-W-E-K9
C887VAM-W-E-K9
C887VAG-S-K9
C887VAG+7-K9
C887VAMG+7-K9
CISCO887W-GN-A-K9
CISCO887W-GN-E-K9
CISCO887M-K9
CISCO887MW-GN-E-K9
CISCO887G-K9
CISCO887GW-GN-A-K9
CISCO887GW-GN-E-K9
CISCO887V-K9
CISCO887VW-GNA-K9
CISCO887VW-GNE-K9
CISCO887VG-K9
CISCO887VGW-GNA-K9
CISCO887VGW-GNE-K9
Cisco 888 Series

Table 2 Supported Routers (continued)

Supported Routers
CISCO888-K9
CISCO888E-K9
CISCO888EA-K9
CISCO888W-GN-A-K9
CISCO888W-GN-E-K9
CISCO888E-K9
CISCO888EW-GNA-K9
CISCO888EW-GNE-K9
CISCO888G-K9
CISCO888GW-G-NA-K9
CISCO888GW-G-NE-K9
C888EG+7-K9
C888SRST-K9
C888SRSTW-GN-A-K9
C888SRSTW-GN-E-K9
Cisco 891 Series
CISCO891-K9
CISCO891W-AGN-A-K9
CISCO891W-AGN-N-K9
Cisco 892 Series
CISCO892-K9
CISCO892F-K9
CISCO892FW-A-K9
CISCO892FW-E-K9
CISCO892W-AGN-E-K9
Cisco 1801
CISCO1801
CISCO1801/K9
CISCO1801-M
CISCO1801-M/K9
CISCO1801W-AG-B/K9
CISCO1801W-AG-C/K9
CISCO1801W-AG-N/K9
CISCO1801WM-AGB/K9
Cisco 1802

Table 2 Supported Routers (continued)

Supported Routers
CISCO1802
CISCO1802/K9
Cisco 1803
CISCO1803/K9
CISCO1803W-AG-B/K9
CISCO1803W-AG-E/K9
Cisco 1805
CISCO1805-D
CISCO1805-D/K9
CISCO1805-EJ
Cisco 1811
CISCO1811/K9
CISCO1811W-AG-B/K9
CISCO1811W-AG-C/K9
CISCO1811W-AG-N/K9
Cisco 1812
CISCO1812/K9
CISCO1812-J/K9
CISCO1812 W-AG-C/K9
CISCO1812W-AG-P/K9
Cisco 1841
CISCO1841
Cisco 1861

Table 2 Supported Routers (continued)

Supported Routers
CISCO1861-SRST-B/K9
CISCO1861-SRST-C-B/K9
CISCO1861-SRST-C-F/K9
CISCO1861-SRST-F/K9
CISCO1861-UC-2BRI-K9
CISCO1861-UC-4FXO-K9
CISCO1861E-SRST-B/K9
CISCO1861E-SRST-C-B/K9
CISCO1861E-SRST-C-F/K9
CISCO1861E-SRST-F/K9
CISCO1861E-UC-2BRI-K9
CISCO1861E-UC-4FXO-K9
CISCO1861W-SRST-C-B/K9
CISCO1861W-SRST-C-F/K9
CISCO1861W-SRST-B/K9
CISCO1861W-SRST-F/K9
CISCO1861W-UC-2BRI-K9
CISCO1861W-UC-4FXO-K9
Cisco 1921
CISCO1921/K9
Cisco 1941
CISCO1941/K9
CISCO1941W-A/K9
CISCO1941W-C/K9
CISCO1941W-E/K9
CISCO1941W-N/K9
CISCO1941W-P/K9
Cisco 2800 Series
CISCO2801
CISCO2811
CISCO2821
CISCO2851
Cisco 2900 Series

Table 2 Supported Routers (continued)

Supported Routers
CISCO2901/K9
CISCO2911/K9
CISCO2921/K9
CISCO2951/K9
Cisco 3800 Series
CISCO3825
CISCO3825-NOVPN
CISCO3845
CISCO3845-NOVPN
Cisco 3900 Series
CISCO3925/K9
CISCO3925E/K9
CISCO3945/K9
CISCO3945E/K9

Supported Phones

Table 3 lists the phones that Cisco CP supports.

Table 3 Supported Phones

Supported Phones	Supported Expansion Modules	Supported Conference Stations
3905		
6901		
6911		
6921		
6941		
6945		
6961		
7902G	7914	7935
7905	7915-12	7936
7906G	7915-24	7937G
7910G	7916-12	
7911G	7916-24	
7912G		
7920		
7921G		
7931G		
7940G		
7941G		
7941G-GE		
7942G		
7945G		
7960G – compatible expansion module (7914)		
7961G – compatible expansion module(7914)		
7961G-GE		
7962G – compatible expansion module(7915,7916)		
7965G – compatible expansion module (7915,7916)		
7970G – compatible expansion module (7914)		
7971G – compatible expansion module (7914)		
7975G – compatible expansion module (7915,7916)		
7985G		

Table 3 Supported Phones (continued)

Supported Phones	Supported Expansion Modules	Supported Conference Stations
8941		
8945		
8961		
9951		
9971		
ATA		
CIPC – Cisco IP Communicator		

Supported Modules and Cards

Table 4 lists the network modules and interface cards that Cisco CP supports.

Table 4 Supported Modules and Cards

Modules and Cards
Advanced Integration
AIM-CUE
AIM2-CUE-K9
AIM-IPS-K9
AIM2-APPRE-104-K9
AIM-VPN/BP II PLUS
AIM-VPN/EP II PLUS
AIM-VPN/HP II PLUS
AIM-VPN/SSL-1
AIM-VPN/SSL-2
AIM-VPN/SSL-3
Analog Dialup
WIC-1AM
WIC-2AM
Analog and Digital Voice/Fax

Table 4 Supported Modules and Cards

Modules and Cards
NM-HD-1V
NM-HD-2V
NM-HD-2VE
NM-HDA-4FXS
NM-HDV2
NM-HDV2-1T1/E1
NM-HDV2-2T1/E1
EVM-HD-8FXS/DID
EM-HDA-8FXS
EM-HDA-4FXO
EM-HDA-6FXO
EM-HDA-3FXS/4FXO
EM-4BRI-NT/TE
EM2-HDA-4FXO
EM3-HDA-8FXS/DID
Application
ISM-SRE-300-K9
SM-SRE-700-K9
SM-SRE-900-K9
NME-WAE-302-K9
NME-WAE-502-K9
NME-WAE-522-K9
NME-APPRE -302-K9
NME-APPRE -502-K9
NME-APPRE -522-K9
Broadband

Table 4 Supported Modules and Cards

Modules and Cards
EHWIC-VA-DSL-A
EHWIC-VA-DSL-B
EHWIC-VA-DSL-M
EHWIC-4SHDSL-EA
EHWIC-1GE-SFP-CU
HWIC-1ADSL
HWIC-1ADSLI
HWIC-1ADSL-M
HWIC-1CABLE-D-2
HWIC-1CABLE-E/J-2
HWIC-1GE-SFP
HWIC-1VDSL
HWIC-2SHDSL
HWIC-4SHDSL
HWIC-4SHDSL-E
HWIC-ADSL-B/ST
HWIC-ADSLI-B/ST
WIC-1SHDSL-V2
WIC-1SHDSL-V3
WIC-1ADSL
WIC 1ADSL-DG
WIC 1ADSL-I-DG
Cisco Unity Voicemail
NME-CUE
NM-CUE
NM-CUE-EC
Ethernet Routed Port
HWIC-1FE
HWIC-2FE
Ethernet Switch

Table 4 Supported Modules and Cards

Modules and Cards
NM-16ESW
NM-16ESW-PWR
NM-16ESW-1GIG
NM-16ESW-PWR-1GIG
NMD-36ESW-PWR
NMD-36ESW-PWR-2GIG
NME-16ES-1G-P
NME-X-23ES-1G-P
NME-XD-24ES-1S-P
NME-XD-48ES-2S-P
SM-32A
SM-ES2-16-P
SM-ES2-24
SM-ES2-24-P
SM-D-ES2-48
SM-ES3-16-P
SM-ES3-24-P
SM-ES3G-16-P
SM-ES3G-24-P
SM-D-ES3-48-P
SM-D-ES3G-48-P
EHWIC-4ESG
EHWIC-4ESG-P
EHWIC-D-8ESG
EHWIC-D-8ESG-P
HWIC-4ESW
HWIC-4ESW-POE
HWIC-D-9ESW
HWIC-D-9ESW-POE
ISDN BRI
WIC-1B-S/T-V3
Multiflex Trunk Voice & WAN Interface Cards
VWIC2-1MFT-T1/E1
VWIC2-2MFT-T1/E1
Serial Sync/Async Interface

Table 4 Supported Modules and Cards

Modules and Cards
HWIC-16A
HWIC-2A/S
HWIC-4A/S
HWIC-8A
HWIC-8A/S-232
WIC-2A/S
Serial WAN Interface
HWIC-1T
HWIC-2T
HWIC-4T
HWIC-1DSU-T1
WIC-1T
WIC-2T
WIC-1DSU-T1-V2
WIC-1DSU-56K4
Voice Interface
VIC-2DID
VIC-4FXS/DID
VIC2-2FXO
VIC2-4FXO
VIC2-2FXS
VIC2-2BRI-NT/TE
VIC2-2E/M
VIC3-4FXS/DID
VIC3-2FXS/DID
VIC3-2FXS-EDID
VPN and Security
NME-IPS-K9
NME-NAC-K9
Wireless AP

Table 4 Supported Modules and Cards

Modules and Cards
HWIC-AP-G-A
HWIC-AP-G-E
HWIC-AP-G-J
HWIC-AP-AG-A
HWIC-AP-AG-E
HWIC-AP-AG-J
Wireless WAN
EHWIC-3G-EVDO-B
EHWIC-3G-EVDO-S
EHWIC-3G-EVDO-V
EHWIC-3G-HSPA+7
EHWIC-3G-HSPA-U
HWIC-3G-CDMA-S
HWIC-3G-CDMA-V
HWIC-3G-HSPA
HWIC-3G-HSPA-A
HWIC-3G-HSPA-G
HWIC-3G-GSM
PCEX-3G-CDMA-V
PCEX-3G-HSPA
PCEX-3G-HSPA-G
PCEX-3G-HSPA-R6
PCEX-3G-HSPA-US
Connected Grid Router
GRWIC-D-ES-6S
GRWIC-D-ES-2S-8PC

Connected Grid

Table 5 lists the connected grid devices that Cisco CP supports.

Table 5 Connected Grid

Switches	Routers
CGS-2520-24TC CGS-2520-16S-8PC	CGR 2010/K9

Cisco IOS Releases

Cisco CP is compatible with the Cisco IOS releases listed in Table 6.

Table 6 Cisco CP-Supported Routers and Cisco IOS Versions

Router Model	Minimum Cisco CP-Supported Cisco IOS Versions
Cisco 815	12.4(11)T
Cisco 850 series	12.4(9)T
Cisco 861	12.4(20)T
Cisco 867	15.0(1)M
Cisco 870 series	12.4(9)T
Cisco 881	12.4(20)T
Cisco 886	15.0(1)M
Cisco 887	15.0(1)M
Cisco 888	12.4(20)T
Cisco 890 series	15.0(1)M
Cisco 1801 Cisco 1802 Cisco 1803	12.4(9)T
Cisco 1805	12.4(15)XY
Cisco 1811 Cisco 1812	12.4(9)T
Cisco 1841	12.4(9)T
Cisco 1861	12.4(20)T
Cisco 1941 Cisco 1941W	15.0(1)M
Cisco 2800 series	12.4(9)T
Cisco 2900 series	15.0(1)M
Cisco 3800 series	12.4(9)T
Cisco 3900 series	15.0(1)M

Determining the Cisco IOS Release

To determine the release of Cisco IOS software currently running on your Cisco router, log into the router and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the Cisco IOS release on the second output line:

```
Router> show version
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.1(2)T1"
```

Required IP Address Configuration Information

Table 7 provides the required IP address configuration for the PC. Use this information to complete the "Task 4: Configure the IP Address On the PC" section in *Cisco Configuration Professional Quick Start Guide*.

Table 7 Required PC IP Address Configurations

Router Model	DHCP Server	Required PC IP Address Configuration
Cisco 815, Cisco 85x, Cisco 86x, Cisco 87x, Cisco 88x, Cisco 89x, Cisco 180x, Cisco 1805, Cisco 1811 and 1812	Yes	Obtains the IP address automatically
Cisco 1841, Cisco 1861, Cisco 28xx, Cisco 38xx, Cisco 29xx, Cisco 39xx	No	Static IP address from 10.10.10.2 to 10.10.10.6 Subnet Mask: 255.255.255.248

Router Configuration Requirements

To run Cisco CP, a router configuration must meet the requirements shown in Table 8.

Table 8 Router Configuration Requirements

Feature	Requirement	Configuration Example

Secure access	SSH and HTTPS	`Router(config)# ip http secure-server`
		`Router(config)# ip http authentication local`
		`Router(config)# line vty 0 15`
		`Router(config)# login local`
		`Router(config-line)# transport input ssh`
		`Router(config-line)# transport output ssh`

Nonsecure access	Telnet and HTTP	`Router(config)# ip http server`
		`Router(config)# ip http authentication local`
		`Router(config)# line vty 0 15`
		`Router(config)# login local`
		`Router(config-line)# transport input telnet`
		`Router(config-line)# transport output telnet`

User privilege level	15	`Router(config)# username cisco privilege 15 secret 0 cisco`

The default configuration file meets all Cisco CP requirements. The default configuration file has the name cpconfig-*model_number*.cfg. For example, the configuration file for the Cisco 860 and Cisco 880 routers is cpconfig-8xx.cfg.

Cisco CP Ordering Options

Table 9 describes the ordering options under which Cisco CP can be ordered. Cisco CP Express is a product that is shipped in router flash memory when the router is ordered with Cisco CP.

Table 9 Cisco CP Ordering Options

Ordering Options	Description
ISR-CCP-CD	Cisco CP: Shipped on CD Cisco CP Express: Shipped in router flash memory SSL Client: Shipped in router flash memory Default Configuration File: Shipped in router flash memory and in NVRAM
ISR-CCP-CD-NOCONF	Cisco CP: Shipped on CD Cisco CP Express: Shipped in router flash memory SSL Client: Shipped in router flash memory Default Configuration File: Shipped in router flash memory
ISR-CCP-EXP	Cisco CP: Not shipped Cisco CP Express: Shipped in router flash memory SSL Client: Shipped in router flash memory Default Configuration File: Shipped in router flash memory and in NVRAM
ISR-CCP-EXP-NOCONF	Cisco CP: Not shipped Cisco CP Express: Shipped in router flash memory SSL Client: Shipped in router flash memory Default Configuration File: Shipped in router flash memory
ISR-CCP-CD=	Cisco CP: Shipped on CD Spare SKU: Mapped to ISR-CCP-CD

New and Changed Information

This section contains new information about Cisco CP and any information about Cisco CP that has changed.

This section contains the following parts:

- New and Changed Features, page 20
- New Hardware Support, page 21

New and Changed Features

There are no new and changed features in this release.

New Hardware Support

The new devices supported are:

- CISCO877VA-GW+7-A-K9
- CISCO877VA-GW+7-E-K9
- CISCO877VA-WD-A-K9
- CISCO877VA-WD-E-K9
- CISCO877VA-V-K9
- CISCO877VA-V-W-E-K9
- CISCO881-V-K9
- CISCO881WD-A-K9
- CISCO881WD-E-K9
- CISCO881GW+7-A-K9
- CISCO881GW+7-E-K9
- CISCO881GW-S-A-K9
- CISCO881GW-V-A-K9
- CISCO888EA-K9

Limitations and Restrictions

This section describes restrictions and limitations that may apply to Cisco CP. It contains the following parts:

- Cisco CP Minimum Screen Resolution, page 21
- JRE Settings for Cisco CP, page 21
- Pop-up Screens Appearing on Primary Monitor if Cisco CP Is Moved to Extended Monitor, page 22

Cisco CP Minimum Screen Resolution

Cisco CP requires a screen resolution of at least 1024 x 768.

JRE Settings for Cisco CP

The following JRE settings are needed for Cisco CP to function properly:

Step 1 Go to **Start > Control Panel > Java**.

Step 2 Click **View** under **Java Applet Runtime Settings**.

Step 3 Select your JRE in use.

Step 4 Set the "Java runtime parameters" with the value "-Xmx256m -Dsun.java2d.d3d=false".

In addition, if JRE is upgraded to versions 1.6.0_11 or above, following settings are needed after Cisco CP installation.

Step 1 Go to **Start > Control Panel > Java > Advance**.

Step 2 Select "Java Plug-in" tree.

Step 3 Uncheck the check box for Enable next-generation Java Plug-in.

Step 4 Restart Cisco CP.

Pop-up Screens Appearing on Primary Monitor if Cisco CP Is Moved to Extended Monitor

If Cisco CP is running on a laptop that is also connected to an external monitor and the screen is set for extended display, pop-up dialog boxes of all SDM applet security pages, routing pages, and help pages appear on the primary monitor. This issue is seen in the following scenario:

Step 1 Connect the monitor to a laptop and set the screen for extended display.

Step 2 Launch Cisco CP and move it to secondary screen.

Step 3 Click **Configure > Security > Security Audit > Perform Security Audit**.

The Audit screen appears in the primary monitor and Cisco CP in the secondary monitor.

Important Notes

This section contains important information for Cisco CP. It contains the following sections:

- Cisco IOS Enforces One-Time Use of Default Credentials, page 22
- Cisco CP Merge and Replace Configuration Functions Fail Under Some Conditions, page 24
- Cisco CP May Lose Connection to Network Access Device, page 24
- Popup Blockers Disable Cisco CP Online Help, page 25
- Screencasts for Cisco CP Features, page 25
- Temporary Internet Files—Impact on Launch, page 25

Cisco IOS Enforces One-Time Use of Default Credentials

To address CSCsm25466, Cisco IOS images included with recent shipments of Cisco 800, Cisco 1800, Cisco 2800, Cisco 2900, Cisco 3800 and Cisco 3900 routers, enforce the one-time use of the default user name and password provided in the Cisco CP configuration file. If you bypass Cisco CP or Cisco CP Express and use a console or Telnet connection to log into the router, the login and exec banners warn you that you must change the user name to “cisco” and the password to “cisco” before you log off the router. If you do not change the credentials as directed, you will not be able to log into the router the next time that you attempt to do so.

The following Cisco IOS releases enforce the one-time use of the default credentials:

- 12.4(11)T or later

- 12.4(11)SW, 12.4(11)SW1, 12.4(11)XV, 12.4(11)XJ
- 12.4(9)T5, 12.4(9)T6
- 15.0(1)M or later

Follow the procedure in this section to secure the router by creating a new username and password, to remove the login banner and exec banner warnings, and to save the configuration changes to the router startup configuration.

Note If you log into the router using a Telnet or a console connection but do not complete the steps in this procedure, be aware of the following:

- If you do not change the default username and password, and then log off the router, you will not be able to log into the router again without entering the **reload** command. No additional warning is given before you log off.
- If you do not change the default username and password, but do enter the **write memory** command before ending the session, future logins will be disabled. In this case, you will need to follow the password recovery procedure at the following link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml

To secure the router, remove the banner warnings and save the changes to the router startup config, complete the following steps:

Step 1 Connect the blue console port on your router to a serial port on your PC using the light blue console cable, included with your router. Refer to your router's hardware installation guide for instructions.

Step 2 Connect the power supply to your router, plug the power supply into a power outlet, and turn on your router. Refer to your router's quick start guide for instructions.

Step 3 Use HyperTerminal or a similar terminal emulation program on your PC, with the terminal emulation settings of 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control, to connect to your router.

Step 4 When prompted, enter the username **cisco**, and password **cisco**.

Step 5 Enter configuration mode by entering the following command:

```
yourname# configure terminal
Create a new username and password by entering the following command:
yourname(config)# username username privilege 15 secret 0 password
```

Replace *username* and *password* with the username and password that you want to use.

Step 6 Remove the default username and password by entering the following command:

```
yourname(config)# no username cisco
```

Step 7 To remove the login banner, enter the following command:

```
yourname(config)# no banner login
```

The login banner warning will no longer appear.

Step 8 To remove the exec banner, enter the following command:

```
yourname(config)# no banner exec
```

The exec banner warning will no longer appear.

Step 9 Leave configuration mode, by entering the following command:

```
yourname(config)# end
```

Step 10 Copy the configuration changes to the startup configuration by entering the following command:

```
yourname# copy running-config startup-config
```

When logging into the router in the future, use the username and password that you created in Step 6.

Cisco CP Merge and Replace Configuration Functions Fail Under Some Conditions

The problem described here is caveat CSCsj21989. If you attempt to merge configuration changes made using the Cisco CP Config Editor feature, or replace the running configuration with a configuration from the Config Editor, the router configuration will not be changed if there is a network device with a Network Address Translation (NAT) IP address, or a cache engine in the connection between the PC and the router. If you need to make changes to the router configuration that you would normally make using the Cisco CP Config Editor, use the Cisco IOS CLI instead.Cisco CP Security Dashboard May Display Threats Unrelated to Your Cisco IOS IPS Installation

Some (or all) of the top threats you obtain using the Cisco CP Security Dashboard may not pertain to your Cisco IOS IPS installation. After you deploy the signatures applicable to the top threats displayed by the Cisco CP Security Dashboard, the dashboard may still display some (or all) top threats with a red icon because applicable signatures could not be found. Those remaining top threats are unrelated to your Cisco IOS IPS installation and are not a danger to your router running Cisco IOS software.

Cisco CP May Lose Connection to Network Access Device

This note concerns the Network Admission Control (NAC) feature.

If the PC used to invoke Cisco CP returns a posture state (Healthy, Infected, Checkup, Quarantine, or Unknown) and if the group policy on the ACS server attached to the posture token assigned to the PC has a redirect URL configured, the connection between Cisco CP and the router acting as the Network Access Device (NAD) may be lost. The same problem can occur if an exception list entry attached to a policy with a redirect URL is configured with the IP address or MAC address of the PC.

If you try to reinvoke Cisco CP from this type of PC, you will not be able to do so because the browser will be redirected to the location specified in the redirect URL.

There are two workarounds for this problem:

- Ensure that the PC that you use to invoke Cisco CP attains a posture token that has an associated group policy on the ACS server that is not configured with a redirect URL.
- Alternatively, use Cisco CP to create a NAC exception list entry with the IP address or MAC address of the PC you use to invoke Cisco CP. Note that the exception list entry created for the PC should be associated to an exception policy that does not have a redirect URL configured in it.

For more information, see the links on the Cisco CP NAC online help pages.

Popup Blockers Disable Cisco CP Online Help

If you have enabled popup blockers in the browser you use to run Cisco CP, online help will not appear when you click the help button. To prevent this from happening, you must disable the popup blocker when you run Cisco CP. Popup blockers may be enabled in search engine toolbars, or may be standalone applications integrated with the web browser.

Microsoft Windows XP with Service Pack 2 blocks popups by default. To turn off popup blocking in Internet Explorer, go to **Tools** > **Pop-up Blocker** > **Turn Off Pop-up Blocker**.

If you have not installed and enabled third-party pop up blockers, go to **Tools** > **Internet Options** > **Privacy**, and uncheck the **Block popups** checkbox.

Screencasts for Cisco CP Features

Instead of online help, screencasts have been provided for the following Cisco CP 2.6 features:

These screencasts are located at:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html

You must have Internet access to view the screencasts.

Temporary Internet Files—Impact on Launch

Because of Microsoft Windows Java caching issues, Cisco CP is sometimes unable to complete discovery of a device. To fix this issue, complete the following steps:

Step 1 Choose **Application** > **Exit** to shut down Cisco CP.

Step 2 Close all existing Internet Explorer windows.

Step 3 Go to **Start** > **Control Panel** > **Java**. The General tab is displayed.

Step 4 In the Temporary Internet Files box, click **Delete Files**.

Step 5 In the displayed dialog, leave all file types checked, and click **OK**.

Step 6 Click **OK** in the Java control panel to close it.

Step 7 Restart Cisco CP.

Caveats

Caveats describe unexpected behavior in Cisco CP. This section contains the following:

- Resolved Caveats, page 26
- Open Caveats, page 26

Resolved Caveats

Table 10 lists caveats that are resolved in Cisco CP 2.6.

Table 10 Resolved Caveats in Cisco CP 2.6

Bug ID	Summary
CSCtn10418	Devices get stuck in the discovering state.

Open Caveats

Table 11 lists caveats that are open in Cisco CP 2.6.

Table 11 Open Caveats in Cisco CP 2.6

Bug ID	Summary	Additional Information
CSCtw51884	The create/edit/delete action fails on the GSM profile screen when the hostname has the + character.	**Symptom** The Create, Edit or Delete action fails on the GSM profile screen and Cisco CP displays this error message *Error has occurred while configuring Cellular GSM modem profile*. However, Cisco CP configures the router successfully. **Conditions** This problem is seen when the hostname of the router has any illegal character. For example: !,@, #, $,%, ^, &, *, (), and +. For example, C881GW+7 is not a valid hostname. **Workaround** .Remove the illegal characters from the hostname and rediscover the device.
CSCtt45687	The VPN design guide does not launch on the Google chrome browser.	**Symptom** The Cisco CP does not display the VPN design guide when you select **Configure > Security > VPN > VPN Design Guide**. **Conditions** This problem is seen when the Google chrome browser is set as the default browser in the system. **Workaround** Set the Mozilla Firefox or Internet Explorer as the default browser in your system.

Table 11 Open Caveats in Cisco CP 2.6 (continued)

Bug ID	Summary	Additional Information
CSCtu18162	Editing the non-persistent backup to persistent does not remove the cellular route.	**Symptom** Editing the non-persistent backup configuration to persistent backup configuration using Cisco CP does not remove the existing default IP route via the cellular interface while creating a new default route via dialer interface. **Conditions** This problem is seen when you try to edit an existing non-persistent back-up configuration that is associated with the cellular interface to persistent backup configuration. **Workaround** After configuring the cellular interface as persistent backup configuration, remove the existing IP router via cellular interface. To remove the IP route, follow these steps. 1. Navigate to **Configure > Router > Static and Dynamic Routing**. 2. Select the default route via cellular interface from the Static Routing table. 3. Click **Delete**. 4. Cisco CP will generate the CLI preview window. The CLI will be similar to "no ip route 0.0.0.0 0.0.0.0 cellular 0 1" depending upon the slot number into which the modem is inserted. 5. Click **Deliver** to configure the router.
CSCtr24865	The security/routing screens are not visible fully if the screen display settings is set to 150%.	**Symptom** The security and routing screens are not visible fully. **Conditions** This issue occurs when you select **Control Panel > All Control Panel Items > Display** and set the display settings to 150%. **Workaround** Select the **Control Panel > All Control Panel Items > Display** and set the display settings to 100%.
CSCto13265	Site-to-site VPN displays duplicate tunnel entry.	**Symptom** Cisco CP displays duplicate entries for GREoIPSEC VPN in the summary screen. **Conditions** Duplicate entries are seen when more than one GREoIPSEC tunnel is configured on the router. **Workaround** There is no workaround.

Table 11 Open Caveats in Cisco CP 2.6 (continued)

Bug ID	Summary	Additional Information
CSCtw55536	H323 settings are not available with TDM gateway.	**Symptom** H.323 settings are not available from VoIP settings feature with Unified Communication Mode as SRST, SRST with TDM gateway, and TDM gateway. **Conditions** You cannot configure the H.323 settings in the SRST, SRST with TDM gateway, and TDM gateway modes irrespective of dial-peer protocol and connection settings. **Workaround** Manually configure the H.323 settings under the Voice Service VoIP. However, the default parameters are unaltered.
CSCtw61469	Cannot configure the SIP trunk on Cisco 892F router.	**Symptom** You cannot configure the SIP Trunk on a Cisco 892F-CUBE ISR device. Resetting the Unified Communication mode to default and changing the CUBE settings is not successful due to CLI error. **Conditions** This problem occurs only when a Cisco 892F-CUBE ISR device is configured with CUBE feature. Cisco CP does not allow you to unconfigure or configure the SIP trunk on the device. The following CLIs cannot be configured or unconfigured on the device: • **call threshold global cpu-avg low 68 high 75** • **no call threshold global cpu-avg low 68 high 75** • **call threshold global total-mem low 75 high 85** • **no call threshold global total-mem low 75 high 85** **Workaround** Configure the SIP Trunk manually or follow these steps. 1. Discover the Cisco 892F-CUBE ISR with Unified Communication mode as CUBE. 2. Navigate to SIP Trunks. 3. Select the service provider and provide inputs for the available parameters. 4. Save the generated CLI preview in a text file. 5. Use the Config Editor to upload the file after removing the above mentioned CLIs and apply the config.

Table 11 Open Caveats in Cisco CP 2.6 (continued)

Bug ID	Summary	Additional Information
CSCtu13147	IPS Auto update screen does not display the complete configured information.	**Symptom** Configure the IPS Auto Update settings using the Local Server option. Rediscover the device, part of the configured information related to recurring update schedule is missing from the **Edit IPS > Auto Update > Local Server** screen. **Conditions** This problem is seen when you configure the IPS Auto Update settings using the Local Server option and configure the Update Schedule by selecting the **Setup Recurring Update** check box. The IPS Auto Update screen does not display the complete configured information when you rediscover the device and navigate to IPS Auto Update screen. **Workaround** There is no workaround.
CSCto88259	*GenericJDBCException* seen while launching Cisco CP.	**Symptom** The following error is seen during launch of Cisco CP: `org.hibernate.exception.GenericJDBCException: Cannot open connection` **Conditions** This problem rarely occurs and there are no specific steps which create the problem. Database corruption can cause it. **Workaround** Reinstall Cisco CP.
CSCtn10781	Overlaid extensions do not follow the order you specified.	**Symptom** • Case 1—When selecting multiple extensions to be overlaid on a button, the order of extensions is not the same as specified by you. • Case 2—The display name is overwritten when the extension is part of an overlay group. **Conditions** • Case 1—This occurs when you select multiple extensions to be overlaid on a phone button. • Case 2—This occurs when the same extension is overlaid on multiple phones. **Workaround** There is no workaround. If you require a particular order or display name, you can configure it through the CLI.

Table 11 Open Caveats in Cisco CP 2.6 (continued)

Bug ID	Summary	Additional Information
CSCtn58565	Auto-line command does not work for phones.	**Symptom** When editing a phone, the auto-line incoming command does not run. **Conditions** This problem occurs when editing a phone to set Auto Line Selection to Incoming. **Workaround** There is no workaround. Manually configure the auto-line incoming command under an ephone.
CSCto70309	Unified Communications mode is displayed as CUBE when the **mode border-element** command is not configured.	**Symptom** On an ISR-G2, if the **mode border-element** command is not configured under **voice service voip** and if **telephony service** and **max-dn** commands are configured, Cisco CP displays the Unified Communications feature as CUBE. **Conditions** This problem occurs only on an ISR-G2 if the m**ode border-element** is not configured and if **max-dn** is configured under the **telephony-service** command. **Workaround** Select the appropriate mode in the Unified Communications Features screen and deliver the CLI.
CSCtn98336	Reset to default in Unified Communications Features does not clear some configurations.	**Symptom** The Reset to Default option in the Unified Communications Features screen does not remove some of the configurations from the router. **Conditions** This problem is seen when you configure the Gateway option via Cisco CP and then select Reset to Default. The Universal and Security Transcoding Dspfarm profile in the gateway configuration is not removed from the router. **Workaround** Remove the configuration through the CLI.

Table 11 Open Caveats in Cisco CP 2.6 (continued)

Bug ID	Summary	Additional Information
CSCto67064	Certain date formats not supported in EnergyWise scheduling.	**Symptom** When you try to access the EnergyWise feature, the following error is displayed: `An internal error has occurred.` **Conditions** This issue is seen when you have entered EnergyWise schedule in a format that is not supported by Cisco CP (involving commas). Cisco CP does not support manual configuration of schedules because these schedules can be read incorrectly or can cause existing schedules to be removed. Cisco CP compatible schedules contain a date format in the form of spaced numbers without the use of commas, for example energywise level 1 recurrence importance 1 at 0 1 * * 0. Wildcards (*) are allowed in addition to 0–9. **Workaround** If you have a schedule with an incompatible format, convert it into multiple schedules that are compatible with Cisco CP: energywise level 1 recurrence importance 1 at 0 1 * * 0,1,2,3,4,5,6 should be converted to: energywise level 1 recurrence importance 1 at 0 1 * * 0 energywise level 1 recurrence importance 1 at 0 1 * * 1 energywise level 1 recurrence importance 1 at 0 1 * * 2 energywise level 1 recurrence importance 1 at 0 1 * * 3 energywise level 1 recurrence importance 1 at 0 1 * * 4 energywise level 1 recurrence importance 1 at 0 1 * * 5 energywise level 1 recurrence importance 1 at 0 1 * * 6
CSCto07804	Traffic Monitoring Netflow Services fails to start in some scenarios.	**Symptom** Data Collector Service fails to start as a result of which data is not collected from the router. **Conditions** This can happen if files are not copied properly or get corrupted while installing the Data Collector Service. **Workaround** Reinstall the Data Collector Service.

Table 11 Open Caveats in Cisco CP 2.6 (continued)

Bug ID	Summary	Additional Information
CSCto73606	Traffic Monitoring: Cisco CP displays error when you click Start Monitoring or Stop Monitoring on any interface while Data Collector Services are not running.	**Symptom** Cisco CP displays a pop-up with *Java.lang.NullPointerException* error when you try to stop monitoring by clicking on the Stop Monitoring link, while the Interface Collector Service is not running. **Conditions** Cisco CP displays error when you try to stop monitoring by clicking on the Stop Monitoring link, while the Interface Collector Service is not running. **Workaround** Start the Interface Collector Service and then stop monitoring.
CSCto76962	Traffic Monitoring: Cisco CP displays value as 0 when interface is not being monitored.	**Symptom** Cisco CP displays the value as zero (0) if an interface is not being monitored for some time. **Conditions** If you monitor traffic on an interface for some time, stop and then start monitoring traffic again, Cisco CP displays a value of zero for the time interval when you were not monitoring the interface. **Workaround** There is no workaround.
CSCto96064	Rollback failing when imported phone is SIP.	**Symptom** Cisco CP displays an error message that rollback has failed on Bulk Import and the application does not get updated. You can see bulk imported data under phones, users, and extensions. **Conditions** Rollback on Bulk Import with a SIP phone entry is failing as the commands **no create profile** and **create profile** issued during rollback fails. As a result, rollback is considered as failed although the configuration on the router created due to Bulk Import has reverted successfully. **Workaround** Manually issue the command **no create profile** followed by the command **create profile** under **voice register global** to update the files on the Flash. Rediscover the device.

Table 11 Open Caveats in Cisco CP 2.6 (continued)

Bug ID	Summary	Additional Information
CSCto83180	Multiple virtual machines (VMs) installed on SRE-V are not displayed.	**Symptom** • Case 1—If you did not select a virtual machine in **Configure > Interface Management > Module Configuration > SRE-V > Permissions > User/Group > Edit**, Select is displayed. • Case 2—Adding one more virtual machine using **Configure > Interface Management > Module Configuration > SRE-V > Permissions > User/Group > Edit** removes the previously added virtual machine configuration. • Case 3—Multiple entries are shown in the SRE-V Permissions screen for each user/group. **Conditions** • Case 1—In **Configure > Interface Management > Module Configuration > SRE-V > Permissions > User/Group > Edit**, when you do not select a virtual machine from the drop-down menu, Select is displayed. • Case 2—When the user/group already has one virtual machine associated with it, adding one more virtual machine using **Configure > Interface Management > Module Configuration > SRE-V > Permissions > User/Group > Edit** can remove the previously added virtual machine configuration. • Case 3—When a virtual machine, for example **VM1** is already added to the user/group, adding one more virtual machine may create multiple entries in the Permissions summary screen upon refreshing the page. **Workaround** • Case 1—There is no workaround. Assume that the default virtual machine Host is associated to the user/group when Select is displayed. • Case 2—To add multiple virtual machines to the user/group, use the CLI. • Case 3—Read each entry as corresponding to one instance of virtual machine associated with the user/group.

Table 11 Open Caveats in Cisco CP 2.6 (continued)

Bug ID	Summary	Additional Information
CSCto85895	GRWIC-D-ES-2S-8PC/-6S - 802.1x moving to high-security mode directly fails.	**Symptom** When you click Finish in the 802.1x wizard for GRWIC-D-ES-2S-8PC or GRWIC-D-ES-6S with high-security or low-impact as the mode an error *Configuration failed radius-server vsa send* is seen. **Conditions** This issue is seen when you click **Finish** in the 802.1x wizard for GRWIC-D-ES-2S-8PC or GRWIC-D-ES-6S with high-security mode or low-impact mode. The issue is not seen in the monitor mode. **Workaround** Configure AAA details using monitor mode and then change to low-impact mode or high-security mode.
CSCth67558	Unable to discover switching module.	**Symptom** Cisco CP fails to discover switching module and reports that the module is being reloaded in the discovery details. **Conditions** When the switching module is configured with login local or AAA new-model configuration or both, the module requires one more level of authentication along with the usual authentication. In this case, you need to provide the username and password twice to get into the module prompt. **Workaround** Remove the login local and AAA new-model configuration so that the extra level of authentication is not required.

Table 11 Open Caveats in Cisco CP 2.6 (continued)

Bug ID	Summary	Additional Information
CSCto98404	Number of Retries Remaining displays as NULL if wrong SIM PIN is entered.	**Symptom** Cisco CP displays Numbers of Retries Remaining as NULL, instead of the correct value. **Conditions** This issue is seen when the router has IOS version 151-3.T1 or above and you enter the wrong SIM PIN to run any SIM operations on the HSPA modem. **Workaround** There is no workaround.
CSCth34158	Switching Modules folder is not listed in the left navigation pane.	**Symptom** Switching Modules folder is not listed in the left navigation pane even when the device has supported switch modules that are managed by Cisco CP. **Conditions** • Multiple levels (more than one level) of authentication is required for accessing the switch module console. • Enabled password is configured on the device. • AAA is configured on both the router and the switch modules. • Privilege level 15 is not configured under **line con 0**. **Workaround** • Ensure that the router and switch have the same username (privilege level 15) and a password is configured when switch console requires authentication. • If there is no login configured for **line con 0**, ensure privilege level 15 is configured under l**ine con 0**. • If AAA is configured on the router, make sure that no authentication is required for the switch module and privilege level 15 is configured under **line con 0**.

Related Documentation

Table 12 describes the related documentation available for Cisco CP.

Table 12 Cisco Configuration Professional Documentation

Document Title	Available Formats
Readme First for Cisco Configuration Professional	This document is available at the following locations: • www.cisco.com • Product CD-ROM in the Documentation folder
Cisco Configuration Professional Quick Start Guide	This guide is available at the following locations: • www.cisco.com • Product CD-ROM in the Documentation folder
Cisco Configuration Professional Getting Started Guide	This guide is available at the following locations: • www.cisco.com • Product CD-ROM in the Documentation folder **Note** During the installation process, just before you have finished installing the product, you are provided the option to read the Getting Started guide.
Cisco Configuration Professional User Guide	This guide is available at the following locations: • www.cisco.com • Online help
Cisco Configuration Professional Express User Guide	This guide is available at the following locations: • www.cisco.com • Online help
Release Notes for Cisco Configuration Professional	This document is available at the following location: www.cisco.com
Release Notes for Cisco Configuration Professional Express	This document is available at the following location: www.cisco.com

Note For information on obtaining documentation and technical assistance, product security, and 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.

Glossary

ACEs—Access List Elements

ACLs—Access Control Lists

B-ACD—Basic Automatic Call Distribution

CUBE—Cisco Unified Border Element

HWIC—High-Speed WAN Interface Card

HSPA—High-Speed Packet Access

HSPA—A—High-Speed Packet Access for Americas

HSPA—G—High-Speed Packet Access for Global

PCEX—PC Express

PPP—Point-to-Point Protocol (PPP) PDP type

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.