Release Notes for Cisco Configuration Professional 2.4

December 15, 2010
OL-23724-01

These release notes support Cisco Configuration Professional (Cisco CP) version 2.4. 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 **General Information** > **Release Notes**, and then find the latest release notes for your release.

Contents

This document contains the following sections:

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 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 13

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_21 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

Table 2 and Table 3 list the routers that Cisco CP supports.

Table 2 Supported Integrated Services Routers (ISR)

Cisco 800 Series	Cisco 1800 Series	Cisco 2800 Series	Cisco 3800 Series
CISCO815	CISCO1801	Cisco 2801	Cisco 3825
CISCO815-VPN-K9	CISCO1801-M	Cisco 2811	Cisco 3825-NOVPN
	CISCO1801/K9	Cisco 2821	Cisco 3845
	CISCO1801-M/K9	Cisco 2851	Cisco 3845-NOVPN
	CISCO1801WM-AGE/K9		
	CISCO1801W-AG-B/K9		
	CISCO1801W-AG-C/K9		
	CISCO1801W-AG-N/K9		
CISCO851-K9	CISCO1802		
CISCO851W-G-A-K9	CISCO1802/K9		
CISCO851W-G-E-K9	CISCO1802W-AG-E/K9		
CISCO851W-G-J-K9			
CISCO857-K9	CISCO1803/K9		
CISCO857W-G-A-K9	CISCO1803W-AG-B/K9		
CISCO857W-G-E-K9	CISCO1803W-AG-E/K9		

Table 2 Supported Integrated Services Routers (ISR) (continued)

Cisco 800 Series	Cisco 1800 Series	Cisco 2800 Series	Cisco 3800 Series
CISCO871-K9 CISCO871W-G-A-K9 CISCO871W-G-E-K9 CISCO871W-G-J-K9	CISCO1805-D CISCO1805-D/K9 CISCO1805-EJ		
	CISCO1811/K9 CISCO1811W-AG-B/K9 CISCO1811W-AG-C/K9 CISCO1811W-AG-N/K9		
CISCO876-K9 CISCO876W-G-E-K9	CISCO1812/K9 CISCO1812-J/K9 CISCO1812 W-AG-C/K9 CISCO1812W-AG-P/K9		
CISCO877-K9 CISCO877-M-K9	CISCO1841		
CISCO877W-G-A-K9 CISCO877W-G-E-K9 CISCO877W-G-E-M-K9	C1861E-SRST-B/K9 C1861E-SRST-C-B/K9 C1861E-SRST-C-F/K9 C1861E-SRST-F/K9 C1861E-UC-2BRI-K9 C1861E-UC-4FXO-K9		
CISCO878-K9 CISCO878W-G-A-K9 CISCO878W-G-E-K9	C1861W-SRST-C-B/K9 C1861W-SRST-C-F/K9 CISCO1861W-SRST-B/K9 CISCO1861W-SRST-F/K9 CISCO1861W-UC-2BRI-K9 C1861W-UC-4FXO-K9		

Table 3 Supported Integrated Services Routers - G2 (ISR- G2)

Cisco 800 Series	Cisco 1900 Series	Cisco 2900 Series	Cisco 3900 Series
CISCO861-K9	CISCO1921	CISCO2901/K9	CISCO3925/K9
CISCO861W-GN-A-K9		CISCO2911/K9	CISCO3925E/K9
CISCO861W-GN-E-K9		CISCO2921/K9	CISCO3945/K9
CISCO861W-GN-P-K9		CISCO2951/K9	CISCO3945E/K9
CISCO867-K9	CISCO1941/K9		
CISCO867W-GN-A-K9	CISCO1941W-A/K9		
CISCO867W-GN-E-K9	CISCO1941W-C/K9		
	CISCO1941W-E/K9		
	CISCO1941W-N/K9		
	CISCO1941W-P/K9		
CISCO881G-A-K9			
CISCO881G-G-K9			
CISCO881G-S-K9			
CISCO881G-V-K9			
CISCO881GW-GN-A-K9			
CISCO881GW-GN-E-K9			
CISCO881-K9			
CISCO881SRST-K9			
CISCO881SRSTW-GN-A-K9			
CISCO881SRSTW-GN-E-K9			
CISCO881W-GN-A-K9			
CISCO881W-GN-E-K9			
CISCO881W-GN-P-K9			
CISCO886G-K9			
CISCO886GW-GN-E-K9			
CISCO886-K9			
CISCO886VA-K9			
CISCO886W-GN-E-K9			
CISCO887G-K9			
CISCO887GW-GN-A-K9			
CISCO887GW-GN-E-K9			
CISCO887-K9			
CISCO887M-K9			
CISCO887MW-GN-E-K9			

Table 3 Supported Integrated Services Routers - G2 (ISR- G2) (continued)

Cisco 800 Series	Cisco 1900 Series	Cisco 2900 Series	Cisco 3900 Series
CISCO887VA-K9			
CISCO887VA-M-K9			
CISCO887VG-K9			
CISCO887VGW-GNA-K9			
CISCO887VGW-GNE-K9			
CISCO887V-K9			
CISCO887VSRST-K9			
CISCO887VW-GNA-K9			
CISCO887VW-GNE-K9			
C888ESRSTW-GNA-K9			
C888ESRSTW-GNE-K9			
CISCO888EG-K9			
CISCO888EGW-GNA-K9			
CISCO888EGW-GNE-K9			
CISCO888E-K9			
CISCO888EW-GNA-K9			
CISCO888EW-GNE-K9			
CISCO888G-K9			
CISCO888GW-G-NA-K9			
CISCO888GW-G-NE-K9			
CISCO888-K9			
CISCO888SRST-K9			
CISCO888W-GN-A-K9			
CISCO888W-GN-E-K9			
CISCO891-K9			
CISCO891W-AGN-A-K9			
CISCO891W-AGN-N-K9			
CISCO892F-K9			
CISCO892FW-AGN-A-K9			
CISCO892FW-AGN-E-K9			
CISCO892-K9			
CISCO892W-AGN-E-K9			

Supported Phones

Table 4 lists the phones that Cisco CP supports:

Table 4 Supported Phones

Supported Phones	Supported Expansion Modules	Supported Conference Stations
6901		
6911		
6921		
6941		
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		
ATA		
CIPC – Cisco IP Communicator		

Supported Network Modules

Table 5 and Table 6 list the network modules that Cisco CP supports.

Table 5 Supported Network Modules

Network Modules	Enhanced Network Modules	Wide Area Application Services (WAAS) Modules	Advanced Integration Modules (AIMs)	Voice Network Modules
NM-4T	NME-IPS-K9	NME-WAE-502-K9	AIM-VPN/BP II PLUS	NM-HD-1V
NM-1FE2W-V2	NME-16ES-1G-P	NME-WAE-522-K9	AIM-VPN/EP II PLUS	NM-HD-2V
NM-1FE-FX-V2	NME-X-23ES-1G-P	NME-WAE-302-K9	AIM-VPN/HP II PLUS	NM-HD-2VE
NM-2FE2W-V2	NME-XD-24ES-1S-P		AIM-VPN/SSL-1	NM-HDA-4FXS
NM-1FE-FX	NME-XD-48ES-2S-P		AIM-VPN/SSL-2	NM-HDV2
NM-4A/S (synchronous only)	NME-VMSS-16		AIM-VPN/SSL-3	NM-HDV2-1T1/E1
NM-8A/S (synchronous only)	NME-VMSS-HP-16		AIM-IPS-K9	NM-HDV2-2T1/E1
NM-CIDS-K9	NME-VMSS-HP-32		AIM-CUE	EVM-HD-8FXS/DID
NM-16ESW	NME-APPRE-302-K9		AIM2-CUE-K9	EM-HDA-8FXS
NM-16ESW-1GIG	NME-APPRE-522-K9		AIM2-APPRE-104-K9	EM-HDA-4FXO
NM-16ESW-PWR	NME-APPRE-502-K9			EM2-HDA-4FXO
NM-16ESW-PWR-1GIG				EM-HDA-3FXS/4FXO
NMD-36ESW-PWR				EM-HDA-6FXO
NMD-36ESW-PWR-2GIG				EM-4BRI-NT/TE
				NM-CUE
				NM-CUE-EC
				NME-CUE
				EM3-HDA-8FXS/DID

Table 6 Supported Cisco SRE Internal Service Modules, Cisco SRE Service Modules and EtherSwitch Modules

Cisco SRE Internal Service Modules	Cisco SRE Service Modules	EtherSwitch Modules
ISM-SRE-300-K9	SM-SRE-700-k9	SM-ES2-16-P
	SM-SRE-900-k9	SM-ES2-24
		SM-ES2-24-P
		SM-D-ES2-48
		SM-ES3-16-P
		SM-ES3G-16-P
		SM-ES3-24-P
		SM-ES3G-24-P
		SM-D-ES3-48-P
		SM-D-ES3G-48-P

Supported Interface Cards

Table 7 lists the interface cards that Cisco CP supports.

Table 7 Supported Cards

WAN Interface Cards (WICs)	High-speed WAN Interface Cards (HWICs)	Voice Interface Cards
WIC-1T	EHWIC-4ESG	VIC2-4FXO
WIC-2T	EHWIC-4ESG-P	VIC2-2FXS
WIC-2A/S (Frame Relay, PPP, HDLC, no asynchronous)	EHWIC-8ESG-P	VIC2-2FXO
WIC-1ADSL	EHWIC-D-8ESG	VIC2-2BRI-NT/TE
WIC-1DSU-T1-V2	HWIC-16A	VIC-2DID
WIC-1B-S/T-V3	HWIC-1ADSL	VIC-4FXS/DID
WIC-1AM	HWIC-1ADSLI	VIC3-4FXS/DID
WIC-2AM	HWIC1-ADSL-M	VIC3-2FXS/DID
WIC-4ESW	HWIC-1ADSL-M (WIC card with Annex M)	VWIC2-1MFT-T1/E
WIC-1SHDSL-V2	HWIC-1CABLE-D-2	VWIC2-2MFT-T1/E1
WIC-1SHDSL-V3	HWIC-1CABLE-E/J-2	
WIC 1ADSL-DG	HWIC-1DSU-T1	
WIC 1ADSL-I-DG	HWIC-1FE	
	HWIC-1T	
	HWIC-1VDSL	
	HWIC-2A/S	

Table 7 Supported Cards (continued)

WAN Interface Cards (WICs)	High-speed WAN Interface Cards (HWICs)	Voice Interface Cards
	HWIC-2FE	
	HWIC-2SHDSL	
	HWIC-2T	
	HWIC-3G-CDMA-S	
	HWIC-3G-CDMA-V	
	HWIC-3G-GSM	
	HWIC-3G-HSPA	
	HWIC-3G-HSPA-A	
	HWIC-3G-HSPA-G	
	HWIC-4A/S	
	HWIC-4ESW	
	HWIC-4ESW-POE	
	HWIC-4SHDSL	
	HWIC-4SHDSL-E	
	HWIC-4T	
	HWIC-8A	
	HWIC-8A/S-232	
	HWIC-ADSL-B/ST	
	HWIC-ADSLI-B/ST	
	HWIC-AP-AG-A	
	HWIC-AP-AG-E	
	HWIC-AP-AG-J	
	HWIC-AP-G-A	
	HWIC-AP-G-E	
	HWIC-AP-G-J	
	HWIC-D-9ESW	
	HWIC-D-9ESW-POE	
	PCEX-3G-HSPA-x	

Connected Grid

Table 8 lists the connected grid devices that Cisco CP supports

Table 8 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 9.

Table 9 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

Table 9 Cisco CP-Supported Routers and Cisco IOS Versions (continued)

Router Model	Minimum Cisco CP-Supported Cisco IOS Versions
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 in to 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 10 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 10 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 11.

Table 11 Router Configuration Requirements

Feature	Requirement	Configuration Example

Secure access	SSH and HTTPS	`Router(config)# ip http secure-server`
		`Router(config)# line vty 0 4`
		`Router(config-line)# transport input ssh`

Nonsecure access	Telnet and HTTP	`Router(config)# ip http server`
		`Router(config)# line vty 0 4`
		`Router(config-line)# transport input 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 12 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 12 Cisco CP Ordering Options

Ordering Options	Description
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
CCP-CD-NOCF	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 **Note** This ordering option does not provide the default configuration file for Cisco 800 series routers.
CCP-EXPRESS	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

Table 12 Cisco CP Ordering Options (continued)

Ordering Options	Description
CCP-EXPRESS-NOCF	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 **Note** This ordering option does not provide the default configuration file for Cisco 800 series routers.
ISR-CCP-CD=	Cisco CP: Shipped on CD Spare SKU: Mapped to ISR-CCP-CD
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

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

Cisco CP 2.4 supports the following new and changed features:

- MAC Address
  Cisco CP now supports static and secure MAC addresses, in addition to dynamic addresses. Static and secure MAC address support is currently available only on the Cisco 2520 series switches.
- SIP Trunk Enhancements
  Advanced SIP UA header parameters such as **retry options**, **retry connect**, and **timer** are now available. These parameters are available from the Advanced tab.
- SRSV-CUE
  Cisco CP now supports the Cisco Unity Express SRSV module (SRSV-CUE) which handles voicemail services during a network failure. This module is embedded in a Cisco Integrated Services Router (ISR) or Cisco Integrated Service Routers Generation 2 (ISR G2) platform. Cisco SRSV-CUE protects your communications with voicemail survivability for your organization's remote sites, such as branch offices or other small sites. When a remote site does not have access to your central voicemail system, as during a network service interruption, Cisco Unified Survivable Remote Site Voicemail provides voicemail backup services. This helps to ensure your remote site continues to have voicemail and auto-attendant service. For more information, see http://www.cisco.com/web/go/srsv
- VDSL multi mode (ATM/Ethernet) support
  Cisco CP now provides ADSL/ATM mode support along with VDSL/Ethernet mode support for the CISCO886VA-K9, CISCO887VA-K9, and CISCO887VA-M-K9 platforms. Depending on the DSLAM running mode, you have the option of configuring your router either in the VDSL/Ethernet mode in the ADSL/ATM mode.
- Voice Class Codec
  Cisco CP now supports offer-all keyword.
- Voice Service VoIP
  The following new input fields are now available:
  - Bind interface
  - Session transport SIP/UDP
  - Registrar server
- VoIP Dial Peer
  The following new input fields are now available:
  - DTMF relay
  - Voice-class SIP early-offer forced
  - Bind interface
- VoIP Settings
  The VoIP Settings page now displays the configured VoIP parameters with their values. You can configure general VoIP settings, SIP settings, and H.323 settings from the Edit VoIP Settings page.

For the following features, the look-and-feel has changed:

- Interface Management > Cellular WAN > Edit Cellular WAN Interface
- Utilities > Flash File Management
- Utilities > Configuration Editor
- Utilities > View > Default Rules

Note Licenisng feature is not supported in this release.

New Hardware Support

The new devices supported are:

- CISCO886VA-K9
- CISCO887VA-K9
- CISCO887VA-M-K9
- CISCO887V-K9
- C888ESRSTW-GNA-K9
- C888ESRSTW-GNE-K9
- CISCO888EG-K9
- CISCO888EGW-GNA-K9
- CISCO888EGW-GNE-K9
- CISCO888E-K9
- CISCO888EW-GNA-K9
- CISCO888EW-GNE-K9
- CISCO892F-K9
- CISCO892FW-AGN-A-K9
- CISCO892FW-AGN-E-K9
- CISCO892-K9
- CISCO892W-AGN-E-K9
- EHWIC-4ESG
- EHWIC-4ESG-P
- EHWIC-8ESG-P
- EHWIC-D-8ESG
- HWIC-1VDSL
- HWIC-4SHDSL-E

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

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 which is also connected to an external monitor, and if the screen is set for extended display, pop-up screens are seen in all SDM applet security and routing, and help pages. The steps to reproduce this are:

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

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

Step 3 Go to **security audit** and click **perform security audit**.
The audit screen appears in the primary monitor; whereas, Cisco CP is still 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

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

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
```

Step 6 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 7 Remove the default username and password by entering the following command:

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

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

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

The login banner warning will no longer appear.

Step 9 To remove the exec banner, enter the following command:

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

The exec banner warning will no longer appear.

Step 10 Leave configuration mode, by entering the following command:

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

Step 11 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.

Another problem described here is caveat CSCtj28175. Replacing the running configuration could fail because of various reasons. The following are a few of the possible causes:

- Running configuration contains one or more interactive commands which are not supported in Cisco CP.
- Port 21 is already in use for other applications, for example, FTP server. If this is the case, disable the FTP server and try this operation again.
- Connection to the device was lost.

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 2.4 features:

- 3G Feature Enhancements
- Bulk Import
- Cisco Unified CME B-ACD
- Configuration Editor
- Flash File Management
- Module Configuration
- SIP Trunk
- VoIP Dial Peer

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 IE 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.

Internet Explorer Zoom Level - Impact on Some Cisco CP Screens

If the browser's zoom level is set to a value other than 100%, some portions of the Java screens in Cisco CP are not seen. To fix this issue, complete the following steps:

Step 1 Close the Cisco CP application.

Step 2 Launch Internet Explorer and reset the zoom level to 100% using the "zoom level" selection on the status bar.

Step 3 Close Internet Explorer.

Step 4 Launch Cisco CP.

Caveats

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

Resolved Caveats

Table 13 lists caveats that are resolved in Cisco CP 2.4.

Table 13 Resolved Caveats in Cisco CP 2.4

Bug ID	Summary
CSCth57014	Data between Ports and intf and conn are not synced.
CSCth61991	Need to handle required sub system ID not found error.
CSCth89641	2811,3945 and 2801,1861 do have security and voice license respective.
CSCth90262	MAC Address not listing all dynamic MAC address.
CSCth90328	Trunk configuration fails when encapsulation is negotiated.
CSCth92960	SGBU EtherChannel and 802.1x external link are not correct in online help.

Open Caveats

Table 14 lists caveats that are open in Cisco CP 2.4.

Table 14 Open Caveats in Cisco CP 2.4

Bug ID	Summary	Additional Information

CSCtf87466	SIP on in to self and vice versa leads to unreachable router.	**Symptom** Attaching or removing the management interface (in which CCP is invoked) from the zone-member security of firewall leads to an unreachable router.
		
		Conditions Firewall configurations delivered has the configuration that tries to attach or remove the management interface (for example, Gi0/0, the interface from which CCP is invoked) from the zone-security. IOS tries to reset the communication session, which in return makes the router unreachable and communication is lost.
		`interface GigabitEthernet0/0`
		` zone-member security in`
		` exit`
		
		or
		`interface GigabitEthernet0/0`
		` no zone-member security in`
		` exit`
		
		Workaround Rediscovering the router from Cisco CP might work if the device is reachable.
		• If the device is not reachable after the discovery, the router is blocked by the firewall through the interface IP address.
		• If the router becomes unreachable, the user should remove the firewall-related configurations under the management interface (through which Cisco CP is invoked) through CLI. This will make the router reachable.

CSCtg55407	Refresh button is missing in some instances of module configuration.	**Symptom** Refresh button is missing in the **Interface Management > Module configuration** page. **Conditions** Refresh button is missing in the **Interface Management > Module configuration** page. **Workaround** Clear the IE cache. • Go to **Control Panel > Java**. • In the **General** tab, under temporary settings, click **Settings** and delete temporary files present on your PC.

Table 14 Open Caveats in Cisco CP 2.4 (continued)

Bug ID	Summary	Additional Information
CSCtg84311	Inconsistent Module status shown on repeated refresh.	**Symptom** Inconsistent module status shown for a module in doing repeated refresh in the **Module Configuration** screen. **Conditions** It is an intermittent issue seen on refreshing the module from the **Module Configuration** screen. **Workaround** Rediscover the device using the **Community Member** screen.
CSCth64048	CUBE incorrectly discovered as CME.	**Symptom** Cisco CP may discover CUBE as Call Manager Express (CME). **Conditions** This occurs with telephony-service configuration in CUBE. **Workaround** There is no workaround.
CSCth67558	Unable to discover Switching Module.	**Symptom** Cisco CP fails to discover the 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, the user needs 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 will not be required to session into the module.
CSCtj03097	No Backup/Restore with LEFS flash type.	**Symptom** On using LEFS type Flash, the Backup/Restore functionality does not work for Config editor. A back up of the running config is not created on the Flash and hence restoring to initial config after merge or replace fails. **Conditions** There is no condition. **Workaround** Create a copy of the running config on the Flash manually and reload the router with that copy. CLI: **copy running-config flash** RunningConfig to Restore to this running config: CLI: **copy flash:RunningConfig startup-config** CLI: **Reload**

Table 14 Open Caveats in Cisco CP 2.4 (continued)

Bug ID	Summary	Additional Information
CSCth34158	Switching Modules folder is not listed in the left navigation pane.	**Symptom** Switching Modules folder will not get listed in the left navigation pane even when the device has supported switch modules that are managed by Cisco CP. **Conditions** The user can observe this in the following situations: • 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** The following are the workarounds: • Make sure 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 "line con 0". • If AAA is configured on the router, make sure that no authentication is required for the switch module and Privilege level 15 should be configured under "line con 0".
CSCtj46313	Sub-Interface not listed on the Configure Cellular Wan wizard.	**Symptom** The Sub-interfaces, for example, interface Serial 0/0/0.1 with encapsulation, is not listed under the Configure Cellular WAN Wizard on Cisco Configuration Professional. **Conditions** The problem is seen only with the Sub-Interfaces. All other interface types are listed correctly in the Configure Cellular WAN Wizard. **Workaround** There is no workaround.

Table 14 Open Caveats in Cisco CP 2.4 (continued)

Bug ID	Summary	Additional Information
CSCtj84620	CCP shows the IPSEC tunnel status instead of DMVPN tunnel status.	**Symptom** IPSEC tunnel status is shown when user clicks on DMVPN tunnel. **Conditions** CCP shows the IPSEC tunnel status when clicked on the DMVPN tunnel for the first time. **Workaround** To see the DMVPN tunnel status, click on the DMVPN tunnel node in the right pane tree.
CSCtk07275	Refresh adds more menus in left navigation pane.	**Symptom** Inappropriate Left navigation links show up if F5 is pressed when Cisco Configuration Professional window is active. Some of the new links that show up will not be valid for the current selected device. **Conditions** Press F5 button when the Cisco Configuration Professional screen is active. **Workaround** There is no workaround.

Related Documentation

Table 15 describes the related documentation available for Cisco CP.

Table 15 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

Table 15 Cisco Configuration Professional Documentation (continued)

Document Title	Available Formats
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

MQC—Modular QoS Command

PCEX—PC Express

SID—System Identification Number

NID—Network Identification Number

ESN—Electronic Serial Numbers

PDP—Packet Data Protocol (PDP)

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

REP—Resilient Ethernet Protocol

STP—Spanning Tree Protocol

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