Release Notes for Cisco Configuration Professional 2.1

March 3, 2010

These release notes support Cisco Configuration Professional (Cisco CP) version 2.1. 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, click **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 Cisco access routers. Cisco CP simplifies router, firewall, IPS, VPN, unified communications, WAN, and basic LAN configuration 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 Configuration Professional Express (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 and minimal IOS security features.

System Requirements

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

- PC System Requirements
- Router System Requirements
- Cisco CP Ordering Options

PC System Requirements

Table 1 lists the system requirements for a PC running Cisco CP. Although the Cisco CP application requires 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 also JRE.

Table 1 PC System Requirements

System Component	Requirement
Processor	2 GHz processor or faster
Random Access Memory	1 GB
Hard disk available memory	400 MB
Operating System	Any of the following: • Microsoft Windows 7 - 64 and 32 bit • Microsoft Windows Vista Business Edition • Microsoft Windows Vista Ultimate Edition • Microsoft Windows XP with Service Pack 2 or later • 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 minimum 1.5.0_11 upto 1.6.0_17 are supported.
Adobe Flash Player	Version 10.0 or later, with Debug set to No
Secure Shell (SSH)	Required for secure connections with the router. Versions up to 2.0 are supported.

Router System Requirements

Router System Requirements are described in the following parts:

- Supported Routers
- Supported Phones
- Supported Network Modules
- Supported Interface Cards
- Supported Adapters, Processing Engines, and Service Engines
- Cisco IOS Releases
- Required IP Address Configuration Information
- Router Configuration Requirements

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	Cisco 7000 Series
CISCO815	CISCO1801	Cisco 2801	Cisco 3825	Cisco 7204VXR
CISCO815-VPN-K9	CISCO1801-M	Cisco 2811	Cisco 3825-NOVPN	Cisco 7206VXR
	CISCO1801/K9	Cisco 2821	Cisco 3845	Cisco 7301
	CISCO1801-M/K9	Cisco 2851	Cisco 3845-NOVPN	
	CISCO1801WM-AGE/K9			
	CISCO1801W-AG-E/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	Cisco 7000 Series
CISCO871-K9 CISCO871-SEC-K9 CISCO871W-G-A-K9 CISCO871W-G-E-K9 CISCO871W-G-J-K9	CISCO1805-D CISCO 1805-D/K9			
	CISCO1811/K9 CISCO1811W-AG-B/K9 CISCO1811W-AG-C/K9 CISCO1811W-AG-N/K9			
CISCO876-K9 CISCO876-SEC-K9 CISCO876-SEC-I-K9 CISCO876W-G-E-K9	CISCO1812/K9 CISCO1812 W-AG-E/K9 CISCO1812 W-AG-C/K9			
CISCO877-K9 CISCO877-M-K9 CISCO877-SEC-K9 CISCO877W-G-A-K9 CISCO877W-G-E-K9 CISCO877W-G-E-M-K9	CISCO1841			
CISCO878-K9 CISCO878-SEC-K9 CISCO878W-G-A-K9 CISCO878W-G-E-K9	C1861-UC-4FXO-K9 C1861-UC-2BRI-K9 C1861-SRST-B/K9 C1861-SRST-C-B/K9 C1861-SRST-C-F/K9 C1861-SRST-F/K9			
	C1861W-SRST-C-B/K9 C1861W-SRST-C-F/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 CISCO861W-GN-A-K9 CISCO861W-GN-E-K9 CISCO861W-GN-P-K9	CISCO1941/K9 CISCO1941W-A/K9 CISCO1941W-E/K9 CISCO1941W-P/K9 CISCO1941W-N/K9	CISCO2901/K9 CISCO2911/K9 CISCO2921/K9 CISCO2951/K9	CISCO3925/K9 CISCO3945/K9
CISCO867-W-GN-A-K9 CISCO867-W-GN-E-K9			CISCO3925[1] CISCO3945[1]
CISCO881-K9 CISCO881W-GN-A-K9 CISCO881W-GN-E-K9 CISCO881W-GN-P-K9 CISCO881G-K9 CISCO881GW-GN-A-K9 CISCO881GW-GN-E-K9 CISCO881G-S-K9 CISCO881G-V-K9 CISCO881G-A-K9 CISCO881SRST-K9 CISCO881SRSTW-GN-A-K9 CISCO881SRSTW-GN-E-K9			
CISCO886-K9 CISCO886W-GN-E-K9 CISCO886G-K9 CISCO886GW-GN-E-K9			
CISCO887-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			

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

Cisco 800 Series	Cisco 1900 Series	Cisco 2900 Series	Cisco 3900 Series
887V (VDSL2oPOTS) 3G, WLAN: CISCO887VG-K9 CISCO887VGW-GNA-K9 CISCO887VW-GNA-K9 CISCO887VW-GNE-K9			
887V (VDSL2oPOTS) SRST: C887VSRST-K9 C887VSRSTW-GNA-K9 C887VSRSTW-GNE-K9			
CISCO888-K9 CISCO888W-GN-A-K9 CISCO888W-GN-E-K9 CISCO888G-K9 CISCO888GW-G-AN-K9 CISCO888GW-G-EN-K9			
CISCO888SRST-K9 CISCO888SRSTW-GN-A-K9 CISCO888SRSTW-GN-E-K9			
CISCO891-K9 CISCO891W-AGN-A-K9 CISCO891W-AGN-N-K9			
CISCO892-K9 CISCO892W-AGN-E-K9			

[1] The chassis remains the same as for ISR-G2. The only difference is based on the motherboard chosen.

Supported Phones

Table 4 lists the phones that Cisco CP supports:

Table 4 ***Supported Phones***

Supported Phones	Supported Expansion Modules	Supported Conference Stations
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 – expansion module compatible (7914)		
7961G – expansion module compatible (7914)		
7961G-GE		
7962G – expansion module compatible (7915,7916)		
7965G – expansion module compatible (7915,7916)		
7970G – expansion module compatible (7914)		
7971G – expansion module compatible (7914)		
7975G – expansion module compatible (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			AIM2-CUE-K9	EM-HDA-8FXS
NM-16ESW-1GIG				EM-HDA-4FXO
NM-16ESW-PWR				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	HWIC-1T	VIC2-4FXO
WIC-2T	HWIC-2T	VIC2-2FXS
WIC-2A/S (Frame Relay, PPP, HDLC, no asynchronous)	HWIC-4T	VIC2-2FXO
	HWIC-2A/S	VIC2-2BRI-NT/TE
WIC-1ADSL	HWIC-4A/S	VIC-2DID
WIC-1DSU-T1-V2	HWIC-4ESW	VIC-4FXS/DID
WIC-1B-S/T-V3	HWIC-4ESW-POE	VIC3-4FXS/DID
WIC-1AM	HWIC-8A	VIC3-2FXS/DID
WIC-2AM	HWIC-8A/S-232	VWIC2-1MFT-T1/E
WIC-4ESW	HWIC-D-9ESW	VWIC2-2MFT-T1/E1
WIC-1SHDSL-V2	HWIC-D-9ESW-POE	
WIC-1SHDSL-V3	HWIC-1DSU-T1	
WIC 1ADSL-DG	HWIC-16A	
WIC 1ADSL-I-DG	HWIC-ADSL-B/ST	
	HWIC-ADSLI-B/ST	
	HWIC-1ADSL	
	HWIC-1ADSLI	
	HWIC-1ADSL-M (WIC card with Annex M)	
	HWIC-2SHDSL	
	HWIC-4SHDSL	
	HWIC1-ADSL-M	
	HWIC-1CABLE-D-2	
	HWIC-1CABLE-E/J-2	
	HWIC-1FE	
	HWIC-2FE	
	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-3G-GSM	
	HWIC-3G-CDMA-S	
	HWIC-3G-CDMA-V	

Supported Adapters, Processing Engines, and Service Engines

Table 8 lists the adapters, processing engines, and service engines that Cisco CP supports.

Table 8 Supported Adapters, Processing Engines, and Service Engines

Port Adapters on Cisco 7000 Series Routers	Service Adapters on Cisco 7000 Series Routers	Network Processing Engines and Network Service Engines on Cisco 7000 Series Routers
PA-2FE-TX	SA-VAM	NPE-225
PA-2FE-FX	SA-VAM2	NPE-400
PA-8E	SA-VAM2+	NPE-G1
PA-4E	C7200-VSA	NPE-G2
		NSE-1

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	Earliest 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

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

Router Model	Earliest Cisco CP-Supported Cisco IOS Versions
Cisco 2900 series	• 15.0(1)M
Cisco 3800 series	• 12.4(9)T
Cisco 3900 series	• 15.0(1)M
Cisco 7000	• 12.4(9)T

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 Internetwork Operating System Software
IOS (tm) C1700 Software (c1700-k8sv3y7-mz) Version 12.2(13)ZH
```

Required IP Address Configuration Information

Table 10 provides the required IP address configuration for the PC. Use this information to complete the section “Task 4: Configure the IP Address On the PC” in the *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	Obtain an 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

In order 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 on page 14 describes the ordering options under which Cisco CP can be ordered. Cisco Configuration Professional Express (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

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
- New Hardware Support

New and Changed Features

Cisco CP 2.1 supports the following new features:

- Wireless Support—It is possible to launch the Wireless GUI in Cisco CP. In Cisco CP 2.1, you can also configure the Wireless feature in Cisco CP itself. You can configure Fixed Wireless Platforms and WLAN Access Point Module in the Wizard and Edit modes.
- Environment Information—The ISR-G2 routers display hardware environment information. In Cisco CP 2.1, it is possible to monitor the following, for ISR-G2 routers, at set intervals:
  - Power Supply
  - Fan Status
  - Module/Router Power Consumption
  - Temperature

The following features were updated for Cisco CP 2.1:

- Licensing—Earlier, only CUE image licensing was supported. In Cisco CP 2.1, CUE module licensing is also supported.
- 3G Wireless HWIC—The 3G Wireless HWIC has an embedded modem from Sierra Wireless (MC8775). In Cisco CP 2.1, you can upgrade the firmware for the modem using Cisco IOS commands. The firmware is packaged in a tar distribution file and can be downloaded from the wireless software download page on Cisco.com.

  Cisco CP allows you to upgrade the modem firmware by:
  - Downloading the appropriate firmware release under Wireless Integrated Switches and Routers to PC hard disk.
  - Uploading the firmware distribution into the router flash.
  - Clicking on FW upgrade button to start the upgrade process.
- Voice Security Audit—The Voice Security Audit feature adds voice audit to the existing security audit feature. In Cisco CP 2.1, the CUE restriction table is used to prevent toll fraud and malicious use of the CUE system to make outbound calls. Wildcard patterns are specified in this table to match the outgoing calls. Applications (voice mail features) that use the CUE restriction table are:
  - Fax
  - CUE Live Reply
  - Message Notification
  - Non-Subscriber Message Delivery

  Cisco CP checks if the above mentioned voice mail features are active in CUE. If any of the applications do not have an associated restriction table, then the audit fails. Those applications are then listed in the “Apply fix” section for CUE Restriction table. The “fix” operation obtains patterns from the user and configures them on the applications.
- Left Navigation Pane Changes - All device specific features are now in the left navigation pane. Only non-device specific system wide features are on the menu bar.

New Hardware Support

The new devices supported are:

- CISCO1941/K9
- CISCO1941W-A/K9
- CISCO1941W-E/K9
- CISCO1941W-P/K9
- CISCO1941W-N/K9
- CISCO2901/K9
- CISCO2911/K9
- CISCO2921/K9
- CISCO2951/K9
- CISCO3925/K9
- CISCO3945/K9

The new network modules supported are:

- SM-ES2-16-P
- 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
- SM-D-ES3G-48-P
- SM-SRE-700-k9
- SM-SRE-900-k9
- ISM-SRE-300-K9
- AIM2-CUE-K9
- EM3-HDA-8FXS/DID

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
- Restrictions for Cisco 7204VXR, Cisco 7206VXR, and Cisco 7301 Routers
- Cisco CP and Internet Explorer 8

Cisco CP Minimum Screen Resolution

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

Restrictions for Cisco 7204VXR, Cisco 7206VXR, and Cisco 7301 Routers

The following restrictions apply to Cisco CP running on Cisco 7204VXR, Cisco 7206VXR, and Cisco 7301 Routers:

- The Cisco CP Express application is not supported. You must use the Cisco IOS CLI to give the router an initial configuration that will enable you to connect to the router using a browser.
- WAN configuration is not supported. Cisco CP supports configuration of Ethernet and Fast Ethernet interfaces.
- The Cisco CP Reset feature is not available.
- No default configuration file is supplied. To run Cisco CP, you must provide a configuration that includes the commands necessary to support operation of Cisco CP.

Cisco CP and Internet Explorer 8

In some systems (Windows XP and Windows Vista), with IE8 installed, Cisco CP may not work as expected. This is due to a reported IE 8 caching issue.

IE8 reinstall or clearing the cache does not help. Any Flash based application like Cisco CP will see this issue.

A workaround today is to create another user account with appropriate privileges and run Cisco CP in that user account.

A fix will be made available in Cisco CP 2.1.

Important Notes

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

- Cisco IOS Enforces One-Time Use of Default Credentials
- Cisco CP Merge and Replace Configuration Functions Fail Under Some Conditions
- Cisco CP Security Dashboard May Display Threats Unrelated to Your Cisco IOS IPS Installation
- Cisco CP May Lose Connection to Network Access Device
- Popup Blockers Disable Cisco CP Online Help
- Disable Proxy Settings
- Security Alert Dialog May Remain After Cisco CP Launches
- Screencasts for Cisco CP Features

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, and Cisco 3800 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 “cisco” and password “cisco” before you log off of the router. If you do not change the credentials as directed, you will not be able to log on to 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
- 12.3(21), 12.3(22)

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 login to 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 light blue console cable, included with your router, from the blue console port on your router to a serial port on your PC. 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.

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 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 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 which 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 which does not have a redirect URL configured in it.

For more information, see the links in 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. In order 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.

Disable Proxy Settings

Cisco CP will not start when run under Internet Explorer with proxy settings enabled. To correct this problem, choose **Internet Options** from the Tools menu, click the **Connections** tab, and then click the **LAN settings** button. In the LAN Settings window, disable the proxy settings.

Security Alert Dialog May Remain After Cisco CP Launches

When Cisco CP is launched using HTTPS, a security alert dialog box that informs you of possible security problems and asks you if you want to proceed with program launch may appear. This can happen if the router does not have the following global configuration command in the running configuration:

```
ip http timeout-policy idle 600 life 86400 requests 10000
```

Screencasts for Cisco CP Features

Instead of online help, we have provided screencasts for the following Cisco CP 2.1 features:

- Wireless Support
- Environment Information

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.

Cisco Configuration Professional Is Already Running Message

If Cisco CP has not been shut down properly, and you try to relaunch it, you may see the following message: "Cisco Configuration Professional is already running. Only one occurrence can run at a time." To correct this problem and relaunch Cisco CP, do the following:

Step 1 Press **Ctrl Alt Delete**, and click **Task Manager**.

Step 2 In the Windows Task Manager dialog, click **Processes**.

Step 3 In the Image Name column, highlight the processes **CiscoCP.exe, CiscoCPEngine.exe, IEC2.exe**, and **SplashScreen.exe**.

Step 4 Click **End Process**.

Step 5 Wait 30 seconds, and then restart Cisco CP.

Technical Support Logs Do Not Appear on Desktop

If the technical support logs folder does not appear on the desktop, there may be installed Java applications preventing this feature from working properly. To check, go to **Start** > **Control Panel** > **Add or Remove Programs**, and scan the list for Java applications. Remove the Java applications that you can, and try again.

Discovery Never Completes

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

Step 3 In the Temporary Internet Files box, click **Delete Files**.

Step 4 In the displayed dialog, leave all file types checked, and click **OK**.

Step 5 Click **OK** in the Java control panel to close it.

Step 6 Restart Cisco CP.

Caveats

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

- Resolved Caveats from Cisco CP 2.0
- Open Caveats—Cisco CP 2.1

Resolved Caveats from Cisco CP 2.0

Table 13 lists caveats that are resolved in Cisco CP 2.1.

Table 13 Resolved Caveats in Cisco CP 2.1

Bug ID	Summary
CSCsm91019	Security screens overlap over menu bar options and tool bar information.
CSCsw23556	`Security Applet is not responding` error during discovery.
CSCsx05868	Unable to upload CME phone load tar file.
CSCtc30671	Issues with network object ACL groups.
CSCta71627	Dialer list configuration removed after GSM wizard configuration.
CSCtb43408	Dialer persistent config conflicts with Do Not Configure Now in wizard.
CSCtb05983	Multiple delete fails in offline mode community dashboard.
CSCsz13759	Deleting of extensions fails if configured as Monitor/Shared.
CSCsy87964	CPU utilization at 100% when discovering devices.
CSCsx72139	Cisco CP discover details should give warning in case of insufficient memory.
CSCsx57080	Cisco CP launching issue with Internet Explorer 8.
CSCsw31280	CLI Preview dialog box moves to the background.

Open Caveats—Cisco CP 2.1

Table 14 lists caveats that are open in Cisco CP 2.1.

Table 14 Open Caveats in Cisco CP 2.1

Bug ID	Summary	Additional Information
CSCte49659	Replace Running Configuration does not work for devices with access point.	**Symptom**: Replace Running Configuration does not work in a router with access point module, using Cisco CP. **Conditions**: Router with access point module. In Config Editor, Replace Running Configuration does not work when the modified running configuration file is imported from the PC. **Workaround**: There is no workaround.
CSCsz78794	SDM related screens not aligned properly.	**Symptom**: All Cisco Configuration Professional Security/Routing/Utility screens may not be aligned properly if the Internet Explorer zoom level is set to anything other than 100%. **Workaround**: Set the Internet Explorer zoom level to 100% and restart Cisco Configuration Professional to view and use the Routing/Security/Utility screens properly.
CSCtd99143	**match-all** command not supported in IOS version 15.0.	**Symptom**: Command delivery fails on configuring Application Inspection using Advanced Security. **Conditions**: On configuring layer 7 classmap with match all attribute, command delivery fails. **Workaround:** There is no workaround.
CSCtd90671	VS module init failed when NTP server is unreachable.	**Symptom**: VMSS module post install is not completed by Cisco Configuration Professional when the NTP server status on the IOS is unreachable. **Conditions**: The VMSS module is in post install prompt and the NTP status on the IOS is unreachable. **Workaround**: Configure the NTP master configuration on the IOS. This makes the NTP server reachable. Now the post install will goes through fine.
CSCtc51162	IEC2 MFC application crashed while launching Cisco CP.	**Symptom**: Cisco CP fails to launch with an IEC2 MFC application crash error message. **Conditions:** When trying to launch Cisco CP from the start menu. **Workaround**: Restart the machine and try to launch Cisco CP.

Table 14 Open Caveats in Cisco CP 2.1 (continued)

Bug ID	Summary	Additional Information
CSCtb59307	SNR with the same/leading digits as that of the extension number.	**Symptom**: While configuring SNR to a dn, if the SNR number and the dn tag is the same, CME displays “Can't configure SNR with same dn number” error message **Conditions**: The error thrown from CME, if primary extension and SNR number are configured with the same leading digits. **Workaround**: There is no workaround.
CSCtb80991	EtherSwitch Service Module is not supported on the Template feature.	**Symptom:** The Template feature does not support EtherSwitch Service Modules but the Create Template wizard displays the EtherSwitch Service Module configuration. Also, the Apply Template wizard should not modify or apply the EtherSwitch Service Module configuration, but it does. **Conditions:** The Create Template wizard is used to create a template from the router with EtherSwitch Service Module or Modules. The Apply Template wizard is used to apply the template to the router with the EtherSwitch Service Module or Service Modules. **Workaround**: There is no workaround.
CSCtb33162	Only the last chat script is removed when multiple chat script is configured.	**Symptom**: Only the last chat script gets removed after clicking the delete button for the specified interface. **Conditions**: Configure multiple chat script under Dialer tab in edit mode. **Workaround:** There is no workaround.
CSCsx75097	Cisco Unity Express module discovery fails with SSH version greater than or equal to 2.0.	**Symptom:** Cisco Unity express module discovery fails with an error message stating that the device is configured with unsupported SSH version. The error messages are shown in the discovery details UI. Due to this error message, none of the CUE features are available. **Conditions**: The device is configured with SSH version greater than or equal to 2.0. **Workaround**: Reconfigure the SSH version to lesser than 2.0, or use the non-secure mode to communicate with the device.
CSCsm95507	The Cisco CP icon is changed to IE icon after a while in the titlebar.	**Symptom:** The icon of Cisco CP application window changes to IE icon. **Conditions**: After the successful launch of Cisco CP, minimize the Cisco CP screen. **Workaround**: There is no workaround.

Table 14 Open Caveats in Cisco CP 2.1 (continued)

Bug ID	Summary	Additional Information
CSCsz13428	Configuration error on creating or editing dial plan.	**Symptom**: Dial plan related configuration fails saying dial-peer tag is already in use. This issue may happen when **voice hunt-group** is configured on the router. **Conditions:** When **voice hunt-group** is configured with pilot CLI, and the pilot number is too huge to be dial-peer tag. **Further Problem Description:** When **voice hunt-group** is configured with pilot CLI, the router creates a dial-peer with pilot number as a dial-peer tag. This dial-peer is not displayed in **show run**, and Cisco CP does not read these dial-peers (only **show run** is used to read in dial-peer configurations). However, these dial-peers can be seen in **show dial-peer voice summary**. In normal circumstances, the pilot number is a large number, and so is the dial-peer tag. So this is not an issue for Cisco CP as Cisco CP always chooses the smallest tag number available to configure dial-peers and there is never any overlap of tags. However, if pilot number is too large to be a tag for dial-peer, the router chooses the next available smallest tag number to configure dial-peer for that hunt group. In that case, Cisco CP configuration for dial plan causes an issue as chosen tag by Cisco CP might overlap with an already configured hunt group related dial-peer. This causes configuration failure.
CSCsw39659	Enhancement in Cisco CP for CUE post initialization.	**Symptom**: The data fields for Post Initialization wizard are not retained on Cisco CP, if the user reverts using back button, in the case of any of the fields leading to an error. It is an overhead to enter all the values again. **Conditions**: This issue occurs only when any field value is invalid in the post initialization wizard. **Workaround:** Filling in all correct values at one go will prevent this issue.
CSCta77317	Analog Trunk window not closing on clicking the OK button.	**Symptom: Configure** > **Voice** > **PSTN Trunks** > **Analog Trunks**, **Edit** screen does not close upon clicking the OK button without making any change. **Conditions:** Go to **Configure** > **Voice** > **PSTN Trunks** > **Analog Trunks** screen. Select an entry and choose the Edit button. Without making any change, click on the OK button. The dialog box does not close. **Workaround**: Click on the Cancel button.

Table 14 Open Caveats in Cisco CP 2.1 (continued)

Bug ID	Summary	Additional Information
CSCta77454	Adhoc Conf update with ssh port blocked throws unwarranted error.	**Symptom:** Although discovery is successful with SSH port blocked, updates on Adhoc Conference fail as interactive commands use SSH protocol.The error message does not indicate that the SSH port is blocked. **Conditions**: Modification of Adhoc Conference parameters fail with SSH port blocked and the error message does not indicate the cause. **Workaround**: Unblock the SSH port for any transport or communication errors on Adhoc Conference. **Further Problem Description:** The discovery process on Cisco CP is successful with SSH port blocked but features like Adhoc Conference use DSPs which are interacted with using SSH ports.When the SSH port is blocked all such interactions fail and hence updates on Adhoc Conference profile are not successful. The error message generated does not communicate the solution.
CSCta31020	Whisper intercom does not throw error while editing invalid entry.	**Symptom**: No error message while editing Invalid Whisper Intercom entry. **Conditions:** Whisper intercom dashboard should have invalid entry. Invalid entry should be created via CLI. **Workaround:** There is no workaround.
CSCta60741	Unable to add inspect rule to self zone when editing ZBF.	**Symptom**: Inspect rule is not being configured correctly for the SSL VPN passthrough. **Conditions**: Configure ZBF and then configure SSL VPN. The inspect rule is not configured correctly. This is due to an IOS bug. **Workaround**: There is no workaround.
CSCtb58966	Reload of router unsuccessful after deploying license.	**Symptom**: Reload of device unsuccessful after deploying license or when using reload router button from License Management > Dashboard window. **Conditions:** This is seen with devices with an AP module that requires an input to the following interactive command: **cisco881GW#reload** **Do you want to reload the internal AP? [yes/no]:** **Workaround**: Manually reload the router for the license deployment to take effect and re-discover the router.

Table 14 Open Caveats in Cisco CP 2.1 (continued)

Bug ID	Summary	Additional Information
CSCtb81205	Location to download SDM IPS packages needs to be changed.	**Symptom:** Latest SDM/CP packages for IPS cannot be auto downloaded using Cisco CP. **Conditions:** If the user clicks Download option from IPS, the latest SDM/CP package is not downloaded. Only the IOS-CLI package is downloaded. **Workaround:** Manually download the package from CCO and use it in Cisco CP for configuration or import options.
CSCsy49785	Service group not working for QoS, SSL VPN, NAC, and access-class.	**Symptom**: OGACL with service group not working for QoS, SSL VPN, NAC, and access-class. **Conditions**: When associating an OGACL with service object group to QoS, SSL VPN, NAC, and access-class, the traffic is not matched. This is due to an IOS issue. **Workaround**: There is no workaround. Use normal ACLs with these features.
CSCsm95507	Cisco CP icon is changed to Internet Explorer icon after a while in the titlebar.	**Symptom**: The icon of Cisco CP application window changes to Internet Explorer icon. **Conditions**: After the successful launch of Cisco CP, minimize the Cisco CP screen and keep it minimized for a while. **Workaround**: There is no workaround.
CSCsw39659	Enhancement in Cisco CP for CUE post initialization.	**Symptom**: The data fields for CUE post initialization wizard are not retained on Cisco CP if you use the back button. It is time consuming to enter all the values again. **Conditions**: This issue occurs only when any field value is invalid in the CUE post initialization wizard. **Workaround**: To avoid this situation, make sure that you enter the correct values so that you do not have to use the back button.
CSCsx75097	Unity express module discovery fails with SSH version >=2.0.	**Symptom**: Cisco Unity Express module discovery fails with an error message stating that the device is configured with unsupported SSH version. The error messages are shown in the discovery details user interface. Due to this error message, none of the CUE features are available. **Conditions**: The device is configured with SSH version higher than or equal to 2.0. **Workaround**: Reconfigure the SSH version to lesser than 2.0, or use Telnet to communicate with the device.

Table 14 Open Caveats in Cisco CP 2.1 (continued)

Bug ID	Summary	Additional Information
CSCsy49785	Service group not working for QoS, SSLVPN, NAC, and access-class.	**Symptom**: OGACL with service group not working for QoS, SSLVPN, NAC, and access-class. **Conditions**: When associating an OGACL with service object group to QoS, SSL VPN, NAC, and access-class, the traffic does not match. This is due to an IOS issue. **Workaround**: There is no specific workaround. Use normal ACLs with these features. Once the IOS bug is fixed, this will be fixed in Cisco CP.
CSCsz13428	Configuration error on creating or editing outgoing dial-plan.	**Symptom**: Dial-plan related configuration fails saying dial-peer tag is already in use. This issue occurs occasionally when voice hunt-group is configured on the router. **Conditions**: When hunt-group is configured with pilot CLI, and the pilot number is too huge to be the dial-peer tag. **Further Problem Description**: When hunt-group is configured with pilot CLI, the router creates a dial-peer with the pilot number as the dial-peer tag. This dial-peer is not displayed in **show run**, and Cisco CP does not read these dial-peers (only **show run** is used to read in dial-peer configurations). However, these dial-peers can be seen in **show dial-peer voice summar**y. In normal circumstances, the pilot number and the dial-peer tag are large numbers. This is not an issue for Cisco CP as Cisco CP always chooses the smallest tag number available to configure dial-peers and there is never any overlap of tags. However, if the pilot number is too large to be a tag for dial-peer, the router chooses the next available smallest tag number to configure the dial-peer for that hunt group. In such a situation, Cisco CP configuration for dial-plan might cause a problem because the tag that Cisco CP chooses, can overlap with the already configured hunt group related dial-peer, which results in configuration failure.
CSCta31020	Whisper intercom does not throw error while editing an invalid entry.	**Symptom**: No error message while editing invalid Whisper Intercom entry. **Conditions**: Whisper intercom dashboard should have invalid entry. Invalid entry should be created via the CLI. **Workaround**: There is no workaround.
CSCta60741	Unable to add inspect rule to self zone when editing ZBF.	**Symptom:** Inspect rule does not get configured correctly for the SSL VPN Passthrough. **Conditions: C**onfigure ZBF and then configure SSL VPN. The inspect rule does not get configured correctly. This is due to an IOS bug. **Workaround:** There is no workaround.

Table 14 Open Caveats in Cisco CP 2.1 (continued)

Bug ID	Summary	Additional Information
CSCta77317	Analog Trunk window not closing on clicking the **OK** button.	**Symptom**: Go to **Configure** > **Voice** > **PSTN Trunks** > **Analog Trunks**. The Edit screen does not close when the **OK** button is clicked without making any changes. **Conditions**: Go to **Configure** > **Voice** > **PSTN Trunks** > **Analog Trunks** screen. Select an entry, and then click **Edit**. Without making any changes, click **OK**. The dialog box does not close. **Workaround**: Click **Cancel** button.
CSCta77454	Adhoc Conference update with SSH port blocked throws unwarranted error.	**Symptom**: Although Discovery is successful with SSH port blocked, updates on Adhoc Conference fail as interactive commands use SSH protocol. The error message does not indicate that the SSH port is blocked. **Conditions**: Modification of Adhoc Conference parameters fail with SSH port blocked and the error message does not indicate the cause. **Workaround**: Unblock the SSH port for any transport/communication errors on Adhoc Conference. **Further Problem Description**: The Discovery process on Cisco CP is successful with SSH port blocked but features like Adhoc Conference use DSPs which interact using SSH ports. When the SSH port is blocked, all such interactions fail and hence updates on Adhoc Conference profile are not successful.The error message generated does not communicate the cause.
CSCtb81205	Location to download SDM IPS packages needs to be changed.	**Symptom**: Latest SDM/CP packages for IPS cannot be auto downloaded using Cisco CP. **Conditions**: If the user clicks “Download” option from IPS, the latest SDM/CP package will not be downloaded. Only the IOS-CLI package will be downloaded. **Workaround**: Manually download the package from CCO and use it in Cisco CP for configuration or import options.
CSCtb58966	Reload of router unsuccessful after deploying license.	**Symptom:** Reload of device unsuccessful after deploying license or when using 'Reload router' button from License Management > Dashboard window. **Conditions:** This is seen with devices with an AP module that requires an input to the following interactive command. **cisco881GW#reload** **Do you want to reload the internal AP? [yes/no]:** **Workaround**: Manually reload the router for the license deployment to take effect and re-discover the router.

Table 14 Open Caveats in Cisco CP 2.1 (continued)

Bug ID	Summary	Additional Information
CSCtb33162	Only the last chat script is removed when multiple chat is configured.	**Symptom**: Only the last chat script gets removed upon clicking the delete button for the specified interface. **Conditions**: Configure multiple chat script under Dialer tab in edit mode. **Workaround**: There is no workaround.

CSCtf18476	Cannot launch Cisco CP on a PC that is running the Windows operation system.	**Symptom**: Cisco CP version 2.1fails to launch on a PC that is running the Windows operating system. The following error message appears:
		`org.hibernate.exception.GenericJDBCException: Cannot open connection`
		Conditions: This problem might occur on PCs that have permission restrictions, which do not allow you to edit the files that are located at the default install location, C:\Program Files. This problem might occur on any of the Windows operating system versions (Windows 7, Windows XP, or Windows Vista), or when Cisco CP is installed on Windows on VMWare.
		Note This problem occurs intermittently and is not a general issue on all PCs.
		Workaround: To resolve this problem, you must modify the **hibernate.properties** file. Do the following:
		1. Go to C:/Program Files/Cisco Systems/CiscoCP/webapps/ROOT/WEB-INF/classes/hibernate.properties
		2. Open the **hibernate.properties** file in Notepad, and then search for the following statement:
		`hibernate.connection.url = jdbc:derby:${CP_ROOT_DIR}/cpdb`
		3. Replace the statement with the following:
		`hibernate.connection.url = jdbc:derby:C:/Program Files/Cisco Systems/CiscoCP/webapps/ROOT/WEB-INF/cpdb`
		4. Relaunch Cisco CP.
		Note This problem will be fixed in Cisco CP 2.2, which is scheduled to release in April 2010.

Related Documentation

Table 14 describes the related documentation available for Cisco Configuration Professional.

Table 15 Cisco Configuration Professional Documentation

Document Title	Available Formats
Readme First for Cisco Configuration Professional	This document is available in the following locations: • On Cisco.com. • On the product CD-ROM in the Documentation folder.
Cisco Configuration Professional Quick Start Guide	This guide is available in the following locations: • On Cisco.com. • On the product CD-ROM in the Documentation folder.
Cisco Configuration Professional Getting Started Guide	This guide is available in the following locations: • On Cisco.com. • On the product CD-ROM in the Documentation folder. • 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 in the following locations: • On Cisco.com. • Accessible from Online help.
Cisco Configuration Professional Express User Guide	This guide is available in the following locations: • On Cisco. com. • Accessible from Online help.
Release Notes for Cisco Configuration Professional	This document is available in the following location: • On Cisco.com.
Release Notes for Cisco Configuration Professional Express	This document is available in the following location: • On Cisco.com.

Note For information on obtaining documentation and technical assistance, product security, and additional information, see What's New, which also lists new and revised documents each month.

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