Release Notes for Cisco Configuration Professional 2.3

July 30, 2010

These release notes support Cisco Configuration Professional (Cisco CP) version 2.3. 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, Intrusion Prevention System, 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 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 Java Runtime Error (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 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

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
- Connected Grid
- 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
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 CISCO877W-G-A-K9 CISCO877W-G-E-K9 CISCO877W-G-E-M-K9	CISCO1841		
CISCO878-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 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 CISCO861W-GN-A-K9 CISCO861W-GN-E-K9 CISCO861W-GN-P-K9	CISCO1921	CISCO2901/K9 CISCO2911/K9 CISCO2921/K9 CISCO2951/K9	CISCO3925/K9 CISCO3925E/K9 CISCO3945/K9 CISCO3945E/K9
CISCO867-K9 CISCO867W-GN-A-K9 CISCO867W-GN-E-K9	CISCO1941/K9 CISCO1941W-A/K9 CISCO1941W-C/K9 CISCO1941W-E/K9 CISCO1941W-N/K9 CISCO1941W-P/K9		

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

Cisco 800 Series	Cisco 1900 Series	Cisco 2900 Series	Cisco 3900 Series
CISCO881-K9			
CISCO881W-GN-A-K9			
CISCO881W-GN-E-K9			
CISCO881W-GN-P-K9			
CISCO881G-G-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
CISCO887VG-K9 CISCO887VGW-GNA-K9 CISCO887VGW-GNE-K9 CISCO887VW-GNA-K9 CISCO887VW-GNE-K9			
CISCO887VSRST-K9 CISCO887VSRSTW-GNA-K9 CISCO887VSRSTW-GNE-K9			
CISCO888-K9 CISCO888W-GN-A-K9 CISCO888W-GN-E-K9 CISCO888G-K9 CISCO888GW-G-AN-K9 CISCO888GW-G-EN-K9			
CISCO888SRST-K9 CISCO888GW-G-NA-K9 CISCO888GW-G-NE-K9			
CISCO891-K9 CISCO891W-AGN-A-K9 CISCO891W-AGN-N-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 – 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	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	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	

Table 7 Supported Cards (continued)

(continued)WAN Interface Cards (WICs)	High-speed WAN Interface Cards (HWICs)	Voice Interface Cards
	HWIC-3G-HSPA HWIC-3G-HSPA-A HWIC-3G-HSPA-G PCEX-3G-HSPA-x	

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

Connected Grid

Table 9 lists the connected grid devices that Cisco CP supports

.

Table 9 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 10.

Table 10 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

Table 10 Cisco CP-Supported Routers and Cisco IOS Versions(continued)

Router Model	Minimum Cisco CP-Supported Cisco IOS Versions
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 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 11 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 11 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

To run Cisco CP, a router configuration must meet the requirements shown in Table 12.

Table 12 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 13 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 13 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 13 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
- New Hardware Support

New and Changed Features

Cisco CP 2.3 supports the following new features:

- 3G Feature Enhancements
  Earlier Cisco CP supported cellular modem activation, cellular interface configuration as primary and as backup, and firmware upgrade for both CDMA and GSM technologies. Cisco CP 2.3 supports the following:
  - OMA-DM activation on MC5727 modem for HWIC-3G-CDMA-S (Sprint).
  - SIM features on MC8790 and MC8792V modems for HWIC-3G-HSPA, HWIC-3G-HSPA-A, HWIC-3G-HSPA-G SKUs and AC501 Air card modem on 88x series.
- Advanced Telephony Settings
  The Advanced Telephony Settings feature allows you to configure and manage the following:
  - System information such as system message, directory naming schema, music on hold, and default pin
  - System and customer accounts
  - Timeouts
  - Dial plan pattern
  - Transfer pattern
  - Phone URLs
- Basic Automatic Call Distribution (B-ACD) Prompt and Script
  Cisco CP 2.3 supports B-ACD Prompt and Script. The B-ACD Prompt and Script feature enables you to perform the following operations with respect to a prompt and script:
  - Upload B-ACD tar package to flash
  - Upload Prompt and Script files to flash
  - Delete prompt(s) and script(s) from flash
  - Download prompt(s) and script(s) from flash
- Cisco Application Extension Platform (AXP)
  Cisco CP 2.3 supports Cisco AXP, which makes integration of branch network, applications, and IT infrastructure easier. Cisco CP 2.3 supports AXP module initial setup, which includes the following:
  - AXP modules software installation
  - Module parameter configuration such as DNS, NTP, domain name, time zone, syslog server, and administrator account
  - Installation/upgrade/uninstallation of third party applications on AXP
  - Subinterface configuration and binding of interfaces to applications
- Cisco Unified Border Element (CUBE)
  Cisco CP 2.3 supports CUBE. CUBE is an IP-to-IP gateway that facilitates connectivity between independent unified communications, VoIP, and video networks.
- Cisco Unified CME B-ACD
  Cisco CME B-ACD provides automatic answering of outside calls with greetings and menus that allow callers to select the appropriate department or to dial a known extension number.

  Cisco CP 2.3 supports B-ACD, which allows the following:
  - Create and management of Auto Attendant services and Call Queue

  - Collect call statistics.
- CUE Language Management
  Cisco CP 2.3 module settings feature allows you to perform the following language management operations:
  - System default language configuration
  - Language installation
  - Language uninstallation
- ISAKMP Profile
  Cisco CP supports the coexistence of Easy VPN Server and DMVPN hub. ISAKMP profile for DMVPN Hub is supported in preshared key mode.
- Refresh Button
  In Cisco CP 2.3, a Refresh button is available on the toolbar at the top of the page. Click the Refresh button to:
  - Rediscover the selected device in the Select Community Member drop down menu.
  - Rediscover and reload the current feature.
- Reload feature
  In Cisco CP 2.3, you can click the Reload device button from the Reload Device page to reload the router.
- SFP Interface Enhancements
  Interface Feature Edit dialog box for SFP Gigabit Ethernet interface now has an extra tab to configure Media-type. You can configure Media-type as SFP or RJ45 with fail over options.
- SIP Trunks
  A SIP trunk connects to the traditional PSTN network which is provided by an Internet Telephony Service. It makes full use of installed IP-PBXs. It communicates over IP within the enterprise as well as the outside enterprise.
  Unlike traditional telephony, where bundles of physical wires were once delivered from the service provider to a company, a SIP trunk allows a company to replace these traditional fixed PSTN lines with PSTN connectivity via SIP trunking service provider on the Internet.
- Speed Dial
  In Cisco CP 2.3, you can use the Configure Speed Dial Dialog Box to add or edit speed dial settings for the user's phone.
- Transcoding and DSP Resource Management
  Cisco CP 2.3 supports management of DSP resources for conference and transcoding services.
- VoIP Dial Peer
  The VoIP dial peer is one of the key elements of an IP Telephony system and an integral part of all call processing agents. VoIP dial peer is responsible for instructing the call processing agent, such as Cisco Unified Communication Manager Express (Cisco Unified CME), on how to route IP calls.
- VoIP Settings
  VoIP Parameters is now called VoIP Settings. Advanced Global Parameters is now called Advanced Global Settings. Several new configuration options are available for VoIP, H.323, and SIP in CME and Gateway modes.
- WAAS Express
  Cisco CP 2.3 supports WAAS Express in IOS, which includes the following:
  - Enabling evaluation license for WAAS express on your router

  - Installing digital certificate for WAAS Central Manager (WCM) WCM on your router
  - Registering your router with WCM

Cisco CP 2.3 supports following new switching features:

- The new features for the switching modules are following:
  - Switch Port configuration
  - Vlan
  - EtherChannel

- The configuration functionalities of Connected Grid Switch models CGS-2520-24TC and CGS-2520-16S-8PC are the following:
  - 802.1x
    802.1x defines a user-server-based access control, and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each user connected to a switch port before making any services offered by the switch or the LAN. Cisco CP provides configuration of 802.1x on interfaces.
  - AAA
    Cisco CP provides functionalities to configure AAA server using Radius or TACACS+. AAA server can be used to authenticate, authorize, and account the request to the device.
  - Access Control Lists (ACLs)
    ACLs consist of Access List Elements (ACEs), which are matched against a packet in sequence. An action in the ACE (permit or deny) determines whether the packets are forwarded or dropped. That is, a permitted packet is forwarded, and a denied packet is dropped. If no match is found, the packet is denied by default.
  - Device Alarm
    The Device Alarm window is used to configure primary or secondary alarm settings for switch temperature alarms, redundant power supply alarms, and port pinout alarms.
  - EtherChannel
    Cisco CP provides creation, editing, or deletion of EtherChannel. EtherChannel is a group of Fast or Gigabit Ethernet port that acts as a single logical port for high-bandwidth connections between switches or between switches and servers.
  - MAC Address
    Cisco CP shows the dynamic MAC address of the MAC address table of the switch and allows removal and configuration of all aging parameters of the MAC address.
  - Port Security
    Configuration of port security prevents unknown devices from connecting to the ports without your knowledge. When a port is secure, a user-specified action occurs whenever an address-security violation occurs.
  - QoS
    Cisco CP uses Modular QoS Command-Line Interface (MQC) to configure QoS. It supports QoS Class create, edit, and delete. It allows the user to use these classes in ingress and egress QoS policy definition. Created policies can be assigned to interfaces using Cisco CP.

  - Resilient Ethernet Protocol (REP)
    REP is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time. Cisco CP supports configuration of REP segments and administrator vlan for REP.
  - STP
    Cisco CP supports two types of spanning-tree protocol: rapid-pvst and pvst. It allows configuration and monitoring of various aspects of STP.
  - Switch Port configuration
    Cisco CP allows configuration of physical characteristics of the ports such as duplex, speed, and others. It also allows configuration of administrator status and administrative mode of the port.
  - Smartport Macro
    Smartport macros provide a convenient way to save and share common configurations. Cisco CP allows configuration following pre-defined macro to any port. Examples of pre-defined macros are Switch, Router, Desktop, AccessPoint, etc.
  - Vlan
    Cisco CP provides Vlan configuration and assignment to the port.
- The monitoring functionalities of Connected Grid Switch models CGS-2520-24TC and CGS-2520-16S-8PC are the following:
  - Port Statistics
    Cisco CP shows a snapshot of transmit and receive packets statistics on ports.
  - REP Segment
    REP is a Cisco proprietary protocol that provides an alternative to STP to control network loops, handle link failures, and improve convergence time. Cisco CP shows configured REP segment information.
  - QoS Report
    QoS report shows statistics for DSCP, Class of Services & Policer for configured QoS.
  - Health
    This feature displays the measurements on the utilization of the bandwidth, CPU, memory, device temperature, and packet errors.

New Hardware Support

The new interface cards supported are:

- HWIC-3G-HSPA
- HWIC-3G-HSPA-A
- HWIC-3G-HSPA-G
- PCEX-3G-HSPA-x

The new connected grid devices supported are:

- CGS-2520-24TC
- CGS-2520-16S-8PC
- CGR 2010/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
- JRE Settings for Cisco CP
- Pop-up Screens Appearing on Monitor other than Cisco CP

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 Monitor other than Cisco CP

Pop-up screens are seen in all SDM applet security and routing, and help pages.

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 Go to **security audit** and click on **perform security audit**.
The audit screen comes up in the primary monitor while the 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
- 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 Configuration Professional is Already Running Message
- Temporary Internet Files - Impact on Discovery
- Internet Explorer Zoom Level - Impact on Some Cisco CP Screens

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, screencasts have been provided for the following Cisco CP 2.3 features:

- 3G Feature Enhancements
- Advanced Telephony Settings
- Cisco Unified Border Element (CUBE)
- Cisco Unified CME B-ACD
- Cisco Unified CME B-ACD Prompt and Script Management
- Cisco Application Extension Platform
- CUE Language Management
- DSP Resource Management
- SIP Trunks
- VoIP Dial Peer
- WAAS Express

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 for 30 seconds and then restart Cisco CP.

Temporary Internet Files - Impact on Discovery

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 Cisco CP application.

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

Step 3 Close IE.

Step 4 Launch Cisco CP.

Caveats

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

- Open Caveats, page 29
- Resolved Caveats, page 35

Open Caveats

Table 14 lists caveats that are open in Cisco CP 2.3.

Table 14 Open Caveats in Cisco CP 2.3

Bug ID	Summary	Additional Information
CSCtj44083	Licensing is not supported if device is discovered using hostname.	**Symptom** Cisco CP displays the following error: `Device <hostname> is not legal.` **Conditions** When you try to access a device through the hostname. **Workaround** Use the IP address to access the device.
CSCth92960	EtherChannel and 802.1x external links are not correct in online help.	**Symptom** The external link to EtherChannel documentation does not work. **Conditions** The user navigates to Configure -> Switching -> Ports -> EtherChannel and clicks on online help. The online help displays the following link: http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/Ether_channel.html The user navigates to the **Configure -> Switching -> Security -> 802.1x** left link and clicks on online help. The online help displays the following link: http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/802.1x.html Clicking on the displayed external link results in a "The Page You Have Requested Is Not Available" error. **Workaround** For EtherChannel, type the following link on the browser to navigate to the correct external link: http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swethchl.html For 802.1x, type the following link on the browser to navigate to the correct external link: http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/sw8021x.html

Table 14 Open Caveats in Cisco CP 2.3 (continued)

Bug ID	Summary	Additional Information
CSCth90262	All Dynamic MAC Address are not listed in MAC Address screen under Switching Modules.	**Symptom** All Dynamic MAC Address are not listed in the MAC Address screen under Switching Modules. **Conditions** MAC Address feature will not list all the Switching Modules when term length is not configured as 0, which is the default value. **Workaround** Configure term length to 0 in the device for this feature to work.
CSCth90328	Trunk configuration fails when moved from routed/tunnel.	**Symptom** Cisco CP UI reflects successful configuration of Trunk when configured from Routed/Tunnel. But CLI is out of sync as configuration fails, since CLI expects appropriate Trunk encapsulation configuration. Trunk configuration fails if encapsulation configured on the interface is Auto irrespective of Routed/Tunnel when trunk encapsulation configured is changed to Auto or from the default configuration. **Conditions** Cisco CP will not configure Trunk when moved from Static to Routed to Trunk or from Static to Tunnel and to Trunk if encapsulation is configured as Auto. **Workaround** There is no workaround. User need to configure appropriate trunk encapsulation in CLI for the interface/port for the above configuration to work from Cisco CP.
CSCth89641	2811, 3945, 2801, and 1861 doesn't have security and voice license respectively	**Symptom** Some links/folder under security mode is grayed out/disabled or voice folder is grayed out/disabled. **Conditions** Devices discovered in offline mode. **Workaround** Select other devices in the same family to configure voice/security form in offline devices.
CSCth18231	Help page launches in primary monitor if Cisco CP is in secondary monitor.	**Symptom** Help page launches in primary monitor instead of the monitor in which Cisco CP is placed. **Conditions** System consists of dual/multiple monitors. Cisco CP is placed in non primary monitor. **Workaround** There is no workaround.
CSCth64048	CUBE wrongly discovered as CME.	**Symptom** Cisco CP may discover CUBE as CME (Call Manager Express). **Conditions** This occurs with telephony-service configuration in CUBE. **Workaround** There is no workaround.

Table 14 Open Caveats in Cisco CP 2.3 (continued)

Bug ID	Summary	Additional Information
CSCth26037	License feature not working if CUE is not reachable.	**Symptom** If a user click on **Licensing Dashboard**, he will get the exception "*com.cisco.cp.common.exception.CPCommonException*". **Conditions** The router has CUE in steady state but CUE is not reachable externally. **Workaround** For a Licensing to work on CUE module, configure an IP address to the CUE to make it reachable externally.
CSCth57014	The data between ports and intf and conn are not synced.	**Symptom** Some switching port configuration performed at one screen is not reflected in another screen. **Conditions** Cisco CP provides two ways to configure switching port functionality on a router. • **Interface and Connection** from Interface Management in left navigation. • **Port and Vlan Settings** under Interface Management -> Ports in left navigation. If you modify any of the following parameters of Switching port from one UI, changes will not reflect in another UI without rediscovery of the device. Speed, Duplex, VLAN, Description, Administrative mode and Operation mode. **Workaround** Choose only one from the two options listed above in configuring switch port functionalities. To use both options, rediscover or refresh the device, so that it will be reflected on the other screen as well.
CSCth61991	AXP: Need to handle "Required Subsystem ID not found" error message.	**Symptom** If the app-dev package associated to a package is not installed and an attempt is made to install that package using CLI, the error "Required Subsystem ID was not found either on Installed or Candidate list" is seen. If the user installs the same package through Cisco CP, the user is not informed of any error. Installation window closes after 3-4 minutes. **Conditions** Symptom is seen when a package is installed before installing the associated app-dev package. **Workaround** Install app-dev add on package provided along with the released image before installing any application.

Table 14 Open Caveats in Cisco CP 2.3 (continued)

Bug ID	Summary	Additional Information
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 we need to provide 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.
CSCth34158	Switching Modules folder are 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 is managed by Cisco CP. **Conditions** The user can observe this on 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 has the same username (privilege level 15) and a password is configured when switch console requires authentication • If there is no login is 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"
CSCth17975	SDM applets: Pop-up screens loading in monitor other than that of CCP.	**Symptom** On dual-monitor or multi-monitor screens, security screens pops up on the primary screen even when the CCP application is moved to the secondary or other screens. **Conditions** On systems with dual-monitor or multi-monitor screens, security screens will pop up only on the primary screens. **Workaround** There is no workaround and this is a limitation for this product.

Table 14 Open Caveats in Cisco CP 2.3 (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 **Module Configuration** screen. **Conditions** It's an intermittent issue seen on refreshing the module from the **Module Configuration** screen. **Workaround** Rediscover the device using **Community Member** screen.
CSCtg55407	Refresh button is missing in some instances of module configuration.	**Symptom** Refresh button is missing in **Interface Management-> Module configuration** page. **Conditions** Refresh button is missing in **Interface Management-> Module configuration** page. **Workaround** Clear the IE cache. • Go to **Control Panel-> Java**. • In **General** tab, under temporary settings, click on **Settings** and delete temporary files present on your PC.

Table 14 Open Caveats in Cisco CP 2.3 (continued)

Bug ID	Summary	Additional Information

CSCtf87466	SIP on in to self and vice versa leads to unreachable router.	**Symptom** Attaching/removing the management interface (in which CCP is invoked) from the zone-member security of firewall leads to unreachable router.
		Conditions Firewall configurations delivered has the configuration that tries to attach/remove the management interface (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 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.

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.

Resolved Caveats

Table 15 lists caveats that are resolved in Cisco CP 2.3.

Table 15 Resolved Caveats in Cisco CP 2.3

Bug ID	Summary
CSCtg19665	With Log as option, CCP reads Action as drop instead of Pass.
CSCtb81205	Location to download SDM IPS packages needs to be changed.
CSCtd99143	**match-all** command not supported in IOS version 15.0.

Related Documentation

Table 16 describes the related documentation available for Cisco CP.

Table 16 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.

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.