



Cisco Unified Operating System Administration Guide for Cisco Unified Expert Advisor

Release 7.6(1)

May 2009

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Cisco Unified Operating System Administration Guide for Cisco Unified Expert Advisor
© 2009 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xi

- Purpose 2-xi
- Audience 2-xi
- Organization 2-xi
- Related Documentation 2-xii
- Conventions 2-xii

CHAPTER 1

Introduction 1-1

- Overview 1-1
- Browser Requirements 1-2
- Operating System Status and Configuration 1-2
- Settings 1-2
- Security Configuration 1-3
- Software Upgrades 1-3
- Services 1-3

CHAPTER 2

Log In To Cisco Unified Operating System Administration Console 2-1

- Logging in to Cisco Unified Operating System Operations Console 2-1
- Recovering the Administrator Password 2-2

CHAPTER 3

Status and Configuration 3-1

- Cluster Nodes 3-1
- Hardware Status 3-2
- Network Status 3-2
- Installed Software 3-3
- System Status 3-4
- Rebuilding RAID Drives 3-5

CHAPTER 4

Settings 4-1

- IP Settings 4-1
 - Ethernet Settings 4-1
 - Publisher Settings 4-2

Changing IP Address on a Subsequent Cisco Unified Expert Advisor Node 4-3

NTP Servers 4-3

SMTP Settings 4-4

Time Settings 4-4

CHAPTER 5

System Restart 5-1

Switch Versions and Restart 5-1

Restart Current Version 5-2

Shut Down the System 5-2

CHAPTER 6

Security 6-1

Set Internet Explorer Security Options 6-1

Manage Certificates and Certificate Trust Lists 6-1

Display Certificates 6-2

Download a Certificate or CTL 6-2

Delete and Regenerate a Certificate 6-3

Upload a Certificate or Certificate Trust List 6-4

Using Third-Party CA Certificates 6-4

Monitor Certificate Expiration Dates 6-6

IPSec Management 6-7

Set Up a New IPSec Policy 6-7

Managing Existing IPSec Policies 6-9

CHAPTER 7

Software Upgrades 7-1

Software Upgrade and Installation 7-1

Obtaining the Upgrade File 7-2

Upgrading from Local Source 7-2

Upgrading from Remote Source 7-3

Stalled Upgrades 7-5

Reverting to a Previous Version 7-5

Managing TFTP Server Files 7-5

CHAPTER 8

Services 8-1

Ping 8-1

Remote Support 8-1



Preface

Purpose

The *Cisco Unified Operating System Administration Guide for Cisco Unified Expert Advisor* provides information about using the Cisco Unified Operating System graphical user interface (GUI) to perform many common system- and network-related tasks.



Note

This document may not represent the latest Cisco product information available. You can obtain the most current documentation by accessing Cisco's product documentation page at this URL:
<http://www.cisco.com/go/ea>

Audience

The *Cisco Unified Operating System Administration Guide for Cisco Unified Expert Advisor* provides information for network administrators who are responsible for managing and supporting the Cisco Unified Expert Advisor. Network engineers, system administrators, or telecom engineers use this guide to learn about, and administer, the operating system features. This guide requires knowledge of telephony and IP networking technology.

Organization

The following table shows how this guide is organized:

Chapter	Description
Chapter 1, “Introduction”	This chapter provides an overview of the functions that are available through the Cisco Unified Expert Advisor.
Chapter 2, “Log In To Cisco Unified Operating System Administration Console”	This chapter provides procedures for logging in to the Cisco Unified Operating System and for recovering a lost Administrator password.
Chapter 3, “Status and Configuration”	This chapter provides procedures for displaying operating system status and configuration settings.
Chapter 4, “Settings”	This chapter provides procedures for viewing and changing the Ethernet settings, IP settings, and NTP settings.

Chapter	Description
Chapter 5, “System Restart”	This chapter provides procedures for restarting and shutting down the system.
Chapter 6, “Security”	This chapter provides procedures for certificate management and for IPSec management.
Chapter 7, “Software Upgrades”	This chapter provides procedures for installing software upgrades and for uploading files to the TFTP server.
Chapter 8, “Services”	This chapter provides procedures for using the utilities that the operating system provides, including ping and remote support.

Related Documentation

For additional Cisco Unified Expert Advisor documentation, refer to the following URL:
http://www.cisco.com/en/US/products/ps9675/tsd_products_support_series_home.html

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:



Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:



Tip

Means *the information contains useful tips*.

Cautions use the following conventions:



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:



Warning

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

Obtaining Documentation

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Documentation Feedback

You can provide comments about this document by sending email to the following address: ccbu_docfeedback@cisco.com.



CHAPTER 1

Introduction

For Cisco Unified Expert Advisor, you can perform many common system administration functions through the Cisco Unified Operating System.

This chapter comprises the following topics:

- [Overview](#)
- [Browser Requirements](#)
- [Operating System Status and Configuration](#)
- [Security Configuration](#)
- [Software Upgrades](#)
- [Services](#)

Overview

The Cisco Unified Operating System administration console for Cisco Unified Expert Advisor allows you to configure and manage the Cisco Unified Operating System. Example of operations console tasks include the following:

- Check software and hardware status.
- Check and update IP addresses.
- Ping other network devices.
- Manage NTP servers.
- Upgrade system software and options.
- Manage server security, including IPSec and certificates
- Manage remote support accounts
- Restart the system.

The following sections describe each operating system function in more detail.

Browser Requirements

**Tip**

See the *Hardware and System Software Specification (Bill of Materials)* at the following web site to obtain a complete list of supported hardware and software information for Cisco Unified Expert Advisor: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

**Note**

Cisco does not support or test other browsers, such as Mozilla Firefox.

The URL of the Cisco Unified Operating System for Cisco Unified Expert Advisor server (**https://servername**) must be included in the browser's "Trusted Site Zone" or the "Local Intranet Site Zone" for all product features to work correctly.

Operating System Status and Configuration

From the **Show** menu, you can check the status of various operating system components, including

- Cluster and nodes

**Note**

The term node and server are used interchangeably in this document and refers to a computer that provides services or resources to other computers (called clients) connected to it through a network.

- Hardware
- Network
- System
- Installed software and options

For more information see [Chapter 3, "Status and Configuration."](#)

Settings

From the **Settings** menu, you can view and update the following operating system settings:

- IP—Updates the IP addresses and Dynamic Host Configuration Protocol (DHCP) client settings that were entered when the application was installed.
- NTP Server settings—Configures the IP addresses of an external NTP server; add or delete an NTP server.
- SMTP settings—Configures the SMTP host that the operating system will use for sending e-mail notifications.

For more information see [Chapter 4, "Settings."](#)

From the **Settings > Version** window, you can choose from the following options for restarting or shutting down the system:

- **Switch Versions**—Switches the active and inactive disk partitions and restarts the system. You normally choose this option after the inactive partition has been updated and you want to start running a newer software version.
- **Current Version**—Restarts the system without switching partitions.
- **Shutdown System**—Stops all running software and shuts down the server.



Note This command does not power down the server. To power down the server, press the power button.

For more information see [Chapter 5, “System Restart.”](#)

Security Configuration

The operating system security options enable you to manage security certificates and Secure Internet Protocol (IPSec). From the **Security** menu, you can choose the following security options:

- **Certificate Management**—Manages certificates, Certificate Trust Lists (CTL), and Certificate Signing Requests (CSR). You can display, upload, download, delete, and regenerate certificates. Through Certificate Management, you can also monitor the expiration dates of the certificates on the server.
- **IPSec Management**—Displays or updates existing IPSec policies; sets up new IPSec policies and associations.

For more information see [Chapter 6, “Security.”](#)

Software Upgrades

The software upgrade options enable you to upgrade the software version that is running on the operating system or to install specific software options.

From the **Install/Upgrade** menu option, you can upgrade system software from either a local disc or a remote server. The upgraded software gets installed on the inactive partition, and you can then restart the system and switch partitions, so the system starts running on the newer software version.



Note

For Cisco Unified Operating System for Cisco Unified Expert Advisor, you must perform all software installations and upgrades by using the software upgrades features included in the Cisco Unified Operating System for Cisco Unified Expert Advisor GUI and CLI user interfaces. The system can upload and process only software that Cisco Systems approved. You cannot install or use third-party or Windows-based software applications that you may have been using with a previous version of Cisco Unified Operating System for Cisco Unified Expert Advisor with Cisco Unified Expert Advisor.

For more information see [Chapter 7, “Software Upgrades.”](#)

Services

The application provides the following operating system utilities:

- Ping—Checks connectivity with other network devices.
- Remote Support—Sets up an account that Cisco support personnel can use to access the system. This account automatically expires after the number of days that you specify.

For more information see [Chapter 8, “Services.”](#)



CHAPTER 2

Log In To Cisco Unified Operating System Administration Console

This chapter describes the procedure for accessing the Cisco Unified Operating System administration console and also provides procedures for recovering a lost password.

Logging in to Cisco Unified Operating System Operations Console

To access Cisco Unified Operating System for Cisco Unified Expert Advisor and log in, follow this procedure.

**Note**

Do not use the browser controls (for example, the Back button) while you are using Cisco Unified Operating System administration console.

Procedure

- Step 1** Log in to Cisco Unified Expert Advisor operations console.
- Step 2** From the Navigation menu in the upper, right corner of the Cisco Unified Operating System administration console window, choose **Cisco Unified OS Administration** and click **Go**.

The Cisco Unified Operating System administration console Logon window displays.

**Note**

You can also access Cisco Unified Operating System administration console directly by entering the following URL:

`http://server-name/cmplatform`

- Step 3** Enter your Administrator username and password.

**Note**

The Administrator username and password get established during installation or created by using the command line interface.

- Step 4** Click **Submit**.

The Cisco Unified Operating System administration console window displays.

Recovering the Administrator Password

If you lose the Administrator password and cannot access the system, use the following procedure to reset the Administrator password.

**Note**

During this procedure, you will be required to remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Procedure

- Step 1** Log in to the system with the following username and password:
- Username: **pwrecovery**
 - Password: **pwreset**
- The Welcome to admin password reset window displays.
- Step 2** Press any key to continue.
- Step 3** If you have a CD or DVD in the disk drive, remove it now.
- Step 4** Press any key to continue.
- The system tests to ensure that you have removed the CD or DVD from the disk drive.
- Step 5** Insert a valid CD or DVD into the disk drive.
- The system tests to ensure that you have inserted the disk.
- Step 6** After the system verifies that you have inserted the disk, you get prompted to enter a new Administrator password.
- Step 7** Reenter the new password.
- The system checks the new password for strength. If the password does not contain enough different characters, you get prompted to enter a new password.
- Step 8** After the system verifies the strength of the new password, the password gets reset, and you get prompted to press any key to exit the password reset utility.
-



CHAPTER 3

Status and Configuration

This chapter provides information on administering the system and contains the following topics:

- [Cluster Nodes](#)
- [Hardware Status](#)
- [Network Status](#)
- [Installed Software](#)
- [System Status](#)

You can view the status of the operating system, platform hardware, or the network.

Cluster Nodes



Note

The term node and server are used interchangeably in this document and refers to a computer that provides services or resources to other computers (called clients) connected to it through a network.

To view information on the nodes in the cluster, follow this procedure:

Procedure

- Step 1** From the Cisco Unified Operating System administration console window navigate to **Show > Cluster**. The Cluster Nodes window displays.
- Step 2** For a description of the fields on the Cluster Nodes window, see [Table 3-1](#).

Table 3-1 Cluster Nodes Field Descriptions

Field	Description
Hostname	Displays the complete hostname of the server.
IP Address	Displays the IP address of the server.
Alias	Displays the alias name of the server, when defined.
Type of Node	Indicates whether the server is a primary node or a secondary node.

Hardware Status

To view the hardware status, follow this procedure:

Procedure

Step 1 From the Cisco Unified Operating System administration console window, navigate to **Show>Hardware**.

The Hardware status window displays.

Step 2 For descriptions of the fields on the Platform Hardware status window, see [Table 3-2](#).

Table 3-2 Platform Hardware Status Field Descriptions

Field	Description
Platform Type	Displays the model identity of the platform server.
Processor Speed	Displays the processor speed.
Number of Processors	Displays the number of processors in the platform server.
CPU Type	Displays the type of processor in the platform server.
Memory	Displays the total amount of memory in MBytes.
Object ID	Displays the object ID.
OS Version	Displays the operating system version.
Details	Displays a detailed summary of the platform hardware.

Network Status

The network status information that displays depends on whether Network Fault Tolerance is enabled. When Network Fault Tolerance is enabled, Ethernet port 1 automatically takes over network communications if Ethernet port 0 fails. If Network Fault Tolerance is enabled, network status information displays for the network ports Ethernet 0, Ethernet 1, and Bond 0. If Network Fault Tolerance is not enabled, status information displays only for Ethernet 0.

To view the network status, follow this procedure:

Procedure

Step 1 From the Cisco Unified Operating System administration console window, navigate to **Show > Network**.

The Network Settings window displays.

Step 2 See [Table 3-3](#) for descriptions of the fields on the Network Settings window.

Table 3-3 Network Settings Field Descriptions

Section/Field	Description
Ethernet Details	
DHCP	Indicates whether DHCP is enabled for Ethernet port 0.
Status	Indicates whether the port is Up or Down for Ethernet ports 0 and 1.
IP Address	Shows the IP address of Ethernet port 0 (and Ethernet port 1 if Network Fault Tolerance (NFT) is enabled).
IP Mask	Shows the IP mask of Ethernet port 0 (and Ethernet port 1 if NFT is enabled).
Link Detected	Indicates whether there is an active link.
Queue Length	Displays the length of the queue.
MTU	Displays the maximum transmission unit.
MAC Address	Displays the hardware address of the port.
Receive Statistics	Displays information on received bytes and packets.
Transmit Statistics	Displays information on transmitted bytes and packets.
DNS Details	
Primary	Displays the IP address of the primary domain name server.
Secondary	Displays the IP address of the secondary domain name server.
Options	Displays the timeouts and attempts of the domain name server.
Domain	Displays the domain of the server.
Gateway	Displays the IP address of the network gateway on Ethernet port 0.

Installed Software



Tip

See the Hardware and System Software Specification (Bill of Materials) at the following web site to obtain a complete list of supported hardware and software information for Cisco Unified Expert Advisor: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

To view the software versions and installed software options, follow this procedure:

Procedure

- Step 1** From the Cisco Unified Operating System administration console window, navigate to **Show > Software**.
The Software Packages window displays.
- Step 2** For a description of the fields on the Software Packages window, see [Table 3-4](#).

Table 3-4 Software Packages Field Descriptions

Field	Description
Partition Versions	Displays the software version that is running on the active and inactive partitions.
Active Version	Displays the versions of installed software options that are installed on the active version.
Inactive Version	Displays the versions of installed software options that are installed on the inactive version.
Installed Software Options	Summarizes the installed software version that is running on the active and inactive partitions.

System Status

To view the system status, follow this procedure:

Procedure

- Step 1** From the Cisco Unified Operating System administration console window, navigate to **Show > System**. The System Status window displays.
- Step 2** See [Table 3-5 on page 3-4](#) for descriptions of the fields on the Platform Status window.

Table 3-5 Platform Status Field Descriptions

Field	Description
Host Name	Displays the name of the Cisco MCS host where the operating system is installed.
Date	Displays the date and time based on the continent/region specified during installation.
Time Zone	Displays the time zone that was chosen during installation.
Locale	Displays the language that was chosen during operating system installation.
Product Version	Displays the operating system version.
Platform Version	Displays the platform version.
Uptime	Displays system uptime information.
CPU	Displays the percentage of CPU capacity that is idle, the percentage that is running system processes, and the percentage that is running user processes.
Memory	Displays information about memory usage, including the amount of total memory, free memory, and used memory in KBytes.
Disk/active	Displays the amount of total, free, and used disk space on the active disk.
Disk/inactive	Displays the amount of total, free, and used disk space on the inactive disk.
Disk/logging	Displays the amount of total, free, and disk space that is used for disk logging.

Rebuilding RAID Drives

A RAID drive may fail and may require manual intervention to rebuild one of the physical drives in a logical pair during normal operation.

RAIDed disks, also termed RAID arrays, get arranged in logical pairs. A single logical pair comprises two physical drives. The system keeps the pair of drives in sync with the same data in real time to provide redundancy ultimately for data integrity and assurance. When one physical drive fails to synchronize or begins to experience read or write failures, you may need to rebuild the drive. Many things can cause the failure, but the main concern remains whether the data in a logical drive pair is compromised due to failures in one of the physical drives.

Monitoring software usually detects RAID failures, and failures get reported as a failed drive or a loss of drive redundancy. The procedure for rebuilding a failing drive follows and applies to all applicable servers.

First, check the status of the RAID array by using the CLI **show hardware** command and verify whether the Status field reads Ok or Okay. An example follows:

```
admin:show hardware
HW Platform       : 7835I
Processors        : 1
Type              : Intel(R) Xeon(TM) CPU 3.06GHz
CPU Speed         : 3066
Memory            : 2048 MBytes
Object ID         : 1.3.6.1.4.1.9.1.585
OS Version        : UCOS 2.0.1.0-37
RAID Details      :
Found 1 IBM ServeRAID controller(s).
Read configuration has been initiated for controller 1...
-----
Logical drive information
-----
Logical drive number 1
  Status of logical drive      : Okay (OKAY)
  RAID level                   : 1
  Size (in MB)                 : 70006
  Write cache status           : Temporary write through (TWT)
  Number of chunks              : 2
  Stripe-unit size              : 8 KB
  Access blocked                : No
  Part of array                 : A
Array A stripe order (Channel/SCSI ID) : 1,0 1,1 Command completed successfully.
```

If the RAID array status field does not read Ok or Okay (for example, shows Degraded or Critical), perform the following steps:

-
- Step 1** Log in to console and enter the CLI command, **utils system shutdown**.
 - Step 2** Power off the server (press power off button).
 - Step 3** Extract the failed disk drive.
 - Step 4** Power up the server (press power on button).

If the server is an IBM server (for example, a 7825I, 7835I, or 7845I), the following menu will appear during system reboot:

```
1:ServeRAID-5i Slot 2, Logical drv=1, Firmware=7.12.07, Status=Fail
1 Drive(s) not responding or found at new location(s)
Press F2 Detailed information
      F4 Retry the command
```

```
F5 Change the configuration and set the drive(s) defunct
F10 Continue without changing the configuration
```

- Step 5** Press **F5**
- Step 6** After the login prompt appears in the console window, log in and check the status of the RAID array by using the CLI **show hardware** command; the Status field should read Degraded or Critical.
- Step 7** Insert the failed disk drive into the original slot; be sure to lock it properly in place.
- Step 8** Check the status of the RAID array by using the CLI **show hardware** command; the Status field will read Rebuilding or Critical.
- Step 9** After an hour, recheck the status of the RAID array by using the CLI **show hardware** command and verify that the Status field reads Ok or Okay.

If the status does not read Ok or Okay, you may need to replace the physical drive.



CHAPTER 4

Settings

Use the Settings options to display and change IP settings, host settings, and Network Time Protocol (NTP) settings.

IP Settings

The IP Settings options allow you to view and change IP and port setting for the Ethernet connection and, on subsequent nodes, to set the IP address of the publisher.

Ethernet Settings

The IP Settings window indicates whether Dynamic Host Configuration Protocol (DHCP) is active and also provides the related Ethernet IP addresses, as well as the IP address for the network gateway.

All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The Maximum Transmission Unit (MTU) on Eth0 defaults to 1500.

To view or change the IP settings, follow this procedure:

Procedure

Step 1 From the Cisco Unified Operating System administration console window, navigate to **Settings > IP > Ethernet**.

The Ethernet Settings window displays.

Step 2 To modify the Ethernet settings, enter the new values in the appropriate fields. For a description of the fields on the Ethernet Settings window, see [Table 4-1](#).



Note If you enable DHCP, the Port and Gateway settings get disabled and cannot be changed.

Step 3 To preserve your changes, click **Save**.

Table 4-1 Ethernet Settings Fields and Descriptions

Field	Description
Status	
Status	Displays the status of the currently-issued command or operation within this page.
DHCP Information	
DHCP	Indicates whether DHCP is Enabled or Disabled.
Port Information	
IP Address	Shows the IP address of the system.
Subnet Mask	Shows the IP subnet mask address.
Gateway Information	
Default Gateway	Shows the IP address of the network gateway.

Publisher Settings

On subsequent or subscriber nodes, you can view or change the IP address of the first node or publisher for the node.

To view or change the publisher IP settings, follow this procedure:

Procedure

- Step 1** From the Cisco Unified Operating System administration console window, navigate to **Settings > IP > Publisher**.

The Publisher Settings window displays.



Note You can only view and change the publisher IP address on subsequent nodes of the cluster, not on the publisher itself.

- Step 2** Enter the new publisher IP address.

- Step 3** Click Save.

Changing IP Address on a Subsequent Cisco Unified Expert Advisor Node

**Caution**

While Cisco Unified Expert Advisor allows you to change the IP address on a subsequently added server, it does not allow you to change the hostname.

If the IP address of the first Cisco Unified Expert Advisor node gets changed while a subsequent node is offline, you may not be able to log in to Cisco Unified Operating System administration console on the subsequent node. If this occurs, follow this procedure:

-
- Step 1** Log in directly to Cisco Unified Operating System administration console on the subsequent node by using the following IP address:
- `http://server-name/iptplatform`
- where *server-name* specifies the host name or IP address of the subsequent node.
- Step 2** Enter your Administrator user name and password and click **Submit**.
- Step 3** Navigate to **Settings > IP > Publisher**.
- Step 4** Enter the new IP address for the publisher and click **Save**.
- Step 5** Restart the subsequent node.
-

NTP Servers

Ensure that external NTP server is stratum 9 or higher (1-9). To add, delete, or modify an external NTP server, follow this procedure:

**Note**

You can only configure the NTP server settings on the first node or publisher.

Procedure

-
- Step 1** From the Cisco Unified Operating System administration console window, navigate to **Settings > NTP Servers**.
- The NTP Server Settings window displays.
- Step 2** You can add, delete, or modify an NTP server:
- To delete an NTP server, check the check box in front of the appropriate server and click **Delete**.
 - To add an NTP server, click **Add**, enter the hostname or IP address, and then click **Save**.
 - To modify an NTP server, click the IP address, modify the hostname or IP address, and then click **Save**.

**Note**

Any change you make to the NTP servers can take up to five minutes to complete. Whenever you make any change to the NTP servers, you must refresh the window to display the correct status.

- Step 3** To refresh the NTP Server Settings window and display the correct status, choose **Settings > NTP**.



Note After deleting, modifying, or adding a NTP server, you must restart all the other nodes in the cluster for the changes to take affect.

SMTP Settings

The SMTP Settings window allows you to view or set the SMTP hostname and indicates whether the SMTP host is active.



Tip If you want the system to send you e-mail, you must configure an SMTP host.

To access the SMTP settings, follow this procedure:

Procedure

Step 1 From the Cisco Unified Operating System administration console window, navigate to **Settings > SMTP**.

The SMTP Settings window displays.

Step 2 Enter or modify the SMTP hostname or IP address.

Step 3 Click **Save**.

Time Settings

To manually configure the time, follow this procedure:



Note Before you can manually configure the server time, you must delete any NTP servers that you have configured. See [NTP Servers](#) for more information.

Procedure

Step 1 From the Cisco Unified Operating System administration console window, navigate to **Settings > Time**.

Step 2 Enter the date and time for the system.

Step 3 Click **Save**.



CHAPTER 5

System Restart

This section provides procedures for using the following restart options:

- [Switch Versions and Restart](#)
- [Restart Current Version](#)
- [Shut Down the System](#)

Switch Versions and Restart



Tip

See the Hardware and System Software Specification (Bill of Materials) at the following web site to obtain a complete list of supported hardware and software information for Cisco Unified Expert Advisor: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

You can use this option both when you are upgrading to a newer software version or when you need to fall back to an earlier software version. To shut down the system that is running on the active disk partition and then automatically restart the system using the software version on the inactive partition, follow this procedure:



Caution

This procedure causes the system to restart and become temporarily out of service.

Procedure

- Step 1** From the Cisco Unified Operating System administration console window, navigate to **Settings > Version**.
- The Version Settings window displays, which shows the software version on both the active and inactive partitions.
- Step 2** To switch versions and restart, click **Switch Versions**. To stop the operation, click **Cancel**.
- If you click **Switch Version**, the system restarts, and the partition that is currently inactive becomes active.

Restart Current Version

To restart the system on the current partition without switching versions, follow this procedure:



This procedure causes the system to restart and become temporarily out of service.

Procedure

Step 1 From the Cisco Unified Operating System administration console window, navigate to **Settings > Version**.

The Version Settings window displays, which shows the software version on both the active and inactive partitions.

Step 2 To restart the system, click **Restart**, or to stop the operation, click **Cancel**.

If you click **Restart**, the system restarts on the current partition without switching versions.

Shut Down the System



If you press the power button on the server, the system will immediately shut down.

To shut down the system, follow this procedure:



This procedure causes the system to shut down.

Procedure

Step 1 From the Cisco Unified Operating System administration console window, navigate to **Settings > Version**.

The Version Settings window displays, which shows the software version on both the active and inactive partitions.

Step 2 To shut down the system, click **Shutdown**, or to stop the operation, click **Cancel**.

If you click **Shutdown**, the system halts all processes and shuts down.



Note The hardware does not power down automatically.



CHAPTER 6

Security

This chapter describes Certificate Management and IPSec Management and provides procedures for performing the following tasks:

- [Set Internet Explorer Security Options](#)
- [Manage Certificates and Certificate Trust Lists](#)
- [IPSec Management](#)

Set Internet Explorer Security Options

To download certificates from the server, ensure your Internet Explorer security settings are configured as follows:

Procedure

- Step 1** Start Internet Explorer.
 - Step 2** Navigate to **Tools > Internet Options**.
 - Step 3** Click the **Advanced** tab.
 - Step 4** Scroll down to the Security section on the Advanced tab.
 - Step 5** If necessary, clear the **Do not save encrypted pages to disk** check box.
 - Step 6** Click **OK**.
-

Manage Certificates and Certificate Trust Lists

The functions that you can perform from the Certificate Management menu are described in the following topics:

- [“Display Certificates” section on page 6-2](#)
- [“Download a Certificate or CTL” section on page 6-2](#)
- [“Delete and Regenerate a Certificate” section on page 6-3](#)
- [“Upload a Certificate or Certificate Trust List” section on page 6-4](#)

- [“Using Third-Party CA Certificates” section on page 6-4](#)

**Note**

To access the Security menu items, you must re-log in to Cisco Unified Operating System administration console using your administrator password.

Display Certificates

To display existing certificates, follow this procedure:

Procedure

Step 1 Navigate to **Security > Certificate Management**.

The Certificate List window displays.

Step 2 You can use the Find controls to filter the certificate list.

**Tip**

The certificates relevant to Cisco Unified Expert Advisor are tomcat_cert and ipsec_cert.

Step 3 To view details of a certificate or trust store, click its file name.

The Certificate Configuration window displays information about the certificate.

Step 4 To return to the Certificate List window, select **Back To Find/List** in the Related Links list; then, click **Go**.

Download a Certificate or CTL

To download a certificate or certificate trust list (CTL) to your PC, follow this procedure:

Procedure

Step 1 Navigate to **Security > Certificate Management**.

The Certificate List window displays.

Step 2 You can use the Find controls to filter the certificate list.

Step 3 Click the file name of the certificate or CTL.

The Certificate Configuration window displays.

Step 4 Click **Download**.

Step 5 In the File Download dialog box, click **Save**.

Delete and Regenerate a Certificate

These sections describe deleting and regenerating a certificate:

- “[Deleting a Certificate](#)” section on page 6-3
- “[Regenerating a Certificate](#)” section on page 6-3

Deleting a Certificate

To delete a trusted certificate, follow this procedure:

**Caution**

Deleting a certificate can affect your system operations.

Procedure

-
- Step 1** Navigate to **Security > Certificate Management**.
The Certificate List window displays.
- Step 2** You can use the Find controls to filter the certificate list.
- Step 3** Click the file name of the certificate or CTL.
The Certificate Configuration window displays.
- Step 4** Click **Delete**.
-

Regenerating a Certificate

To regenerate a certificate, follow this procedure:

**Caution**

Regenerating a certificate can affect your system operations.

Procedure

-
- Step 1** Navigate to **Security > Certificate Management**.
The Certificate List window displays.
- Step 2** Click **Generate New**.
The Generate Certificate dialog box opens.
- Step 3** Choose a certificate name from the Certificate Name list.
- Step 4** Click **Generate New**.
-

Upload a Certificate or Certificate Trust List



Caution

Uploading a new certificate or certificate trust list file can affect your system operations.



Note

The system does not distribute trust certificates to other cluster nodes automatically. If you need to have the same certificate on more than one node, you must upload the certificate to each node individually.

The [“Upload a Certificate”](#) section on page 6-4 describes how upload a Certificate Authority (CA) root certificate to the server:

Upload a Certificate

Procedure

-
- Step 1** Navigate to **Security > Certificate Management**.
The Certificate List window displays.
- Step 2** Click **Upload Certificate**.
The Upload Certificate dialog box opens.
- Step 3** Select the certificate name from the **Certificate Name** list.
- Step 4** If you are uploading an application certificate that was issued by a third-party CA, enter the name of the CA root certificate in the **Root Certificate** text box. If you are uploading a CA root certificate, leave this text box empty.
- Step 5** Select the file to upload by doing one of the following steps:
- In the **Upload File** text box, enter the path to the file.
 - Click the **Browse** button and navigate to the file; then, click **Open**.
- Step 6** To upload the file to the server, click the **Upload File** button.
-

Using Third-Party CA Certificates

Cisco Unified Expert Advisor supports certificates that a third-party Certificate Authority (CA) issues with PKCS # 10 Certificate Signing Request (CSR). The following table provides an overview of this process, with references to additional documentation:

	Task	For More Information
Step 1	Generate a CSR on the server.	See the “Generating a CSR” section on page 6-5.
Step 2	Download the CSR to your PC.	See the “Download a CSR” section on page 6-5.
Step 3	Use the CSR to obtain an application certificate from a CA.	Get information about obtaining application certificates from your CA. See “Obtaining Third-Party CA Certificates” section on page 6-6 for additional notes.

	Task	For More Information
Step 4	Obtain the CA root certificate.	Get information about obtaining a root certificate from your CA. See “Obtaining Third-Party CA Certificates” section on page 6-6 for additional notes.
Step 5	Upload the CA root certificate to the server.	See the “Upload a Certificate” section on page 6-4.
Step 6	Upload the application certificate to the server.	See the “Upload a Certificate” section on page 6-4.
Step 7	If you updated the certificate for Cisco Unified Expert Advisor, generate a new Certificate Trust List (CTL) file.	See the <i>Administration and Configuration Guide for Cisco Unified Expert Advisor</i> .
Step 8	Restart the services that are affected by the new certificate.	For all certificate types, restart the corresponding service (for example, restart the Tomcat service if you updated the Tomcat certificate). See the <i>Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor</i> for information about restarting services.

Generating a CSR

To generate a Certificate Signing Request (CSR), follow these steps:

Procedure

-
- Step 1** Navigate to **Security > Certificate Management**.
The Certificate List window displays.
 - Step 2** Click **Generate CSR**.
The Generate Certificate Signing Request dialog box opens.
 - Step 3** Select the certificate name from the **Certificate Name** list.
 - Step 4** Click **Generate CSR**.
-

Download a CSR

To download a CSR, follow this procedure:

Procedure

-
- Step 1** Navigate to **Security > Certificate Management**.
The Certificate List window displays.
 - Step 2** Click **Download CSR**.
The Download Certificate Signing Request dialog box opens.
 - Step 3** Select the certificate name from the **Certificate Name** list.

- Step 4** Click **Download CSR**.
- Step 5** In the File Download dialog box, click **Save**.

Obtaining Third-Party CA Certificates

To use an application certificate that a third-party CA issues, you must obtain both the signed application certificate and the CA root certificate from the CA. Get information about obtaining these certificates from your CA. The process varies among CAs.

Cisco Unified Expert Advisor CSRs include extensions that you must include in your request for an application certificate from the CA. If your CA does not support the ExtensionRequest mechanism, you must enable the X.509 extensions that are listed on the final page of the CSR generation process.

Cisco Unified Operating System generates certificates in DER and PEM encoding formats and generates CSRs in PEM encoding format. It accepts certificates in DER and DER encoding formats.

Cisco verified third-party certificates that were obtained from Microsoft, Keon, and Verisign CAs. Certificates from other CAs might work but have not been verified.

Monitor Certificate Expiration Dates

The system can automatically send you an e-mail when a certificate is close to its expiration date. To view and configure the Certificate Expiration Monitor, follow this procedure:

Procedure

- Step 1** To view the current Certificate Expiration Monitor configuration, navigate to **Security > Certificate Monitor**.
- The Certificate Monitor window displays.
- Step 2** Enter the required configuration information. See [Table 6-1](#) for a description of the Certificate Monitor Expiration fields.
- Step 3** To save your changes, click **Save**.

Table 6-1 Certificate Monitor Field Descriptions

Field	Description
Notification Start Time	Enter the number of days before the certificate expires that you want to be notified.
Notification Frequency	Enter the frequency for notification, either in hours or days.
Enable E-mail Notification	Select the check box to enable e-mail notification.
Email IDs	Enter the e-mail address to which you want notifications sent.
	Note For the system to send notifications, you must configure an SMTP host.

IPSec Management

The functions that you can perform with the IPSec menu are described in the following topics:

- “Set Up a New IPSec Policy” section on page 6-7
- “Managing Existing IPSec Policies” section on page 6-9



Note

IPSec does not get automatically set up between nodes in the cluster during installation.

Set Up a New IPSec Policy

To set up a new IPSec policy and association, follow this procedure:



Note

Because any changes that you make to an IPSec policy during a system upgrade will get lost, do not modify or create IPSec policies during an upgrade.



Caution

IPSec, especially with encryption, will affect the performance of your system.

Procedure

- Step 1** Navigate to **Security > IPSEC Configuration**.
The IPSec Policy List window displays.
- Step 2** Click **Add New**.
The IPSec Policy Configuration window displays.
- Step 3** Enter the appropriate information on the IPSec Policy List window. For a description of the fields on this window, see [Table 6-2](#).
- Step 4** To set up the new IPSec policy, click **Save**.

Table 6-2 *IPSec Policy and Association Field Descriptions*

Field	Description
IPSec Policy Details	
Policy Name	Specifies the name of the IPSec policy. The name can contain only letters, digits, and hyphens.
Association Name	Specifies the association name that is given to each IPSec association. The name can contain only letters, digits, and hyphens.
Authentication Method	Specifies the authentication method.
Preshared Key	Specifies the preshared key if you selected Pre-shared Key in the Authentication Name field.

Table 6-2 *IPSec Policy and Association Field Descriptions (continued)*

Field	Description
Peer Type	Specifies whether the peer is the same type or different.
Certificate Name	Identifies the certificate with a unique name.
Destination Address	Specifies the IP address or FQDN of the destination.
Destination Port	Specifies the port number at the destination.
Source Address	Specifies the IP address or FQDN of the source.
Source Port	Specifies the port number at the source.
Mode	Specifies Tunnel or Transport mode.
Remote Port	Specifies the port number to use at the destination.
Protocol	Specifies the specific protocol, or Any: <ul style="list-style-type: none"> • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices include <ul style="list-style-type: none"> • DES • 3DES
Hash Algorithm	Specifies the hash algorithm <ul style="list-style-type: none"> • SHA1—Hash algorithm that is used in phase 1 IKE negotiation • MD5—Hash algorithm that is used in phase 1 IKE negotiation
ESP Algorithm	From the drop-down list, choose the ESP algorithm. Choices include <ul style="list-style-type: none"> • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
Phase 1 DH Group	
Phase One Life Time	Specifies the lifetime for phase One, IKE negotiation, in seconds.
Phase One DH	From the drop-down list, choose the phase One DH value. Choices include: 2, 1, 5, 14, 16, 17, and 18.
Phase 2 DH Group	
Phase Two Life Time	Specifies the lifetime for phase Two, IKE negotiation, in seconds.
Phase Two DH	From the drop-down list, choose the phase Two DH value. Choices include: 2, 1, 5, 14, 16, 17, and 18.

Table 6-2 IPSec Policy and Association Field Descriptions (continued)

Field	Description
IPSec Policy Configuration	
Enable Policy	Check the check box to enable the policy.

Managing Existing IPSec Policies

To display, enable or disable, or delete an existing IPSec policy, follow this procedure:



Note

Because any changes that you make to an IPSec policy during a system upgrade will get lost, do not modify or create IPSec policies during an upgrade.



Caution

IPSec, especially with encryption, will affect the performance of your system. Any changes that you make to the existing IPSec policies can impact your normal system operations.

Procedure

Step 1 Navigate to **Security > IPSEC Configuration**.



Note To access the Security menu items, you must re-log in to Cisco Unified Operating System administration console using your Administrator password.

The IPSec Policy List window displays.

Step 2 To display, enable, or disable a policy, follow these steps:

- a. Click the policy name.
The IPSec Policy Configuration window displays.
- b. To enable or disable the policy, use the **Enable Policy** check box.
- c. Click **Save**.

Step 3 To delete one or more policies, follow these steps:

- a. Select the check box next to the policies that you want to delete.
You can click **Select All** to select all policies or **Clear All** to clear all the check boxes.
- b. Click **Delete Selected**.



CHAPTER 7

Software Upgrades

You can use the Software Upgrades options to upgrade the application software and install Cisco Unified Expert Advisor.



Tip

See the Hardware and System Software Specification (Bill of Materials) at the following web site to obtain a complete list of supported hardware and software information for Cisco Unified Expert Advisor: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

Software Upgrade and Installation

With this version of Cisco Unified Expert Advisor, you can install upgrade software on your server while the system continues to operate. Two partitions exist on your system: an active, bootable partition and an inactive, bootable partition. The system boots up and operates entirely on the partition that is marked as the active partition.

When you install upgrade software, you install the software on the inactive partition. The system continues to function normally while you are installing the software. When you are ready, you activate the inactive partition and reboot the system with the new upgrade software. The current active partition will then get identified as the inactive partition when the system restarts. The current software remains in the inactive partition until the next upgrade. Your configuration information migrates automatically to the upgraded version in the active partition.

If for any reason you decide to back out of the upgrade, you can restart the system to the inactive partition that contains the older version of the software. However, any configuration changes that you made since upgrading the software will be lost.



Note

You can only make changes to the database on the active partition. The database on the inactive partition does not get updated. If you make changes to the database after an upgrade, you must repeat those changes after switching the partition.

You can install a patch or upgrade version from a DVD (local source) or from a network location (remote source) that the Cisco Unified Expert Advisor server can access.

In Cisco Unified Expert Advisor, you must upgrade and switch the active partition on the first node before performing an upgrade and /or switching to the subscriber nodes.

**Note**

Be sure to back up your system data before starting the software upgrade process. For more information, see the *Disaster Recovery System Administration Guide for Cisco Unified Expert Advisor Option*.

**Tip**

See the Hardware and System Software Specification (Bill of Materials) at the following web site to obtain a complete list of supported hardware and software information for Cisco Unified Expert Advisor: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

Obtaining the Upgrade File

**Tip**

See the Hardware and System Software Specification (Bill of Materials) at the following web site to obtain a complete list of supported hardware and software information for Cisco Unified Expert Advisor: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

Before you begin the upgrade process, you must obtain the appropriate upgrade file from Cisco.com.

**Note**

Do not rename the patch file before you install it because the system will not recognize it as a valid file.

**Note**

Do not unzip or untar the file. If you do, the system may not be able to read the upgrade files.

You can access the upgrade file during the installation process from either a local disk (CD or DVD) or from a remote FTP or SFTP server.

**Caution**

TFTP file management is not used by Cisco Unified Expert Advisor. It continues to show up in the operations console as it remains part of the legacy platform for the Cisco Unified Communications Manager.

Upgrading from Local Source

You can install software from a CD or DVD that is located in the local disc drive and then start the upgrade process.

To install or upgrade software from a CD or DVD, follow this procedure:

Procedure**Step 1**

Create an upgrade disk by using the upgrade file that you downloaded from Cisco.com.

- If you are using an upgrade file with the tar.gz.sgn extension, copy the upgrade file to a writeable DVD.
- If you are using an upgrade file with the sgn.iso extension, you must create an ISO image on a writable DVD from the upgrade file. Just copying the .iso file to the DVD will not work.

- Step 2** Insert the new DVD into the disc drive on the local server that is to be upgraded.
- Step 3** Log into Cisco Unified Operating System administration console.
- Step 4** Navigate to **Software Upgrades > Install/Upgrade**.
The Software Installation/Upgrade window displays.
- Step 5** Choose **DVD/CD** from the **Source** list.
- Step 6** Enter the path to the patch file on the CD or DVD in the Directory field.
If the file is in the root directory, or if you created an ISO image DVD, enter a slash (/) in the Directory field.
- Step 7** To continue the upgrade process, click **Next**.
- Step 8** Choose the upgrade version that you want to install and click **Next**.
- Step 9** In the next window, monitor the progress of the download.
When the download completes, the next window displays a checksum value if you are using an upgrade file with the tar.gz.sg extension. No checksum is displayed if you burned an ISO image DVD.
- Step 10** Verify the checksum value against the checksum for the file that you downloaded that is shown on Cisco.com.

**Caution**

The two checksum values must match to ensure the authenticity and integrity of the upgrade file. If the checksum values do not match, download a fresh version of the file from Cisco.com and try the upgrade again.

- Step 11** Click **Next**.
- Step 12** If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts running the upgraded software.
- Step 13** If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, do the following steps:
- Choose **Do not reboot after upgrade**.
 - Click **Next**.
The Upgrade Status window displays the Upgrade log.
 - When the installation completes, click **Finish**.
 - To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts running the upgraded software.

Upgrading from Remote Source

To upgrade the software from a network location or remote server, use the following procedure.

Procedure

- Step 1** Put the upgrade file on an FTP or SFTP server that the server you are upgrading can access.

- Step 2** Log into Cisco Unified Operating System administration console.
- Step 3** Navigate to **Software Upgrades > Install/Upgrade**.
The Software Installation/Upgrade window displays.
- Step 4** Choose **Remote Filesystem** from the **Source** list.
- Step 5** Enter the path to the directory that contains the patch file on the remote system in the **Directory** field.
If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter **/patches**. If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.
- Step 6** In the **Server** field, enter the server name or IP address.
- Step 7** In the **User Name** field, enter your user name on the remote server.
- Step 8** In the **User Password** field, enter your password on the remote server.
- Step 9** Select the transfer protocol from the **Transfer Protocol** field.
- Step 10** To continue the upgrade process, click **Next**.
- Step 11** Choose the upgrade version that you want to install and click **Next**.
- Step 12** In the next window, monitor the progress of the download.
When the download completes, the next window displays a checksum value if you are using an upgrade file with the tar.gz.sg extension. No checksum is displayed if you burned an ISO image DVD.
- Step 13** When the download completes, verify the checksum value against the checksum (if available) for the file you that downloaded that is shown on Cisco.com.

**Caution**

The two checksum values must match to ensure the authenticity and integrity of the upgrade file. If the checksum values do not match, download a fresh version of the file from Cisco.com and try the upgrade again.

- Step 14** Click **Next**.
- Step 15** If you are installing upgrade software, skip to [Step 16](#).
- Step 16** If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts running the upgraded software.
- Step 17** If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, do the following steps:
- a. Choose **Do not reboot after upgrade**.
 - b. Click **Next**.
The Upgrade Status window displays the Upgrade log.
 - c. When the installation completes, click **Finish**.
 - d. To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts running the upgraded software.

Stalled Upgrades

During the installation of upgrade software, the upgrade may appear to stall. The upgrade log stops displaying new log messages. When the upgrade stalls, you must cancel the upgrade, disable I/O throttling, and restart the upgrade procedure. When you successfully complete the upgrade, you do not need to reenable I/O throttling.

To disable I/O throttling, enter the CLI command **utils iothrottle disable**.

To display the status of I/O throttling, enter the CLI command **utils iothrottle status**.

To enable I/O throttling, enter the CLI command **utils iothrottle enable**. By default, iothrottle is enabled.

If the system does not respond to the cancellation, you must reboot the server, disable I/O throttling, and restart the upgrade process procedure.

Reverting to a Previous Version

After upgrading, you can revert to the software version that was running before the upgrade, by restarting your system and switching to the software version on the inactive partition.

Procedure

-
- Step 1** Open Cisco Unified Operating System administration console directly by entering the following URL:
https://server-name/cmplatform
where *server-name* is the host name or IP address of the Cisco Unified Expert Advisor server.
- Step 2** Enter your Administrator username and password.
- Step 3** Choose **Settings > Version**.
The Version Settings window displays.
- Step 4** Click the **Switch Versions** button.
When you verify that you want to restart the system, the system restarts running the upgraded software. This restart might take several minutes.
-

Managing TFTP Server Files



Caution

TFTP file management is not used by Cisco Unified Expert Advisor. It continues to show up in the operations console as it remains part of the legacy platform for the Cisco Unified Communications Manager.

To upload and delete TFTP server files, follow this procedure:

Procedure

-
- Step 1** From the Cisco Unified Operating System administration console window, navigate to **Software Upgrades > TFTP File Management**.

The TFTP File Management window displays and shows a listing of the current uploaded files. You can filter the file list by using the Find controls.

- Step 2** To upload a file, follow this procedure:

- a. Click **Upload File**.

The Upload File dialog box opens.

- b. To upload a file, click **Browse** and then choose the file that you want to upload.

- c. To upload the file to a subdirectory of the `tftp` directory, enter the subdirectory in the **Directory** field.

- d. To start the upload, click **Upload File**.

The Status area indicates when the file uploads successfully.

- e. After the file uploads, restart the Cisco TFTP service.



Note If you plan to upload several files, restart the Cisco TFTP service only once, after you have uploaded all the files.

For information about restarting services, refer to *Cisco Unified Serviceability Administration Guide for Cisco Unified Expert Advisor*.

- Step 3** To delete files, follow this procedure:

- a. Check the check boxes next to the files that you want to delete.

You can also click **Select All** to select all of the files, or **Clear All** to clear all selection.

- b. Click **Delete Selected**.
-



CHAPTER 8

Services

This chapter describes the utility functions that are available on the operating system, which include pinging another system and setting up remote support.

Ping

The Ping Utility window enables you to ping another server in the network.

To ping another system, follow this procedure:

Procedure

- Step 1** From the Cisco Unified Operating System administration console window, navigate to **Services > Ping**. The Ping Remote window displays.
- Step 2** Enter the IP address or network name for the system that you want to ping.
- Step 3** Enter the ping interval in seconds.
- Step 4** Enter the packet size.
- Step 5** Enter the ping count, the number of times that you want to ping the system.



Note When you specify multiple pings, the ping command does not display the ping date and time in real time. Be aware that the Ping command displays the data after the number of pings that you specified completes.

- Step 6** Choose whether you want to validate IPsec.
 - Step 7** Click **Ping**.
The Ping Remote window displays the ping statistics.
-

Remote Support

From the Remote Account Support window, you can set up a remote account that Cisco support personnel can use to access the system for a specified period of time.

The remote support process works like this:

1. The customer sets up a remote support account. This account includes a configurable time limit on how long Cisco personnel can access it.
2. When the remote support account is set up, a pass phrase gets generated.
3. The customer calls Cisco support and provides the remote support account name and pass phrase.
4. Cisco support enters the pass phrase into a decoder program that generates a password from the pass phrase.
5. Cisco support logs into the remote support account on the customer system by using the decoded password.
6. When the account time limit expires, Cisco support can no longer access the remote support account.

To set up remote support, follow this procedure:

Procedure

- Step 1** From the Cisco Unified Operating System administration console window, navigate to **Services > Remote Support**.

The Remote Access Configuration window displays.

- Step 2** Enter an account name for the remote account and the account life in days.



Note Ensure the account name is at least six-characters long and is all lowercase, alphabetic characters.

- Step 3** Click **Save**.

The Remote Support Status window displays. For descriptions of fields on the Remote Support Status window, see [Table 8-1](#).

Table 8-1 Remote Support Status Fields and Descriptions

Field	Description
Decode version	Indicates the version of the decoder in use.
Account name	Displays the name of the remote support account.
Expiration	Displays the date and time when access to the remote account expires.
Pass phrase	Displays the generated pass phrase.

- Step 4** To access the system by using the generated pass phrase, contact your Cisco personnel.

- Step 5** To delete the remote access support account, click the **Delete** button.



GLOSSARY

The *Glossary for the Cisco Unified Expert Advisor* document is specific to the Cisco Unified Expert Advisor documentation set and explains the commonly-used terms in the context of this product.



Note

This document may not represent the latest Cisco product information available. You can obtain the most current documentation by accessing Cisco's product documentation page at this URL:

<http://www.cisco.com/go/ea>

- [A](#)
- [B](#)
- [C](#)
- [D](#)
- [E](#)
- [F](#)
- [H](#)
- [I](#)
- [L](#)
- [M](#)
- [N](#)
- [O](#)
- [P](#)
- [R](#)
- [S](#)
- [T](#)
- [U](#)
- [V](#)
- [W](#)
- [X](#)

A

ACD

Automatic Call Distributor. A feature that automatically routes incoming calls to an agent or attendant in accordance with a set of configurable rules such as longest idle [agent](#).

ACL

Access Control List. In the incoming ACL, you can configure patterns that control which hosts and domains can access Cisco Unified Presence.

Active Directory

Active Directory. For [expert\(s\)](#) to be able to search the directory for other users, add users to their contact lists, and place calls to other users from Cisco Unified Personal Communicator, you must configure an [LDAP](#) server, or Active Directory server that supports [LDAP](#). The Active Directory implementation is also used to authenticate Cisco Unified Expert Advisor [administrators](#).

active server

The active server makes global decisions for the [cluster](#) and keeps track of calls, expert states, and historical detail [records](#). The active server provides all system services and resources. Only one server in the [cluster](#) can be the active server at any given time. Which server is active is determined by which of the two servers has an active connection to the [Unified Gateway](#). If the active server fails, the system automatically fails over to the [standby server](#). Both servers are synchronized when administrative changes are made on the active server.

administrator

During the [Cisco Unified Expert Advisor](#) installation, you specify two administrator accounts (user name/password):

- The [super user](#) (or application administrator): can access the serviceability web pages and perform daily management functions (such as adding and maintaining [assignment queues](#), [agents](#), [skill groups](#), [message sets](#), and [attributes](#)).
- The platform administrator: can access OS administration and DRS web pages, as well as the CLI. You can create additional platform administrators from the CLI.

See the *Installation Guide for Cisco Unified Expert Advisor* for more information.

agent

An agent generally refers to the formal contact center agent who initially handled an incoming customer call and transfers it to the [expert\(s\)](#).

In the reporting context, an agent interchangeably refers to the [expert\(s\)](#).

alarm

Signals that declare the run-time status and state of the [Cisco Unified Expert Advisor](#) system and provide information for troubleshooting. Alarms can be forwarded to a [syslog](#) server, to an [SNMP agent](#), or to a [log file](#) for an [event](#).

alarm catalog

A file that contains alarms definitions.

alarm definition

A list of alarms and their properties. The definition for each alarm includes the alarm name, a description, an explanation, recommended actions, and related information.

alarm message

An alarm name followed by the reason for the alarm or the module name.

alarm service

A service that receives alarms from the [Cisco Unified Expert Advisor](#) and its [subsystems](#).

AMC

Alert Manager and Collector (AMC). The Cisco AMC service logs the server data in [CSV](#) format. The header of the log comprises the time zone information and a set of columns with the previous counters for a [Cisco Unified Expert Advisor](#) node. These sets of columns repeat for every node.

The ServerDown alert is generated when the currently “active” AMC (primary AMC or the backup AMC, when the primary is not available) cannot reach another [node](#) in a [cluster](#). This alert identifies network connectivity issues in addition to a ServerDown condition.

application

In general, an application is a program that helps you accomplish a specific task; for example, a word processing program, a spreadsheet program, or an FTP client. On a Cisco Unified Expert Advisor runtime or reporting server, the Cisco Unified Expert Advisor application runs on the [Cisco Unified Operating System](#).

In [Cisco Unified Expert Advisor](#), application is an internal object that is created every time an [assignment queue](#) is created. The name of each application is autogenerated and is prepended with APP_. A separate instance of each application is created for each [assignment queue](#), as the script values may differ.

application user

During the installation, an application user is created on the Application User Configuration screen. The installation passes the user name and password for this application user to the User Management screen in the Cisco Unified Expert Advisor [operations console](#). This user becomes the default Cisco Unified Expert Advisor [super user](#).

assignment queue

Assignment queues handle the assignment of contacts to resources. Assignment queues are used to match [expert\(s\)](#) with incoming contact requests. Assignment queues have a one-to-one relationship with [skill groups](#). When an assignment queue is created on the [Cisco Unified Expert Advisor](#) system, a skill group is also created and tied to the assignment queue.

A skill group is the [Unified ICM](#) concept (and object) that corresponds to an [assignment queue](#) in [Cisco Unified Expert Advisor](#).

attributes

Attributes are customizable [variables](#) associated with [expert\(s\)](#) and contacts. You can create resource attributes and associate them with [expert\(s\)](#), then use those attributes to match [expert\(s\)](#) with [assignment queues](#). You can also map contact attributes from Unified ICM [ECC](#) variables, [Unified ICM](#) call variables, or [SIP](#) header variables to attributes in [Cisco Unified Expert Advisor](#).

auto-configuration

Auto-configuration occurs when certain data are pulled from the [EADB](#) and uploaded to the [Unified ICM](#) database. This is a function of the [Unified Gateway](#), which also tracks configuration changes on the [Cisco Unified Expert Advisor](#) and uploads those changes to keep the databases synchronized.

Automatic Call Distribution

See [ACD](#).

Automatic failover

If the [active server](#) fails, the [Cisco Unified Expert Advisor](#) application provides automatic failover to the [standby server](#). After a failover the [high availability runtime server](#) becomes the active server, and the primary (when it comes up again) becomes the [standby server](#). Both servers are synchronized when administrative changes are made on the [active server](#). The system uses database replication to copy the data automatically from the [active server](#) to the [standby server](#).

B**broadcast notice**

A broadcast notice is a request sent to one or more [expert\(s\)](#) (based on the configuration in the [assignment queue](#)). When a broadcast notice is sent, the system sends the call to the first expert who accepts the request. The system then sends a *Task Cancelled* message to all other broadcast experts. No action is required by the expert(s) receiving a task cancellation message.

BRE

Business Rules Engine. The application object ([assignment queue](#)) maps the incoming address to a BRE script to be executed.

C**CA**

Certificate Authority (CA). You can import the server authentication certificate that the CA provides for each [server](#) in the [cluster](#). Cisco recommends that you import the certificates before using the [Trace & Log Central](#) option. You cannot change any data that displays for the certificate.

call control

The [Cisco Unified Expert Advisor](#) system uses [SIP](#) for call control. A call control feature refers to any new call, transferred call, or call that is placed on hold.

category

Categories allow you to organize objects in [RTMT](#), such as performance monitoring counters and devices. For example, the default category under performance monitoring, [RTMT](#) allows you to monitor six performance monitoring counters in graph format. If you want to monitor more counters, you can configure a new category and display the data in table format.

CDP

Cisco Discovery Protocol (CDP). Media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. CDP runs on all media that support SNMP, including LANs, Frame Relay, and ATM media.

Cisco Security Agent

Cisco Security Agent (CSA). This application detects and prevents security intrusion. It integrates with various Cisco products to provide a collaborative network and endpoint solution.

Cisco Unified Expert Advisor

Cisco Unified Expert Advisor is a product option within a unified contact center. It extends the contact center by allowing an “[expert\(s\)](#)” to handle certain incoming contacts. For example, there might be a situation where the contact center customer requires a discussion or advice from a specialist or [expert\(s\)](#). This expert is not a member of the formal contact center but agrees to be “on call” to provide consultation services.

Cisco Unified Expert Advisor Database

See [EADB](#).

Cisco Unified Contact Center Enterprise

Cisco Unified Contact Center Enterprise (Unified CCE), an integral component of the Cisco Unified Communications system, delivers a comprehensive solution that provides intelligent routing and call treatment with blending of multiple communication channels. It handles traditional ACD calls and functions as a virtual ACD. Capabilities of Unified CCE include intelligent multichannel contact routing, ACD functionality, network-to-desktop CTI, IVR integration, call queuing, and consolidated reporting.

Cisco Unified Communications Manager

The Cisco Unified Communications Manager (Unified CM) software extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, VoIP gateways, and multimedia applications.

Cisco Unified Intelligent Contact Management

See [Unified ICM](#)

Cisco Unified Operating System

You can perform many common system administration functions through the Cisco Unified Operating System. The Cisco Unified Operating System administration console for the Cisco Unified Expert Advisor application allows you to configure and manage the Cisco Unified Operating System.

For more information, see the *Cisco Unified Operating System Administration Guide for Cisco Unified Expert Advisor*.

CLI

Command Line Interface. The platform CLI provides a limited set of commands accessible from any of the server consoles or through a SSH session. These commands allow basic maintenance and failure recovery and also enable some system administration when the Cisco Unified Expert Advisor [operations console](#) online interface is unavailable. The [Cisco Unified Expert Advisor operations console](#) is enabled for login at the completion of the installation and is the primary interface for administering, configuring, and maintaining [Cisco Unified Expert Advisor](#).

cluster

A Cisco Unified Expert Advisor cluster deployment consists of two required (primary and [high availability](#)) servers and one optional (reporting) server running [Cisco Unified Expert Advisor](#). The first server you install is always the primary, or publisher, and all additional servers in the same cluster are considered subscribers.

components

Core components of the [Cisco Unified Expert Advisor](#) system include:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unified Presence Server
- Cisco Unified Contact Center Enterprise
- Cisco Unified Customer Voice Portal
- Microsoft Active Directory Server ([Active Directory](#))
- Optional LDAP Server ([LDAP](#))
- [IM client](#)
 - Cisco Unified Personal Communicator
 - IP Phone Messenger (IPPM)
 - Microsoft Office Communicator ([MOC](#))

contacts

A person needing help from a resource.

contact manager subsystem

The component ([subsystem](#)) responsible for handling contacts. This subsystem orchestrates the interaction of a contact from the time the contact begins interacting with [Cisco Unified Expert Advisor](#) until the interaction has completed.

CSA

See [Cisco Security Agent](#).

CSV

Comma-Separated Values (CSV).

D

DHCP

Dynamic Host Configuration Protocol (DHCP). The IP Settings window indicates whether DHCP is active and provides the related Ethernet IP addresses, as well as the IP address for the network gateway.

DNS

Domain Name System (DNS) is an internet directory service which translates domain names into IP addresses. The DNS service is defined during the [Cisco Unified Expert Advisor](#) installation.

drawer

The left panel of the Cisco Unified Expert Advisor [operations console](#) uses the visual concept of a drawer as a container for related system functions. Similar to a menu, a drawer allows access to one or more utilities that have similar purposes or similar user permissions.

DRF

Disaster Recovery Framework (DRF) which provides the customer interface for the disaster recovery process. DRF itself, does not backup or restore any data—it merely provides a user interface and set of tools/utilities to perform different disaster recovery tasks

DRS

The Disaster Recovery System (DRS), which can be invoked from [Cisco Unified Expert Advisor operations console](#), provides full data backup and restore capabilities for all servers in the [cluster](#). The DRS allows you to perform regularly scheduled, automatic or user-invoked data backups.

The DRS performs a cluster-level backup, which means that it collects backups for all servers in a Cisco Unified Expert Advisor [cluster](#) to a central location and archives the backup data to physical storage device.

E

EADB

[Cisco Unified Expert Advisor](#) database (EADB), which stores configuration information for the entire system. This database is installed on all servers in the Cisco Unified Expert Advisor [cluster](#).

ECC

Extended Call Contact (ECC). ECC variables are specific to [Unified ICM](#). The Contact Attribute Sources page in the Cisco Unified Expert Advisor [operations console](#) allows you to map external call variables, such as [Unified ICM](#) ECC variables, to the [Cisco Unified Expert Advisor](#) system attributes.

event

An occurrence that is significant to an application and that may call for a response from the application.

Excel (XLS) format

Format of data in the Microsoft Excel spreadsheet application.

expert(s)

[Cisco Unified Expert Advisor](#) is an optional feature for Cisco Unified Contact Center. It extends the contact center to allow an *expert advisor* to handle certain incoming calls. An expert advisor is a specialist who is not employed by the contact center—but who agrees to be 'on call' to provide services as a consultant.

Experts establish their presence and availability to take a contact by the state of their [IM client](#).

F**firewall**

A firewall is a set of related programs that protect the resources of a network by examining (screening) each network packet to determine whether to forward it toward its destination. For [Cisco Unified Expert Advisor](#), only ports and protocols that are specifically named will be allowed by the firewall.

fault tolerance

Fault tolerance differs based on the [server](#) in question:

- **active server failure:** When a failure condition is encountered, whether in a [subsystem](#) of the [active server](#), in the [Unified Gateway](#), or in the communication path between servers, the standby server assumes control. This should result in little or no disruption to the call center expert advisor operation.
- **standby server failure:** There is no effect on call center operations, except that the standby server will not be able to take control if the [active server](#) has also failed.
- **reporting server failure:** When the [reporting server](#) fails, you will not be able to run Historical reports. Like the [runtime server](#), the [reporting server](#) is also integrated in the [DRF](#) for backup and restore functions.

field

A field is an item in a database [record](#) and is also referred to as a database field. For example, name, city, or zip code. A group of fields make up a [record](#).

H**high availability**

With high availability, if an [active server](#) becomes unavailable, the [standby server](#) immediately and automatically becomes the [active server](#). Both [runtime servers](#) must be in the same location as the corresponding [Unified Gateway](#) on a connected LAN.

high availability runtime server

The [high availability](#) server (also referred to as a [runtime server](#) or [standby server](#) or secondary server) is one of the servers installed in the [cluster](#).

HRDB

Historical database (HRDB), which stores data used in the historical reporting templates as well as system tables for the [reporting server](#). This database is installed on the [reporting server](#) only.

IM

Instant Messaging (IM) is used to notify [expert\(s\)](#) about an incoming task request. The [expert\(s\)](#) respond to the IM by accepting or rejecting the request (if configured with the required permissions); the expert can also provide an alternate phone number at which to be called.

IM client

The IM client effectively serves as the “desktop” for [expert\(s\)](#), who establish their willingness to take a contact by responding to an IM contact request from the [Cisco Unified Expert Advisor](#) system.

Informix

Informix is a relational database management system used by the CUEA databases.

LDAP

Lightweight Directory Access Protocol. An application protocol for querying and modifying directory services running over TCP/IP.

For [expert\(s\)](#) to be able to search the directory for other users, add users to their contact lists, and place calls to other users from Cisco Unified Personal Communicator, you must configure an LDAP server, or [Active Directory](#) server that supports LDAP.

license

The [Cisco Unified Expert Advisor](#) includes five free seats. These five seats are referred to as the default license. When completing the initial configuration, you can optionally upload the license that you additionally purchase. If you do not upload any additional purchased license, the five free seats are used by default.

localization

Localization is the process of adapting a product or service to a particular language and culture. This includes idiomatic language translation and details as time zones and currency. [Cisco Unified Expert Advisor](#) has been localized for more than a dozen languages.

log file

A file that keeps track of the activity of a computer or an application.

LPM

Log Partition Monitor (LPM). The LPM monitors the current log file partition disk usage and purges files when the log partition high water mark is exceeded.

local agent

The server has a local agent to perform backup and restore functions. Each server in a Cisco Unified Expert Advisor [cluster](#), including the server that contains the [master agent](#), must have its own local agent to perform backup and restore functions for its server. By default, a local agent automatically gets activated on each server in the [cluster](#). The local agent runs backup and restore scripts on each server in the [cluster](#).

M**master agent**

The master agent stores backup data on a locally attached tape drive or a remote network location. The master agent maintains a complete set of scheduled tasks in the database. When it receives updates from the user interface, the master agent sends executable tasks to the applicable local agents, as scheduled ([local agents](#) execute immediate-backup tasks without delay). You access the master agent through the DRS user interface to perform activities such as configuring storage locations, scheduling backups by adding new backup schedules, viewing or updating an existing schedule, displaying status of executed schedules, and performing system restoration.

message set

A group of messages by language and client format type. Messages from message sets are sent to and/or received from [expert\(s\)](#).

MIB

Management Information Base (MIB). Database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a graphical user interface network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MOC

Microsoft Office Communicator (MOC). Microsoft's instant messaging and presence client. It can be used with Unified Expert Advisor as an IM client. Unified Expert Advisor supports either Cisco Unified Personal Communicator clients or MOC clients, but not both in the same installation.

MTU

Maximum Transmission Unit (MTU). All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The MTU on Eth0 defaults to 1500.

N

NAT

Network Access Translation (NAT). To use the Trace & Log Central feature in the [RTMT](#), make sure that [RTMT](#) can access the server directly without NAT. If you have set up a NAT to access devices, configure the [Cisco Unified Expert Advisor](#) with a host name instead of an IP address and make sure that the host names and their routable IP address are in the [DNS](#) server or host file.

NIC

Network Interface Card (NIC). Each [server](#) in the [cluster](#) is required to have a NIC. The NIC is configured during installation for two connection settings: speed and duplex.

node

See [server](#).

The term node and [server](#) are used interchangeably in this document and refer to a computer that provides services or resources to other computers (called clients) connected to it through a network.

NTP

Network Time Protocol (NTP). You can only configure the NTP server settings on the first Cisco Unified Expert Advisor [publisher](#). After deleting, modifying, or adding a NTP server, you must restart all the other [nodes](#) in the [cluster](#) for the changes to take affect.

O

OAMP tasks

Operations, Administration, Maintenance, and Provisioning tasks

OCS

Microsoft Office Communication Server (OCS).

operations console

The web-based user interface that runs on the primary [runtime server](#) and allows you to perform OAMP tasks on multiple [servers](#) in a Cisco Unified Expert Advisor [cluster](#).

P

pane

A part of a window that is devoted to a specific function.

partition

Cisco Unified Expert Advisor software creates three partitions during each installation: an active bootable partition, an inactive bootable partition, and a common partition. A fresh (first-time) installation places the new Cisco Unified Expert Advisor software and operating system on the active partition. The system boots up and operates on the active partition.

PG

Peripheral Gateways (PG). The Unified ICM central controller communicates with each peripheral through a monitoring node referred to as the PG. Unified ICM software has a unique PG for each device it supports. Unified ICM treats Cisco Unified Expert Advisor as a peripheral. The primary runtime server and the high availability runtime server each connect with Unified CM with a dedicated Unified Gateway.

ports

In a communications network, a logical channel is identified by its unique port number.

post-routing

Process of making a routing decision after a call reaches a termination point.

pre-routing

Process of making a routing decision before a call reaches a termination point.

primary runtime server

The primary server (also referred to as a runtime server or a publisher or active server) in the Cisco Unified Expert Advisor cluster. This is the first runtime server installed in a cluster.

After a failover the high availability runtime server becomes the active server, and the primary (when it comes up again) becomes the standby server.

prompts

A message from a computer that asks the operator to do something, such as enter a command, enter a password, or enter data, or that indicates that the computer is ready to accept input.

publisher

The primary runtime server is also referred to as a publisher as it publishes (replicates) the OAMP configuration data in the Cisco Unified Expert Advisor cluster.

In Cisco Unified Expert Advisor, the terms publisher and subscriber are used in the context of database replication. The Cisco Unified Expert Advisor publisher (primary runtime server) publishes OAMP configuration data. The Cisco Unified Expert Advisor subscribers (high availability and reporting servers) subscribe to the data.

purge

To delete both a set of data and all references to the data.

R

Real-Time Monitoring Tool

See [RTMT](#).

record

In a database, a group of [fields](#) that make up one complete entry is called a record (or database record). For example, a record about a customer might contain fields for name, address, and telephone number.

reporting adapter

The reporting adapter is the software subsystem in each runtime server which forwards reporting events to the reporting server.

reporting server

The reporting server is added as a subsequent server in a Cisco Unified Expert Advisor [cluster](#) (also referred to as [subscribers](#)). The reporting server, also referred to as the historical reporting server, is an optional server.

reporting user

Cisco Unified Expert Advisor reporting users are created in the Cisco Unified Expert Advisor [operations console](#) after the installation. They have read-only access to the Reporting database and can generate reports using the Cisco predefined templates.

See also [super user](#) and [administrator](#).

resource

A person or automaton (for example, a self-service prompt/response) that can provide help to a Contact.

RISDC

Real-time Information Server Data Collection (RISDC). Cisco Unified Expert Advisor collects system performance information that is written on the Cisco Unified Expert Advisor [server](#). You can use this performance data to troubleshoot problems. By default, RISDC perfmon logging gets enabled. Be aware that RISDC perfmon logging is also known as Troubleshooting Perfmon Data logging.

RTMT

The Real-Time Monitoring Tool (RTMT) for [Cisco Unified Expert Advisor](#), which runs as a client-side application, uses HTTPS and TCP to monitor system performance and device status for Cisco Unified Expert Advisor. RTMT can connect directly to devices via HTTPS to troubleshoot system problems.

runtime server

The [primary runtime server](#) is also referred to as a runtime server or a [publisher](#) or [active server](#). This is the first runtime server installed in a [cluster](#). If the [primary runtime server](#) fails, you cannot configure the system.

S

scheduler

A program that resides on a Cisco Unified Expert Advisor [reporting server](#). The Scheduler maintains information about each scheduled report, including when the report should execute and what information the report should contain. The scheduler also executes scheduled reports at their scheduled times, based on the time and date of the [reporting server](#).

schedule backups

A Cisco Unified Expert Advisor [administrator](#) can schedule backups at predesignated times. [DRS](#) includes a comprehensive scheduling system which provides the ability to backup one time, daily, weekly, or monthly.

script

A sequence of steps constructed to control the flow of a call. Scripts are sometimes also called *flows*, *call flows*, or *work flows*.

server

See [node](#).

A computer that belongs to a [cluster](#). A server is also referred to as a [node](#). The term [node](#) and server are used interchangeably in the Cisco Unified Expert Advisor documentation set.

service

A program, routine, or process that performs a specific system function to support other programs, particularly at a low (close to the hardware) level.

serviceability

Generally, *serviceability* refers to the collection tools and mechanisms by which a customer, partner, or technical assistance engineer can service the product. In a Cisco Unified Expert Advisor system, some of those tools are contained in the Serviceability drawer in the Cisco Unified Expert Advisor system's operations console, and some are in the Cisco Unified Serviceability for Cisco Unified Expert Advisor application. This application is available from the Navigation dropdown list in the upper right corner of the operations console.

session (historical reporting)

Historical reporting seats are also called historical reporting sessions. Historical reporting sessions (seats) refer to the number of historical reporting clients that can be started at the same time on different client machines.

SFTP server

Secure File Transfer Protocol (SFTP) server. You must have an SFTP server configured in order to back up data to a remote network device. You must have access to an SFTP server to configure a network storage location. The SFTP path must exist prior to the backup. The account that is used to access the SFTP server must have write permission for the selected path.

You may use any SFTP server:

- Open SSH (for Unix systems)
- Cygwin (refer to <http://sshtwindows.sourceforge.net/>)
- freeFTPD (refer to <http://www.freeftpd.com/?ctt=download>)

SFTP network location

A SFTP network location to store backup is specified as a remote server. This server is not one of [node](#) in a Cisco Unified Expert Advisor [cluster](#). The server must have sufficient disk space to hold one or more backups. This network storage server can be Windows or Linux based.

SIP

Session Initiation Protocol. A peer-to-peer, multimedia signaling protocol developed in the IETF. SIP is ASCII-based, resembling HTTP, and reuses existing IP protocols ([DNS](#), [SDP](#), etc.) to provide media setup and tear down.

You may need to create a SIP Trunk on Cisco Unified Communications Manager so that the Unified Presence server can communicate with Cisco Unified Communications Manager. Optionally, you may need to configure Unified CVP to use an outbound SIP proxy to send all SIP-based calls to the Cisco Unified Presence Server to take advantage of static routes.

skill group

When you create an [assignment queue](#) in the [Cisco Unified Expert Advisor](#) system, the system automatically creates a corresponding skill group in [Unified ICM](#). A skill group automatically configured in [Unified ICM](#) is marked in Unified ICM as “used by peripheral”. Such items cannot be edited using the Unified ICM configuration tools. If you later delete that [assignment queue](#), once the [auto-configuration](#) operation completes, Unified ICM removes the “used by peripheral” flag, but it does not delete the skill group. The skill group, along with any subordinate objects and references from other objects, remains intact and can only be deleted manually.

A skill group is the [Unified ICM](#) concept (and object) that corresponds to an [assignment queue](#) in [Cisco Unified Expert Advisor](#).

SMTP

SimpleMail Transfer Protocol (SMTP). When you install Cisco Unified Expert Advisor, you can choose to configure an optional SMTP host for outbound e-mail. If you want the system to send you e-mail, you must configure an SMTP host. The SMTP Settings window in the Cisco Unified Operating System administration console allows you to view or set the SMTP host name and indicates whether the SMTP host is active.

SNMP

Simple Network Management Protocol (SNMP). The standard protocol for network management software. Using SNMP, programs called [SNMP agents](#) monitor devices on the network. The database created by the monitoring operations is called a [MIB](#).

SNMP agent

Hardware or software that monitors devices on a network. Data from an [SNMP](#) agent, which is contained in a [MIB](#), helps in network management and troubleshooting.

SNMP service

An operating system service that provides a framework for [SNMP](#) and provides the [SNMP agent](#) that interfaces with [SNMP subagents](#).

SNMP subagent

Cisco provides SNMP subagents to support each [MIB](#). The [SNMP](#) service loads the [SSNMP subagent](#) and it exchanges [SNMP](#) messages with the [SNMP subagent](#). The SNMP service formats information as [MIBs](#) and sends this information to a Network Management System (NMS). It also sends traps from the [SNMP subagent](#) to the appropriate [SNMP](#) trap receivers.

standby server

You must deploy at least two servers in each Cisco Unified Expert Advisor [cluster](#) for [high availability](#): one [active server](#) (master) and one standby (not active) server. The non-active server will be in PARTIAL-SERVICE.

subscriber

Subsequent servers in the Cisco Unified Expert Advisor [cluster](#) are referred to as subscribers. These servers include the secondary [runtime server](#) and the [reporting server](#).

In Cisco Unified Expert Advisor, the terms [publisher](#) and subscriber are used in the context of database replication. The Cisco Unified Expert Advisor [publisher](#) (primary server) publishes OAMP configuration data. The Cisco Unified Expert Advisor subscribers ([high availability](#) and [reporting servers](#)) subscribe to the data.

subsystem

A subsystem is an extensible modular development environment that performs a particular function. In the context of Cisco Unified Expert Advisor, each subsystem has a specific set of responsibilities which when joined together create Cisco Unified Expert Advisor functionalities such as Resource Manager, Contact Manager and Work Assigner.

super user

The application user defined in the installation wizard becomes the default [Cisco Unified Expert Advisor](#) super user. The super user has access to all Daily Management and system level features, such as installing upgrades. The default super user can create additional users from the [Cisco Unified Expert Advisor](#) operations console. These additional users include additional super users, other administrators (who have no access to system-level functions), and [reporting users](#).

See the *Installation Guide for Cisco Unified Expert Advisor* for more information.

See also [administrator](#).

syslog

A Cisco standard that allows for logging of errors across an enterprise. Provides local logging of network [events](#) to files. Also provides remote logging to various systems via standard protocols.

system

The Cisco Unified Expert Advisor system is referred to as *system*.

T

table (also database table)

A presentation of information organized in rows and columns.

tape device

A tape device is a USB-based external device such as a Digital Linear Tape (DLT) backup solution.

TFTP

Trivial File Transfer Protocol. A simple file transfer protocol used to transfer small files between hosts on a network.

trace route

A TCP/IP utility that allows you to determine the route packets are taking to a particular host. Trace route works by increasing the “time to live” value of packets and seeing how far they get, until they reach the given destination.

Trace & Log Central

Trace and Log Central is part of the RTMT for the [Cisco Unified Expert Advisor](#). It is used to manage and collect trace and log files from the Cisco Unified Expert Advisor [servers](#).

translation routing

Translation routing is a process that ensures that the association between a call and its related data is maintained throughout the life of the call.

trap (also SNMP trap)

A program interrupt, usually caused by some exceptional situation in an application. In most cases, after such an interrupt, the operating system performs some action, then returns control to the application.

U

Unified Gateway

The Unified Gateway is a [PG](#) which you configure on the [Unified ICM](#) software. The Unified Gateway provides for the integration of the [Unified ICM](#) system with [Cisco Unified Expert Advisor](#).

Unified ICM

[Cisco Unified Intelligent Contact Management](#). The Unified Contact Center component that is responsible for making routing decisions and performing ACD functions.

USB drive

Universal Serial Bus (USB) drive is a data storage device integrated with a USB connector. [Cisco Unified Expert Advisor](#) supports the use of a USB drive for downloading and storing configuration data.

V**variable**

A placeholder for data.

W**wizard**

A wizard is a computer utility designed to lead you through the execution of tasks. [Cisco Unified Expert Advisor](#) uses wizards for installation and for initial configuration.

X**XML**

Extensible Markup Language. A programming language developed by the World Wide Web Consortium (W3C) that allows Web developers to create customized tags that will organize and deliver efficiently. XML is a metalanguage, containing a set of rules for constructing other markup languages.



INDEX

A

administrator password [2-2](#)

B

browser requirements [1-2](#)

C

certificates

deleting [6-3](#)

displaying [6-2](#)

downloading [6-2](#)

downloading a signing request [6-5](#)

expiration monitor fields (table) [6-6](#)

managing [6-1](#)

monitoring expiration dates [6-6](#)

regenerating [6-3](#)

uploading [6-4](#)

Certificate Trust List

See CTL

cluster nodes

fields (table) [3-1](#)

procedure [3-1](#)

configuration

operating system [1-2, 3-1](#)

CTL

downloading [6-2](#)

managing [6-1](#)

uploading [6-4](#)

E

Ethernet settings [4-1](#)

H

hardware, status

fields (table) [3-2](#)

procedure [3-2](#)

I

install/upgrade, menu [1-3](#)

installed software

fields (table) [3-4](#)

procedure [3-3](#)

Internet Explorer

set security options [6-1](#)

IPSec

changing policy [6-9](#)

displaying policy [6-9](#)

management [6-7](#)

policy fields (table) [6-7](#)

setting up new policy [6-7](#)

L

logging in

overview [2-1](#)

procedure [2-1](#)

M

menu
 install/upgrade [1-3](#)
 security [1-3](#)
 settings [1-2](#)
 show [1-2](#)

N

network status
 fields (table) [3-3](#)
 procedure [3-2](#)

nodes, cluster
 fields (table) [3-1](#)
 procedure [3-1](#)

NTP server settings [4-3](#)

O

operating system
 administrator password [2-2](#)
 browser requirements [1-2](#)
 configuration [1-2,3-1](#)
 hardware status
 fields (table) [3-2](#)
 procedure [3-2](#)
 introduction [1-1](#)
 logging in [2-1](#)
 network status fields (table) [3-3](#)
 overview [1-1](#)
 restart [5-2](#)
 security [1-3](#)
 services [1-3](#)
 settings [1-2,4-1](#)
 software upgrades [1-3](#)
 status [1-2,3-1](#)

P

password, recovering [2-2](#)
 ping [8-1](#)
 publisher settings [4-2](#)

R

remote support
 setting up [8-1](#)
 status fields (table) [8-2](#)

restart
 current version [5-2](#)
 system [5-1](#)

S

security
 configuration [1-3](#)
 menu [1-3](#)
 overview [6-1](#)
 set IE options [6-1](#)

services
 overview [8-1](#)
 ping [1-3,8-1](#)
 remote support [1-3](#)
 overview [8-1](#)
 setting up [8-1](#)

settings
 Ethernet
 fields (table) [4-2](#)
 procedure [4-1](#)
 IP [4-1](#)
 menu [1-2](#)
 NTP servers [4-3](#)
 overview [4-1](#)
 publisher [4-2](#)
 SMTP [4-4](#)
 time [4-4](#)

show, menu [1-2](#)
shutdown, operating system [5-2](#)
SMTP settings [4-4](#)
software
 installation [7-1](#)
 installed
 fields (table) [3-4](#)
 procedure [3-3](#)
 upgrades [1-3](#)
 from local source [7-2](#)
 from remote source [7-3](#)
 overview [7-1](#)
 procedure [7-1](#)
status
 hardware
 fields (table) [3-2](#)
 procedure [3-2](#)
 network
 fields (table) [3-3](#)
 procedure [3-2](#)
 operating system [1-2, 3-1](#)
 system
 fields (table) [3-4](#)
 procedure [3-4](#)
system
 restart [5-1](#)
 shutdown [5-2](#)
 status
 fields (table) [3-4](#)
 procedure [3-4](#)

V

version, restart [5-2](#)

T

TFTP server, installing files [7-5](#)
time settings [4-4](#)

