Administration Overview

Cisco Unified CM Administration Overview

Cisco Unified CM Administration, a web-based application, is the main administration and configuration interface for Cisco Unified Communications Manager. You can use Cisco Unified CM Administration to configure a wide range of items for your system including general system components, features, server settings, call routing rules, phones, end users, and media resources.

Configuration Menus

The configuration windows for Cisco Unified CM Administration are organized under the following menus:

- System—Use the configuration windows under this menu to configure general system settings such as server information, NTP settings, Date and Time groups, Regions, DHCP, LDAP integration, and enterprise parameters.
- Call Routing-—Use the configuration windows under this tab to configure items related to how Cisco Unified Communications Manager routes calls, including route patterns, route groups, hunt pilots, dial rules, partitions, calling search spaces, directory numbers, and transformation patterns.
- Media Resources—Use the configuration windows under this tab to configure items such as media resource groups, conference bridges, annunciators, and transcoders.
- Advanced Features—Use the configuration windows under this tab to configure features such as voice-mail pilots, message waiting, and call control agent profiles.
- Device—Use the configuration windows under this tab to set up devices such as phones, IP phone services, trunks, gateways, softkey templates, and SIP profiles.
- Application—Use the configuration windows under this tab to download and install plug-ins such as Cisco Unified JTAPI, Cisco Unified TAPI, and the Cisco Unified Real-Time Monitoring Tool.

- User Management—Use the configuration windows under the User Management tab to configure end users and application users for your system.
- Bulk Administration-—Use the Bulk Administration Tool to import and configure large numbers of end users or devices at a time.
- Help—Click this menu to access the online help system. The online help system contains documentation that will assist you in configuring settings for the various configuration windows on your system.

Operating System Administration Overview

Use Cisco Unified Communications Operating System Administration to configure and manage your operating system and perform the following administration tasks:

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

Operating System Status

You can check the status of various operating system components, including the following:

- Clusters and nodes
- Hardware
- Network
- System
- Installed software and options

Operating System Settings

You can view and update the following operating system settings:

- IP—Updates the IP addresses and DHCP client settings that ypu entered when the application was installed.
- NTP Server settings—Configures the IP addresses of an external NTP server; adds an NTP server.
- SMTP settings—Configures the simple mail transfer protocol (SMTP) host that the operating system will use for sending email notifications.

Operating System Security Configuration

You can manage security certificates and IPsec settings. From the **Security** menu, you can choose the following security options:

- Certificate Management—Manages certificates and certificate signing requests (CSRs). You can display, upload, download, delete, and regenerate certificates. Through certificate management, you can also monitor the expiration dates of the certificates on the node.

- IPsec Management—Displays or updates existing IPsec policies; sets up new IPsec policies and associations.

Software Upgrades

You can upgrade the software version that is running on the operating system or to install specific software options, including Cisco Unified Communications Operating System locale installers, dial plans, and TFTP server files.

From the **Install/Upgrade** menu option, you can upgrade system software from either a local disc or a remote server. The upgraded software is 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. For more information, see the *Upgrade Guide for the Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Note You must perform all software installations and upgrades through the software upgrade features that are included in the Cisco Unified Communications Operating System interface and the CLI. The system can upload and process only software that is Cisco Systems approved. You cannot install or use third-party or Windows-based software applications.

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.

CLI

You can access the CLI from the Operating System or through a secure shell connection to the server. For more information, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Authenticated Network Time Protocol Support

With Cisco Unified Communications Manager release 12.0 (1), the authenticated Network Time Protocol (NTP) capability for Unified Communications Manager is supported. This support is added to secure the NTP server connection to Unified Communications Manager. In the previous releases, the Unified Communications Manager connection to the NTP server was not secure.

This feature is based on symmetric key-based authentication and is supported by NTPv3 and NTPv4 servers. Unified Communications Manager supports only SHA1-based encryption. The SHA1-based symmetric key support is available from NTP version 4.2.6 and above.

- Symmetric Key
- No Authentication

You can check the authentication status of the NTP servers through administration CLI or **NTP Server List** page of the **Cisco Unified OS Administration** application.

Auto Key Authenticated Network Time Protocol Support

Cisco Unified Communications Manager also supports Network Time Protocol (NTP) authentication through Auto-key functionality (Public Key Infrastructure- based authentication). This feature is applicable only on the publisher node.

Redhat recommends symmetric key authentication over autokey. For more information, see https://access.redhat.com/support/cases/#/case/01871532.

This feature is added, as PKI-based authentication is mandatory for Common Criteria certification.

You can configure the PKI-based authentication with the IFF identity scheme on the NTP server only if you enable common criteria mode on the Cisco Unified Communication Manager.

You can enable either symmetric key or PKI-based NTP authentication on Cisco Unified Communications Manager.

If you try to enable the symmetric key on the PKI enabled server, the following warning message is displayed:

Warning NTP authentication using Autokey is currently enabled and must be disabled before the symmetric key is enabled. Use the command 'utils ntp auth auto-key disable' to disable NTP authentication, then retry this command.

If you try to enable the Autokey on the symmetric key enabled server, the following warning message is displayed:

Warning NTP authentication using symmetric key is currently enabled and must be disabled before Autokey is enabled. Use the command 'utils ntp auth symmetric-key disable' to disable NTP authentication, then retry this command.

Note NTP servers require ntp version 4 and the rpm version ntp-4.2.6p5-1.el6.x86_64.rpm and above.

You can check the authentication status of the NTP servers through administration CLI or NTP Server List page of the Cisco Unified OS Administration application.

Cisco Unified Serviceability Overview

Cisco Unified Serviceability is a web-based troubleshooting tool that provides a host of services, alarms, and tools that assist administrators in managing their systems. Among the features that Cisco Unified Serviceability offers to administrators are:

- Start and Stop Services—Administrators can set up an assortment of services that help administrators manage their systems. For example, you can start the Cisco CallManager Serviceability RTMT service thereby allowing administrators to use the Real-Time Monitoring Tool to monitor the health of your system.

- SNMP—SNMP facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.
- Alarms—Alarms provide information on the runtime status and state of your system, so that you can troubleshoot problems that are associated with your system.
- Traces—Trace tools help you to troubleshooting issues with voice applications.
- Cisco Serviceability Reporter—The Cisco Serviceability Reporter generates daily reports in Cisco Unified Serviceability.
- SNMP—SNMP facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.
- CallHome—Configure the Cisco Unified Communications Manager Call Home feature, allowing Cisco Unified Communications Manager to communicate and send the diagnostic alerts, inventory, and other messages to the Smart Call Home back-end server

Additional Administrative Interfaces

Using Cisco Unified Serviceability, you can start services that allow you to use the following additional administrative interfaces:

- Real-Time Monitoring Tool—The Real-Time Monitoring Tool is a web-based interface that helps you to monitor the health of your system. Using RTMT, you can view alarms, counters and reports that contain detailed information on the health of your system.
- Dialed Number Analyzer—The Dialed Number Analyzer is a web-based interface that helps administrators to troubleshoot issues with the dial plan.
- Cisco Unified CDR Analysis and Reporting—CDR Analysis and Reporting collects call details records showing the details of the calls that are placed on your system.

For details about how to use Cisco Unified Serviceability, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Cisco Unified Reporting Overview

The Cisco Unified Reporting web application generates consolidated reports for troubleshooting or inspecting cluster data. You can access the application at the Unified Communications Manager and Unified Communications Manager IM and Presence Service consoles.

This tool provides an easy way to take a snapshot of cluster data. The tool gathers data from existing sources, compares the data, and reports irregularities. When you generate a report in Cisco Unified Reporting, the report combines data from one or more sources on one or more servers into one output view. For example, you can view the following reports to help you administer your system:

- Unified CM Cluster Overview—View this report to get a snapshot of your cluster, including Cisco Unified Communications Manager and IM and Presence Service versions, server hostnames, and hardware details.

- Phone Feature List—View this report if you are configuring features. This report provides a list of which phones support which Cisco Unified Communications Manager features.
- Unified CM Phones Without Lines—View this report to see which phones in your cluster do not have a phone line.

For a full list of reports offered through Cisco Unified Reporting, as well as instructions on how to use the application, see the *Cisco Unified Reporting Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Disaster Recovery System Overview

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified Communications Manager Administration, provides full data backup and restore capabilities. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups.

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up and restores the `drfDevice.xml` and `drfSchedule.xml` files. When the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup and restore functions.
- Scheduled backups.
- Archive backups to a physical tape drive or remote SFTP server.

Bulk Administration Tool Overview

In Cisco Unified CM Administration, uses the Bulk Administration menu and submenu options to configure entities in Unified Communications Manager through use of the Bulk Administration Tool.

The Unified Communications Manager Bulk Administration Tool (BAT), a web-based application, lets administrators perform bulk transactions to the Unified Communications Manager database. BAT lets you add, update, or delete a large number of similar phones, users, or ports at the same time. When you use Cisco Unified CM Administration, each database transaction requires an individual manual operation, while BAT automates the process and achieves faster add, update, and delete operations.

You can use BAT to work with the following types of devices and records:

- Add, update, and delete Cisco IP Phones, gateways, phones, computer telephony interface (CTI) ports, and H.323 clients
- Add, update, and delete users, user device profiles, Cisco Unified Communications Manager Assistant managers and assistants
- Add or delete Forced Authorization Codes and Client Matter Codes
- Add or delete call pickup groups
- Populate or depopulate the Region Matrix

- Insert, delete, or export the access list
- Insert, delete, or export remote destinations and remote destination profiles
- Add Infrastructure Devices

For details on how to use the Bulk Administration Tool, refer to the *Bulk Administration Guide for Cisco Unified Communications Manager*.