Documentation Supplement for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)SU1

First Published: July 07, 2016

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

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

PART I About the Release 1

CHAPTER 1 Introduction 3

About this Release 3

About this Guide 3

Documentation for this Release 4

CHAPTER 2 New and Changed Features 5

Enhanced Security Updates 5

Enhanced Security Mode 5

Rank Based Access Control 6

Remote Logging of Platform Logs using FileBeat 6

File Integrity Check 7

Maximum Session Limit CLI Update 7

User Interface Updates 7

APIC-EM Controller QoS Support 8

User Interface Updates for APIC-EM 8

New Alarms for APIC-EM Controller 9

Communication Updates for APIC-EM 9

PART II Documentation Updates 11

CHAPTER 3 Configure QoS with APIC-EM Controller 13

APIC-EM Controller Overview 13

APIC-EM Controller Prerequisites 14

APIC-EM Controller Configuration Task Flow 14

Upload APIC-EM Controller Certificate 15

Configure HTTPS Connection to APIC-EM Controller 15

Enable External QoS Service for System 16
Configure External QoS Service at SIP Profile Level 16
Assign SIP Profile to Phones 17
APIC-EM Feature Restrictions 18
Troubleshooting Tips for APIC-EM Controller 18

CHAPTER 4 Configure User Access 21
User Access Overview 21
Roles Overview 22
Access Control Group Overview 23
User Rank Overview 23
User Access Prerequisites 23
User Access Configuration Task Flow 24
Create a Custom User Rank 24
Create a Custom Role 25
Copy an Existing Role 26
Create Access Control Groups 26
Copy Access Control Group 27
Assign Roles to Access Control Group 28
Configure Overlapping Privilege Policy 29
Standard Roles and Access Control Groups 29

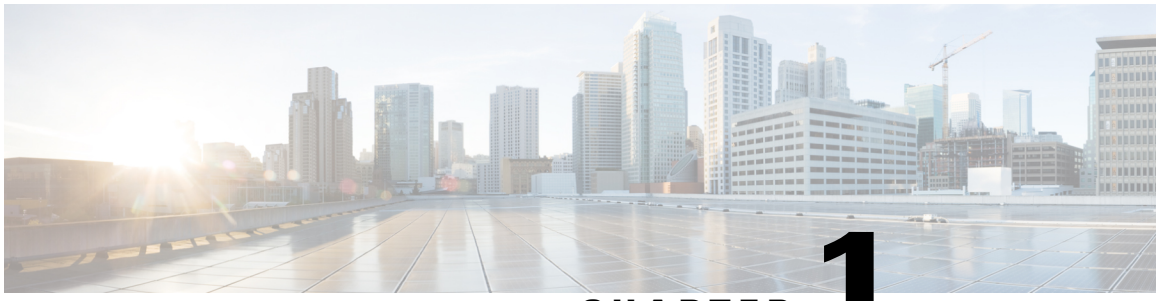
CHAPTER 5 Audit Logs 39
Audit Logs 39
Audit Logging (Standard) 39
Audit Logging (Detailed) 42
Audit Log Types 43
System Audit Logs 43
Application Audit Logs 43
Database Audit Logs 43
Audit Log Configuration Task Flow 43
Set up Audit Logging 44
Configure Remote Audit Log Transfer Protocol 44
Configure Email Server for Alert Notifications 45
Enable Email Alerts 45

Configure Remote Audit Logging for Platform Logs 46
Configure Logstash Server Information 46
Configure the FileBeat Client 47
Audit Log Configuration Settings 47

PART I

About the Release

- Introduction, page 3
- New and Changed Features, page 5



CHAPTER 1

Introduction

- About this Release, page 3
- About this Guide, page 3
- Documentation for this Release, page 4

About this Release

This Release Notes supplement covers Release 11.5(1)SU1 of Cisco Unified Communications Manager and IM and Presence Service. This release is a service update (SU) to the main 11.5(1) release and contains some additional features and fixes that are not in the main release.

The version numbers for the 11.5(1)SU1 are as follows:

- Cisco Unified Communications Manager version
- IM and Presence Service version

About this Guide

This guide contains information on the feature updates that are a part of Release 11.5(1)SU1 for Cisco Unified Communications Manager and IM and Presence Service. This guide supplements documentation for the main 11.5(1) release.

This book contains the following sections with updated documentation:

- New and Changed Features—This chapter summarizes the feature updates that are a part of Release 11.5(1)SU1.
- Documentation Updates—The chapters in this Part are revisions to existing chapters in the Release 11.5(1) documentation set. Each of these chapters replaces an existing chapter due to additional updates for this release.

Documentation for this Release

11.5(1)SU1 Documentation

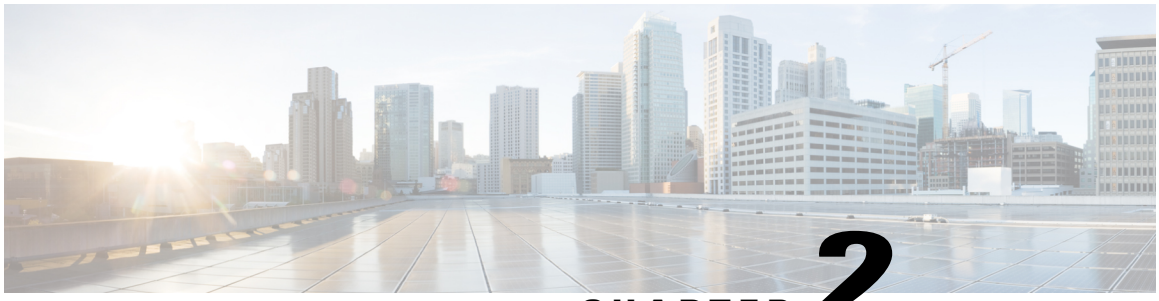
Release Notes Supplement—This supplement contains information on the new features that have been added to this service update (SU) release. The New and Changed Features chapter of this document summarizes the feature updates. In addition, the Documentation Updates chapter contains the full documentation updates for this release.

Readme File for Cisco Unified Communications Manager Release 11.5(1)SU1—Contains information on caveats, fixes, and important notes that are specific to this release.

Existing 11.5(1) Documentation

Release11.5(1)SU1 release is a service update (SU) to the main 11.5(1) release. The full set of documents for Cisco Unified Communications Manager and IM and Presence Service Release 11.5(1) can be used for this SU release as well. For 11.5(1) release, see the following documents:

- Documentation Guide—Contains information on the documentation set that is available for Release 11.5(1) of Cisco Unified Communications Manager and IM and Presence Service.
- Release Notes—Contains information on the New and Changed Features that are available in Release 11.5(1) of Cisco Unified Communications Manager and IM and Presence Service.



CHAPTER 2

New and Changed Features

- Enhanced Security Updates, page 5
- APIC-EM Controller QoS Support, page 8

Enhanced Security Updates

The following enhanced security updates have been added for this release:

- Enhanced Security Mode—A new system running mode that enables the system with a set of risk management controls, such as a stricter credential policy.
- Rank Based Access Control—A new user rank-based set of accces controls, which overlays the existing access control group framework.
- Remote logging for platform audit logs, remote support logs, and Bulk Administration csv files.
- File integrity protection—SHA512 checksums are available for all file downloads.
- Concurrent session limits—Applies to all interfaces.

Enhanced Security Mode

Cisco Unified Communications Manager and the IM and Presence Service can be enabled to operate in Enhanced Security Mode. When the system is enabled for Enhanced Security Mode, the system implements the following security and risk management controls:

- Stricter credential policy is implemented for user passwords and password changes
- Contact search authentication feature becomes enabled
- TCP becomes the default protocol for remote audit logging

Credential Policy Updates

When Enhanced Security Mode is enabled, a stricter credential policy takes effect for password changes:

- Password Length should be between 14 to 127 characters.

- Password should have at least 1 lowercase, 1 uppercase, 1 digit and 1 special character.
- Any of the previous 24 passwords cannot be reused.
- Minimum age of the password is 1 day and Maximum age of the password is 60 days.
- Any newly generated password's character sequence will need to differ by at least 4 characters from the old password's character sequence.

After Enhanced Security Mode is enabled, administrators can use the **set password ***** series of CLI commands to modify any of these requirements.

CLI Command Updates

To configure Enhanced Security Mode for Cisco Unified Communications Manager and IM and Presence Service, the following CLI commands are added:

- **utils EnhancedSecurityMode enable—**Run this command to enable a cluster node for Enhanced Security Mode. Do not run this command on all nodes simultaneously.
- **utils EnhancedSecurityMode disable—**Run this command to disable a cluster node for Enhanced Security Mode. Do not run this command on all nodes simultaneously.
- **utils EnhancedSecurityMode status—**Run this command to verify whether Enhanced Security Mode is enabled.

Rank Based Access Control

User Rank Access Control provides a set of controls over the level of access that an administrator can provide to an end user or application user. The **User Rank** parameter is a 1–10 integer with 1 being the highest possible rank. The user rank is assigned to both users and access control groups thereby creating a rank hierarchy that governs which users can be assigned to a particular access control group.

When provisioning end users or application users, administrators must assign a user rank for each user. Administrators must also assign a user rank to each access control group. Administrators can assign users to only those access control groups with the same or lower rank. For example, if an end user has a user rank of 3, they can be assigned to access control groups that have a user rank between 3 and 10. That user cannot be assigned to an access control group that requires a user rank of 1.

Administrators can customize user rank hierarchy within the **User Rank Configuration** window and then assign those ranks to end users, application users, and access control groups.

Remote Logging of Platform Logs using FileBeat

Release 11.5(1)SU1 adds remote audit logging support in real time for platform audit logs and remote support logs. Previously, these audit logs could be stored locally only. Cisco Unified Communications Manager and IM and Presence Service use the FileBeat client to upload these logs to an external logstash server. In addition, you can also use the FileBeat client to upload the csv files that the Bulk Administration Tool uses.

This feature allows you to upload these types of audit logs:

- Platform audit logs—These logs are saved locally in `/var/log/active/audit/vos-audit.logx`
- Remote support logs—These logs capture the activity of the remote support account. For example, `remote_activity.log_<timestamp>`

- csv files—FileBeat uploads to the logstash server the files that the Bulk Administration Tool uses.

New CLI Commands to Configure FileBeat

To use this feature, you must use CLI commands to configure the external logstash server and to enable uploads with the FileBeat client. The following commands are available for privilege level 4 admin users:

- **utils FileBeat configure**—Use this command to configure the FileBeat client with the external logstash server information.
- **utils FileBeat enable**—Use this command to enable uploads to an external logstash server. Do not run this command on all nodes simultaneously.
- **utils FileBeat disable**—Use this command to disable uploads to an external logstash server. Do not run this command on all nodes simultaneously.
- **utils FileBeat status**—Use this command to confirm whether the system is enabled or disabled for FileBeat uploads.

File Integrity Check

To confirm file integrity for downloads, Cisco Unified Communications Manager and IM and Presence Service now provide the SHA-512 checksum value for all download files. For example, the SHA-512 checksum for application plugin downloads such as the Cisco AXL Toolkit or the Cisco Unified Real-Time Monitoring Tool, appears in the **Description** column of the **Find and List Application Pugins** window.

To confirm that the download did not contain errors, administrators can use an external program to compare the posted checksum against the checksum of the downloaded file. If the checksums match, there was no error in the download.

Maximum Session Limit CLI Update

With this release, the existing **set session maxlimit <value>** CLI command has been updated. As of this release, this command now sets the maximum number of concurrent sessions for the Cisco Unified OS Administration user interface, Disaster Recovery System user interface, and SSH client sessions.

User Interface Updates

For Release 11.5(1)SU1, the following user interface updates have been made to enhance security:

User Rank Configuration window

The **User Rank Configuration** window is new for this release. You can access this window at **User Management** > **User Settings** > **User Rank**. This window allows you to configure the user ranks that you can assign to end users and application users. It has the following fields:

- User Rank
- User Rank Name
- Description

User Rank Fields

The **User Rank** field has been added to the following configuration windows. This field allows you to assign the user rank for an end user or application user that you configure via these configuration windows:

- End User Configuration
- Application User Configuration
- Quick User/Phone Add
- LDAP Directory
- BAT User Template

Minimum Rank for Access Control Groups

In the **Access Control Group Configuration** window, the new **Available for users with User Rank as** drop-down menu has been added. This field allows you to assign the minimum rank that a user must meet to be assigned to that group.

APIC-EM Controller QoS Support

Relieve congested networks by using the APIC-EM Controller to manage priority settings for SIP media flows.

With this release, you can now configure support for the APIC-EM Controller within a SIP Profile. This enhancement helps you manage network QoS by allowing you to enable or disable the APIC-EM Controller integration for groups of users. For example, you could configure your SIP Profiles such that all Cisco Jabber endpoints use the APIC-EM to manage SIP media flows while all Cisco Unified IP Phones use Cisco Unified Communications Manager internal QoS mechanisms.

SIP Media Flow Management

For SIP calls that use APIC-EM, Cisco Unified Communications Manger sends the policy request to the APIC-EM Controller at the call outset notifying the APIC-EM of the media flow that is being set up. The policy request contains information about the call, including the IP address and ports for source and destination devices, the media type for the flow and the protocol.

The APIC-EM notifies the switch at the beginning of the call flow of the DSCP values for the associated media flows. The switch inserts those DSCP values into individual media packets, overwriting any values that the endpoint inserts. If a gateway in the call flow experiences congestion, that gateway sends through the packets with the higher DSCP values first. This ensures that high priority audio and video streams are not blocked by lower-priority network traffic such as email, print jobs, or software downloads. When the call ends, Cisco Unified Communications Manager notifies the APIC-EM and the APIC-EM notifies the switch to delete the flow.

User Interface Updates for APIC-EM

The following check box has been added to the **SIP Profile Configuration** window:

- **Enable External QoS—**Check this check box to configure the devices that use this SIP Profile for external QoS support. With this feature enabled, you can use an APIC-EM Controller to manage QoS for SIP media flows from this device.

Note This check box appears only if the **External QoS Enabled** clusterwide service parameter is set to **True**.

The following four fields have been added to the **HTTP Profile** window:

- **User Name—**Assign a user name for this connection to an HTTP server. The user name must match the configured user name on the HTTP server. Refer to your HTTP server documentation for user name restrictions.
- **Password—**Assign a password for this connection. You must configure the same password in the HTTP server. Refer to your HTTP server documentation for password restrictions such as acceptable characters.
- **Request Timeout—**After Cisco Unified Communications Manager sends a request to the HTTP server, this timer specifies the maximum time, in milliseconds, that Cisco Unified Communications Manager waits for a response.
- **Maximum Request Retries—**If the Request Timeout timer expires, the Maximum Request Retries field specifies the maximum number of times that Cisco Unified Communications Manager will resend the request.

Note Although the **HTTP Profile** fields appear in the 11.5(1) user interface, you must have at least the 11.5(1)SU1 installed to use them.

New Alarms for APIC-EM Controller

The following alarms have been added for the APIC-EM Controller support in the 11.5(1)SU1 release:

- **ExternalQoSTokenUnavailable—**This error alarm gets generated when Cisco Unified Communications Manager fails to connect with the APIC-EM Controller. This can occur if the access token is not available from the APIC-EM Controller, such as in the event of an authentication or network error.

  To resolve the error, fix that the username and password in the **HTTP Profile** window match the policy admin credentials that are configured in the APIC-EM. Once the issue is corrected, initiate a new connection attempt by toggling the **External QoS Enabled** service parameter to **False** and then back to **True**.
- **ExternalQoSTokenAvailable—**This informational alarm gets generated to confirm that Cisco Unified Communications Manager was able to obtain a valid access token from the APIC-EM Controller. The alarm is generated only if an **ExternalQoSTokenUnavailable** alarm was generated first.

  No action is required for this alarm.

Communication Updates for APIC-EM

Upon startup, or upon the service parameter being set, Cisco Unified Communications Manager sends a service ticket request to get an access token from the APIC-EM. After receiving the new token from the APIC-EM, Cisco Unified Communications Manager sends the token with every northbound REST API to validate that

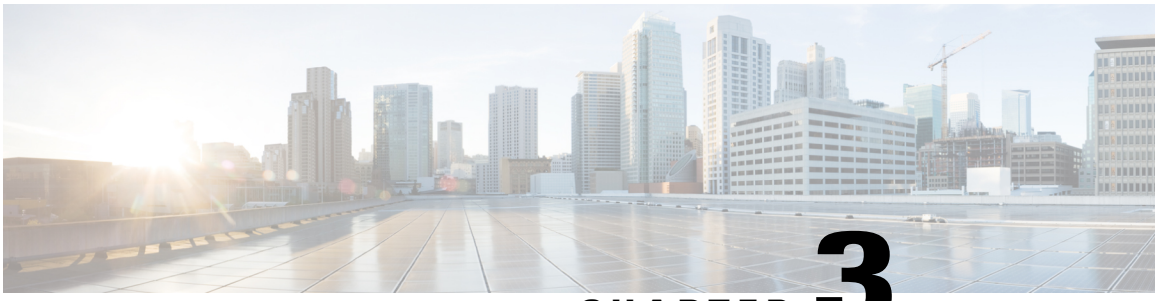
the request is from an authorized user. If the username or password are changed, or the service parameter is toggled to **False** and then to **True**, Cisco Unified Communications Manager requests a new token.

For APIC-EM developer documentation, go to https://developer.cisco.com/site/apic-em/.

PART II

Documentation Updates

- Configure QoS with APIC-EM Controller, page 13
- Configure User Access, page 21
- Audit Logs, page 39



CHAPTER 3

Configure QoS with APIC-EM Controller

Note This chapter replaces the existing 'Configure QoS with APIC-EM' chapter from the *System Configuration Guide for Cisco Unified Communications Manager, Release 11.5(1)*. This chapter describes how to configure the system to use an APIC-EM controller for QoS management. Updated with new functionality for this Service Update (SU) release.

- APIC-EM Controller Overview, page 13
- APIC-EM Controller Prerequisites, page 14
- APIC-EM Controller Configuration Task Flow, page 14
- APIC-EM Feature Restrictions, page 18
- Troubleshooting Tips for APIC-EM Controller, page 18

APIC-EM Controller Overview

The APIC-EM Controller provides a centralized system for managing network traffic so that you always have the bandwidth to maintain communications, even in congested networks. You can configure Cisco Unified Communications Manager to use the APIC-EM Controller to manage SIP media flows thereby providing the following benefits:

- Centralizes QoS management, thereby eliminating the need for endpoints to assign DSCP values.
- Applies differential QoS treatment for different media flows. For example, you can prioritize audio over video to ensure that basic audio communication is always maintained, even when network bandwidth is low.
- External QoS setting in the SIP Profile allows you to target which users will use the APIC-EM. For example, you may have Cisco Jabber users use the APIC-EM to manage media flows, while Cisco Unified IP Phone users use the DSCP settings in Cisco Unified Communications Manager.

SIP Media Flow Management

For SIP calls that use APIC-EM, Cisco Unified Communications Manger sends the policy request to the APIC-EM Controller at the call outset notifying the APIC-EM of the media flow that is being set up. The policy request contains information about the call, including the IP address and ports for source and destination devices, the media type for the flow and the protocol.

The APIC-EM notifies the switch at the beginning of the call flow of the DSCP values for the associated media flows. The switch inserts those DSCP values into individual media packets, overwriting any values that the endpoint inserts. If a gateway in the call flow experiences congestion, that gateway sends through the packets with the higher DSCP values first. This ensures that high priority audio and video streams are not blocked by lower-priority network traffic such as email, print jobs, or software downloads. When the call ends, Cisco Unified Communications Manager notifies the APIC-EM and the APIC-EM notifies the switch to delete the flow.

External QoS Support

In order for Cisco Unified Communications Manager to use the APIC-EM to manage media flows, the External QoS parameter must be enabled at both the system level, via a clusterwide service parameter, and at the device level, via the SIP Profile.

APIC-EM Controller Prerequisites

Complete the following configurations in the APIC-EM Controller user interface:

- Add Cisco Unified Communications Manager as a new user on the APIC-EM Controller with the ROLE_POLICY_ADMIN role. In addition, Dynamic QoS must be enabled.
- Configure the DSCP settings for various SIP media types. These are the values that the APIC-EM will communicate to the switch in a call flow.

For APIC-EM configuration details, refer to the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide* at: http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-installation-and-configuration-guides-list.html.

APIC-EM Controller Configuration Task Flow

Complete these tasks on Cisco Unified Communications Manager to enable APIC-EM Controller to manage SIP media flows.

Procedure

	Command or Action	Purpose
Step 1	Upload APIC-EM Controller Certificate, on page 15	Upload the APIC-EM certificate into Cisco Unified OS Administration.
Step 2	Configure HTTPS Connection to APIC-EM Controller, on page 15	Configure an HTTP Profile that points to the APIC-EM service.
Step 3	Enable External QoS Service for System, on page 16	Enable the **External QoS Enable** service parameter to configure the system to use the APIC-EM to manage media

	Command or Action	Purpose
		flows. The service parameter must be enabled for devices to use the APIC-EM for SIP media flow management. **Note** You must also enable external QoS within the SIP Profile for devices that will use the APIC-EM for SIP media flow management.
Step 4	Configure External QoS Service at SIP Profile Level, on page 16	Enable external QoS within a SIP Profile. All devices that use this SIP Profile will be able to use the APIC-EM to manage SIP media flows You can use the SIP Profile setting to configure which devices and device types you want the APIC-EM to manage media flows.
Step 5	Assign SIP Profile to Phones, on page 17	Associate the external QoS-enabled SIP Profile to a phone.

Upload APIC-EM Controller Certificate

Use this procedure to upload the APIC-EM controller certificate into Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate Chain**.
The **Upload Certificate/Certificate Chain** popup window appears.

Step 3 From the **Certificate Purpose** drop-down list, choose **CallManager-trust**.

Step 4 Enter a **Description** for the certificate.

Step 5 Click **Browse** to search for, and select, the certificate.

Step 6 Click **Upload**.

What to Do Next

Configure HTTPS Connection to APIC-EM Controller, on page 15

Configure HTTPS Connection to APIC-EM Controller

Use this procedure to set up an HTTP Profile to connect Cisco Unified Communications Manager to the APIC-EM Controller. In this connection, Cisco Unified Communications Manager acts as an HTTP user and the APIC-EM acts as the HTTP server.

Before You Begin

Upload APIC-EM Controller Certificate, on page 15

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **HTTP Profile**.

Step 2 Enter a **Name** for the service.

Step 3 Enter the **User Name** and **Password** for this HTTP connection. The user name does not have to be a configured end user in Cisco Unified Communications Manager, but the user name and password must match the values that are configured in the APIC-EM Controller.

Step 4 In the **Web Service Root URI** text box, enter the IP address or fully qualified domain name of the APIC-EM service.

Step 5 Configure any remaining fields in the HTTP Profile window. For help with the fields and their options, refer to the online help.

Step 6 Click **Save**.

What to Do Next

Enable External QoS Service for System, on page 16

Enable External QoS Service for System

Use this procedure to configure Cisco Unified Communications Manager to use an external service for QoS management. You must enable this service parameter in order to use an APIC-EM controller for QoS.

Before You Begin

Configure HTTPS Connection to APIC-EM Controller, on page 15

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, select the publisher node.

Step 3 From the **Service** drop-down list, select **Cisco CallManager**.

Step 4 Set the value of the **External QoS Enabled** service parameter to **True**.

Step 5 Click **Save**.

Note To use the APIC-EM to manage call flows for devices, you must also enable external QoS within the SIP Profile for the device.

What to Do Next

Configure External QoS Service at SIP Profile Level, on page 16

Configure External QoS Service at SIP Profile Level

If you have enabled the **External QoS Enabled** clusterwide service parameter, use this procedure to enable external QoS for SIP devices that use this SIP Profile.

Note External QoS must be enabled at both the system level and in the SIP Profile to use the APIC-EM to manage QoS.

Before You Begin

Enable External QoS Service for System, on page 16

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile**.

Step 2 Do one of the following:

- Click **Find** and select an existing SIP Profile.
- Click **Add New** to create a new SIP Profile.

Step 3 Check the **Enable External QoS** check box. This check box must be checked for phones that use this SIP Profile to use the APIC-EM Controller to manage QoS.

Step 4 Complete the remaining fields in the **SIP Profile Configuration** window. For help with the fields and their settings, see the online help.

Step 5 Click **Save**.

What to Do Next

Assign SIP Profile to Phones, on page 17

Assign SIP Profile to Phones

Use this procedure if you want to assign the external QoS-enabled SIP Profile that you created to a phone.

Tip Use the Bulk Administration Tool to update the SIP Profile for a large selection of phones in a single operation. For details, see the *Bulk Administration Guide for Cisco Unified Communications Manager.*

Before You Begin

Assign SIP Profile to Phones, on page 17

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select an existing phone.

Step 3 From the **SIP Profile** drop-down list box, select the SIP Profile that you updated for phones that will use the APIC-EM Controller to manage traffic.

Step 4 Complete any remaining fields in the **Phone Configuration** window. For help with the fields and their settings, see the online help.

Step 5 Click **Save**.

APIC-EM Feature Restrictions

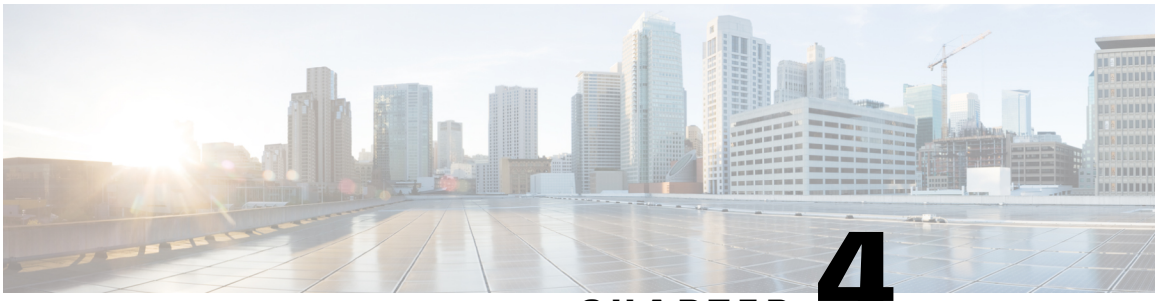
Feature	Restriction
Devices	Supported for SIP lines and trunks only.
Source IP Address and Port	The APIC-EM create flow includes the source IP address and port as well as the destination IP address and port, However, the SDP sent by the device includes only the destination IP address and port Cisco Unified Communications Manager assumes that the endpoint will use the same IP address and port for sending and receiving SIP messages.
Software Upgrades/Backups on the APIC-EM	An error occurs when you either upgrade software or run a backup/restore operation on the APIC-EM Controller. After the task completes, Cisco Unified Communications Manager will be unable to send policy information for new flows to the APIC-EM. To resolve this situation, once the upgrade or backup/restore operation on the APIC-EM is completed, toggle the **ExternalQoSEnable** service parameter to **False** and back to **True**. This will trigger a service ticket request from Cisco Unified Communications for an updated APIC-EM access token, and the connection will be restored.

Troubleshooting Tips for APIC-EM Controller

The following table contains troubleshooting tips for the APIC-EM controller.

Table 1: Troubleshooting Tips for APIC-EM Controller

Error	Remedy
Service Ticket Request receives a “Authentication failure from APIC-EM. Invalid service Ticket returned” 401 error response.	Verify that the username and password that are configured in the **HTTP Profile** window match the policy admin credentials that are configured on the APIC-EM Controller.
Service Ticket Request receives an “Unable to establish secure connection to server” 443 error response.	Verify that the APIC-EM Controller certificates have been uploaded to Cisco Unified Communications Manager.
No Dynamic QoS related messages are being sent.	Verify that both of the following conditions are true: • **External Qos Enabled** service parameter is **True**. • **Enable External QoS** check box is checked within the SIP Profile.
The **ExternalQoSTokenUnavailable** Alarm gets generated.	Check the network connectivity between Cisco Unified Communications Manager and the APIC-EM Controller. Confirm that the username and password that are configured in the **HTTP Profile** page match the policy admin credentials that are configured in the APIC-EM Controller. Once you finish your updates, toggle the **External QoS Enabled** service parameter to **False** and back to **True**.
HTTP policy request for a new flow receives following 400 error: "Error while applying QoS policies for a new flow. Duplicate flow. Flow cannot be processed".	Check the value of the **Enable External QoS** parameter for the SIP trunks in your network. You can do this by checking the SIP Profile for the SIP trunks in your network: For intercluster SIP trunks that connect different Cisco Unified Communications Manager clusters, the **Enable External QoS** check box must be left unchecked.



CHAPTER 4

Configure User Access

Note This chapter replaces the existing 'Configure Roles and Access Control Groups' chapter from the *System Configuration Guide for Cisco Unified Communications Manager, Release 11.5(1)*. The chapter has been renamed and revised to include the Rank Based Access Control feature that is introduced with this SU. The chapter describes how to configure user access, including user rank, access control groups, and roles.

- User Access Overview, page 21
- User Access Prerequisites, page 23
- User Access Configuration Task Flow, page 24
- Standard Roles and Access Control Groups, page 29

User Access Overview

You can manage user access to Cisco Unified Communications Manager by assigning the following items to your end users:

- Roles
- Access Control Groups
- User Rank

Roles, access control groups and user rank controls provide multiple levels of security to Cisco Unified Communications Manager. Each role defines a set of permissions for a specific resource within Cisco Unified Communications Manager. When you assign a role to an access control group and then assign end users to that access control group, you grant those end users all the access permissions that are defined by the role.

The User Rank framework overlays the roles and access control group framework and governs which groups are available for an end user. End users and application users can be assigned to only those access control groups that their user rank allows.

Roles Overview

When you provision end users, you must decide on what roles you want to assign to your users. You can assign roles to an end user, application user, or to an access control group. You can assign multiple roles to a single user.

Each role contains a set of privileges that are attached to a specific resource or application. For example, the Standard CCM End Users role provides users who are assigned that role with access to the Cisco Unified Communications Self Care Portal. You can also assign roles that provide access to resources such as Cisco Unified Communications Manager Administration, Cisco CDR Analysis and Reporting, the Dialed Number Analyzer, and the CTI interface. For most resources with graphical user interfaces, such as a specific configuration window, the privileges that are attached to the role allow the user to view or update data in that window, or in a group of related windows.

Configuring and Assigning Roles

You must decide whether you want to assign standard roles to your users, or create custom roles:

- Standard roles—Standard roles are predefined, default roles that come installed in Cisco Unified Communications Manager. You cannot edit the privileges or modify the role in any way.
- Custom roles—Custom roles are roles that you create. You can create custom roles when there are no standard roles that contain the privileges that you want to assign to your users. For example, if you want to assign a standard role, but want to modify one of the privileges, you can copy the privileges of the standard role into a custom role and then edit the privileges in that custom role.

Privilege Types

Each role contains a set of privileges that are attached to a specific resource. There are two types of privileges that you can assign to a resource:

- Read—Read privilege gives the user the ability to view the settings for that resource, but the user cannot make any configuration updates. For example, the privilege may allow the user to view the settings on a particular configuration window, but the configuration window for that application will not display update buttons or icons.
- Update—Update privileges give the user the ability to modify the settings for that resource. For example, the privileges may allow the user to make updates in a specific configuration window.

End User and Administrator Roles

The Standard CCM End Users role provides end users with access to the Cisco Unified Communications Self Care Portal. For additional privileges, such as CTI access, you must assign additional roles, such as the Standard CTI Enabled role.

The Standard CCM Admin Users role is the base role for all administration tasks and serves as the authentication role. This role provides users with administrative access to the Cisco Unified Communications Manager Administration user interface. Cisco Unified Communications Manager Administration defines this role as the role that is necessary to log in to Cisco Unified Communications Manager Administration.

Related Topics

Standard Roles and Access Control Groups, on page 29

Access Control Group Overview

You can use access control groups along with roles to quickly assign network access permissions to a group of users with similar access requirements.

An access control group is a list of end users and application users. You can assign end users or application users who share similar access needs to an access control group that contains the roles and permissions that they need. For an end user or application user to be assigned to an access control group, the user must meet the minimum rank requirement for that access control group. For example, an end user with a User Rank of 4 can be assigned only to access control groups with minimum rank requirements between 4 and 10.

The system includes a set of predefined standard access control groups. Each standard access control group has a set of roles assigned by default. When you assign a user to that access control group, those roles are also assigned to that end user.

You cannot edit the roles that are assigned to standard access control groups. However, you can create customized access control groups and assign the roles that you choose to your customized access control groups.

Related Topics

Standard Roles and Access Control Groups, on page 29

User Rank Overview

User Rank Access Control provides a set of controls over the level of access that an administrator can provide to an end user or application user. The **User Rank** parameter is a 1–10 integer with 1 being the highest possible rank. The user rank is assigned to both users and access control groups thereby creating a rank hierarchy that governs which users can be assigned to a particular access control group.

When provisioning end users or application users, administrators must assign a user rank for each user. Administrators must also assign a user rank to each access control group. Administrators can assign users to only those access control groups with the same or lower rank. For example, if an end user has a user rank of 3, they can be assigned to access control groups that have a user rank between 3 and 10. That user cannot be assigned to an access control group that requires a user rank of 1.

Administrators can customize user rank hierarchy within the **User Rank Configuration** window and then assign those ranks to end users, application users, and access control groups.

User Access Prerequisites

Before you provision end users:

- Standard Roles and Access Control Groups, on page 29—Review the list of predefined roles and access control groups. Determine if you will need to configure customized roles and groups.
- Plan which user ranks you will assign to your users and groups.

User Access Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Create a Custom User Rank, on page 24	Set up the user rank hierarchy for your system.
Step 2	If you need to create a new role, use one of the following methods: • Create a Custom Role, on page 25 • Copy an Existing Role, on page 26	Use the 'Create' procedure if you want to create and configure a new role from scratch. Use the 'Copy' procedure if the new role has similar privileges to an existing role. You can copy the privileges from the existing role into a new role, and then make edits to the privileges in the new role.
Step 3	If you need to create new access control groups, use one of the following methods: • Create Access Control Groups, on page 26 • Copy Access Control Group, on page 27	Use the 'Create' procedure to create a new access control group from scratch. Use the 'Copy' procedure if the new access control group has similar settings to an existing access control group. You can copy the settings from the existing access control group into a new group and then edit the settings.
Step 4	Assign Roles to Access Control Group, on page 28	If you created a new access control group, assign roles to your access control group.
Step 5	Configure Overlapping Privilege Policy, on page 29	Configure an enterprise policy to cover overlapping access privileges. This covers the situation where end users or application users are assigned to multiple access control groups or roles, each with conflicting privilege settings.

Related Topics

Standard Roles and Access Control Groups, on page 29

Create a Custom User Rank

Use this procedure to create a custom user rank for your rank hierarchy.

Procedure

Step 1 From Cisco Unified CM Administration, choose**User Management** > **User Settings** > **User Rank**.

Step 2 Click **Add New**.

Step 3 From the **User Rank** drop-down menu, select a rank setting between 1–10. The highest rank is 1.

Step 4 Enter a **Rank Name** and **Description**.

Step 5 Click **Save**.

Create a Custom Role

Create a custom role when there is no system-defined role with the privilege settings that you require.

Tip If the privileges in the new role that you want to create are similar to that of an existing role, follow the procedure Copy an Existing Role, on page 26 to copy the existing privileges into a new role that you can edit.

Procedure

Step 1 In Cisco Unified CM Administration, click **User Management** > **User Settings** > **Role**.

Step 2 From the **Application** drop-down list box, choose the application with which this role associates.
The **Role Configuration** window displays.

Step 3 Click **Next**.

Step 4 In the **Name** text box, enter a name for the role.
Names can comprise up to 128 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.

Step 5 In the **Description** text box, enter a description for the role.
Descriptions can have up to 128 characters.

Step 6 For each resource in the new role, edit the privileges as follows:

- if you want the role to be able to view that resource, click the **Read** check box
- if you want the role to be able to edit that resource, click the **Update** check box
- if you want the role to be able to view and edit that resource, check both the **Read** and **Update** check boxes
- If you do not want the role to have any access to that resource, leave both check boxes unchecked.

Step 7 Click **Grant access to all** or **Deny access to all** button to grant or remove privileges to all resources that display on a page for this role.

Note If the list of resources displays on more than one page, this button applies only to the resources that display on the current page. You must display other pages and use the button on those pages to change the access to the resources that are listed on those pages.

Step 8 Click **Save**.

What to Do Next

Create Access Control Groups, on page 26

Copy an Existing Role

The **Copy** command allows you to create new roles that are based on the settings of existing roles. Cisco Unified Communications Manager does not allow you to edit standard roles, but you can use the **Copy** command to create a new role with the identical resources and privileges as the standard role. You can then edit the privileges in the new role that you created.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, click **User Management** > **User Settings** > **Role**.

Step 2 Click **Find** and select the role whose resources and privileges you want to copy.

Step 3 Click **Copy**.

Step 4 Enter the name of the new role and click **OK**.
The **Role Configuration** window displays the settings of the new role. The privileges for the new role are the same as the privileges for the role you copied.

Step 5 For any of the resources in the new role, edit the privileges as follows:

- Check the **Read** check box to allow users to view the resource.
- Check the **Update** check box to allow users to edit the resource.
- To restrict access to the resource, leave both check boxes unchecked.

Step 6 Click **Save**.

What to Do Next

Create a new access control group using one of the following methods:

- Create Access Control Groups, on page 26
- Copy Access Control Group, on page 27

Related Topics

Standard Roles and Access Control Groups, on page 29

Create Access Control Groups

Use this procedure is you need to create a new access control group. You may need to create a new access control group if the system-defined access control groups do not meet your deployment needs.

Before You Begin

If you need to create new roles, perform one of the following procedures:

- Create a Custom Role, on page 25
- Copy an Existing Role, on page 26

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Groups.**

Step 2 Click **Add New**.

Step 3 Enter a **Name** for the access control group.

Step 4 From the **Available for Users with User Rank as** drop-down, select the minimum User Rank for a user to be assigned to this group. The default user rank is 1.

Step 5 Click **Save**.

What to Do Next

Assign Roles to Access Control Group, on page 28

Copy Access Control Group

Create a custom access control group by copying the settings from an existing access control group. When you copy an existing access control group, the system copies all the settings, including any assigned roles and users, to the new access control group. However, unlike default access control groups, you can make edits to the roles assigned to a custom access control group.

Before You Begin

If you need to create a new role, perform either of the following steps:

- Create a Custom Role, on page 25
- Copy an Existing Role, on page 26

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Groups**.

Step 2 Click **Find** and select the access control group whose settings you want to copy.

Step 3 Click **Copy**.

Step 4 Enter a name for the new access control group and click **OK**.

Step 5 From the **Available for Users with User Rank as** drop-down, select the minimum User Rank for a user to be assigned to this group.

Step 6 Click **Save**.

What to Do Next

Assign Roles to Access Control Group, on page 28

Related Topics

Standard Roles and Access Control Groups, on page 29
Assign LDAP Users to Access Control Group
Assign Local Users to Access Control Group

Assign Roles to Access Control Group

For any new access control groups that you create, assign roles to the access control group. If you copied the access control group from an existing group, you may also need to delete a role.

Note You cannot edit the role assignments for any of the standard access control groups that are are configured by default.

Before You Begin

Perform either of the following tasks to create a new access control group:

- Create Access Control Groups, on page 26
- Copy Access Control Group, on page 27

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group**.

Step 2 Click **Find** and select an access control group.

Step 3 From the **Related Links** drop-down list box, select **Assign Role to Access Control Group** and click **Go**.

Step 4 If you need to assign a role:

a) Click **Assign Role to Group**.
b) In the **Find and List Roles** window, check the roles that you want to assign to the group.
c) Click **Add Selected**.

Step 5 If you need to delete a role:

a) In the **Role** list box, highlight the role that you want to delete.
b) Click **Delete Role Assignment**.

Step 6 Click **Save**.

What to Do Next

Configure Overlapping Privilege Policy, on page 29

Configure Overlapping Privilege Policy

Configure how Cisco Unified Communications Manager handles overlapping user privileges in access control group assignments. This is to cover situations where an end user is assigned to multiple access control groups, each with conflicting roles and access privileges.

Before You Begin

Assign Roles to Access Control Group, on page 28

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Under **User Management Parameters**, configure one of the following values for the **Effective Access Privileges For Overlapping User Groups and Roles** as follows:

- **Maximum—**The effective privilege represents the maximum of the privileges of all the overlapping access control groups. This is the default option.
- **Minimum—**The effective privilege represents the minimum of the privileges of all the overlapping access control groups.

Step 3 Click **Save**.

Standard Roles and Access Control Groups

The following table summarizes the standard roles and access control groups that come preconfigured on Cisco Unified Communications Manager. The privileges for a standard role are configured by default. In addition, the access control groups that are associated with a standard role are also configured by default.

For both standard roles and the associated access control group, you cannot edit any of the privileges, or the role assignments.

Table 2: Standard Roles, Privileges, and Access Control Groups

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard AXL API Access	Allows access to the AXL database API	Standard CCM Super Users
Standard AXL API Users	Grants login rights to execute AXL APIs.	
Standard AXL Read Only API Access	Allows you to execute AXL read only APIs (list APIs, get APIs, executeSQLQuery API) by default.	
Standard Admin Rep Tool Admin	Allows you to view and configure Cisco Unified Communications Manager CDR Analysis and Reporting (CAR).	Standard CAR Admin Users, Standard CCM Super Users

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard Audit Log Administration	Allows you to perform the following tasks for the audit logging feature : • View and configure audit logging in the Audit Log Configuration window in Cisco Unified Serviceability • View and configure trace in Cisco Unified Serviceability and collect traces for the audit log feature in the Real-Time Monitoring Tool • View and start/stop the Cisco Audit Event service in Cisco Unified Serviceability • View and update the associated alert in the RTMT	Standard Audit Users
Standard CCM Admin Users	Grants log-in rights to Cisco Unified Communications Manager Administration.	Standard CCM Admin Users, Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Monitoring, Standard CCM Super Users, Standard CCM Server Maintenance, Standard Packet Sniffer Users
Standard CCM End Users	Grant an end user log-in rights to the Cisco Unified Communications Self Care Portal	Standard CCM End Users

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Feature Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View, delete, and insert the following items by using the Bulk Administration Tool: ◦ Client matter codes and forced authorization codes ◦ Call pickup groups • View and configure the following items in Cisco Unified Communications Manager Administration: ◦ Client matter codes and forced authorization codes ◦ Call park ◦ Call pickup ◦ Meet-Me numbers/patterns ◦ Message Waiting ◦ Cisco Unified IP Phone Services ◦ Voice mail pilots, voice mail port wizard, voice mail ports, and voice mail profiles	Standard CCM Server Maintenance
Standard CCM Gateway Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure gateway templates in the Bulk Administration Tool • View and configure gatekeepers, gateways, and trunks	Standard CCM Gateway Administration

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Phone Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and export phones in the Bulk Administration Tool • View and insert user device profiles in the Bulk Administration Tool • View and configure the following items in Cisco Unified Communications Manager Administration: ◦ BLF speed dials ◦ CTI route points ◦ Default device profiles or default profiles ◦ Directory numbers and line appearances ◦ Firmware load information ◦ Phone button templates or softkey templates ◦ Phones ◦ Reorder phone button information for a particular phone by clicking the Modify Button Items button in the Phone Configuration window	Standard CCM Phone Administration
Standard CCM Route Plan Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure application dial rules • View and configure calling search spaces and partitions • View and configure dial rules, including dial rule patterns • View and configure hunt lists, hunt pilots, and line groups • View and configure route filters, route groups, route hunt list, route lists, route patterns, and route plan report • View and configure time period and time schedule • View and configure translation patterns	

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Service Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure the following items: ◦ Annunciators, conference bridges, and transcoders ◦ audio sources and MOH servers ◦ Media resource groups and media resource group lists ◦ Media termination point ◦ Cisco Unified Communications Manager Assistant wizard • View and configure the Delete Managers, Delete Managers/Assistants, and Insert Managers/Assistants windows in the Bulk Administration Tool	Standard CCM Server Maintenance

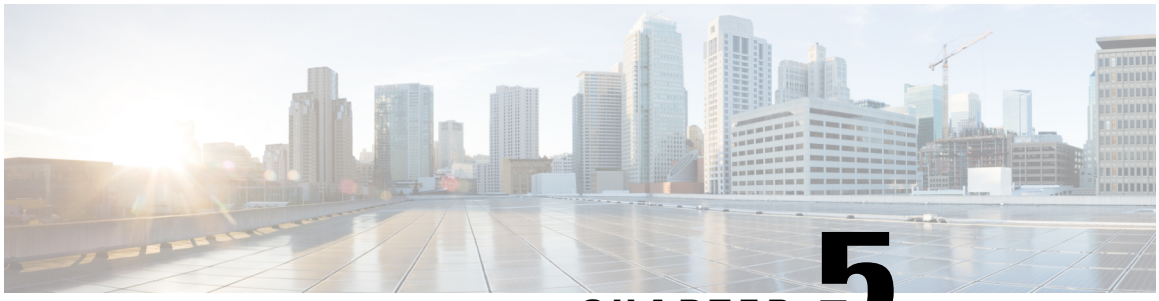
Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM System Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure the following items: ◦ Automate Alternate Routing (AAR) groups ◦ Cisco Unified Communications Managers (Cisco Unified CMs) and Cisco Unified Communications Manager groups ◦ Date and time groups ◦ Device defaults ◦ Device pools ◦ Enterprise parameters ◦ Enterprise phone configuration ◦ Locations ◦ Network Time Protocol (NTP) servers ◦ Plug-ins ◦ Security profiles for phones that run Skinny Call Control Protocol (SCCP) or Session Initiation Protocol (SIP); security profiles for SIP trunks ◦ Survivable Remote Site Telephony (SRST) references ◦ Servers • View and configure the Job Scheduler windows in the Bulk Administration Tool	Standard CCM Server Maintenance
Standard CCM User Privilege Management	Allows you to view and configure application users in Cisco Unified Communications Manager Administration.	
Standard CCMADMIN Administration	Allows you access to all aspects of the CCMAdmin system	
Standard CCMADMIN Administration	Allows you to view and configure all items in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Super Users
Standard CCMADMIN Administration	Allows you to view and configure information in the Dialed Number Analyzer.	
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCMADMIN Read Only	Allows you to view configurations in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Maintenance, Standard CCM Server Monitoring
Standard CCMADMIN Read Only	Allows you to analyze routing configurations in the Dialed Number Analyzer.	
Standard CCMUSER Administration	Allows access to the Cisco Unified Communications Self Care Portal.	Standard CCM End Users
Standard CTI Allow Call Monitoring	Allows CTI applications/devices to monitor calls	Standard CTI Allow Call Monitoring
Standard CTI Allow Call Park Monitoring	Allows CTI applications/devices to use call park	Standard CTI Allow Call Park Monitoring
Standard CTI Allow Call Recording	Allows CTI applications/devices to record calls	Standard CTI Allow Call Recording
Standard CTI Allow Calling Number Modification	Allows CTI applications to transform calling party numbers during a call	Standard CTI Allow Calling Number Modification
Standard CTI Allow Control of All Devices	Allows control of all CTI-controllable devices	Standard CTI Allow Control of All Devices
Standard CTI Allow Control of Phones Supporting Connected Xfer and conf	Allows control of all CTI devices that supported connected transfer and conferencing	Standard CTI Allow Control of Phones supporting Connected Xfer and conf
Standard CTI Allow Control of Phones Supporting Rollover Mode	Allows control of all CTI devices that supported Rollover mode	Standard CTI Allow Control of Phones supporting Rollover Mode
Standard CTI Allow Reception of SRTP Key Material	Allows CTI applications to access and distribute SRTP key material	Standard CTI Allow Reception of SRTP Key Material
Standard CTI Enabled	Enables CTI application control	Standard CTI Enabled
Standard CTI Secure Connection	Enables a secure CTI connection to Cisco Unified Communications Manager	Standard CTI Secure Connection
Standard CUReporting	Allows application users to generate reports from various sources	

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CUReporting	Allows you to view, download, generate, and upload reports in Cisco Unified Reporting	Standard CCM Administration Users, Standard CCM Super Users
Standard EM Authentication Proxy Rights	Manages Cisco Extension Mobility (EM) authentication rights for applications; required for all application users that interact with Cisco Extension Mobility (for example, Cisco Unified Communications Manager Assistant and Cisco Web Dialer)	Standard CCM Super Users, Standard EM Authentication Proxy Rights
Standard Packet Sniffing	Allows you to access Cisco Unified Communications Manager Administration to enable packet sniffing (capturing).	Standard Packet Sniffer Users
Standard RealtimeAndTraceCollection	Allows an you to access Cisco Unified Serviceability and the Real-Time Monitoring Tool view and use the following items: • Simple Object Access Protocol (SOAP) Serviceability AXL APIs • SOAP Call Record APIs • SOAP Diagnostic Portal (Analysis Manager) Database Service • configure trace for the audit log feature • configure Real-Time Monitoring Tool, including collecting traces	Standard RealtimeAndTraceCollection

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SERVICEABILITY	Allows you to view and configure the following windows in Cisco Unified Serviceability or the Real-Time Monitoring Tool: • Alarm Configuration and Alarm Definitions (Cisco Unified Serviceability) • Audit Trace (marked as read/view only) • SNMP-related windows (Cisco Unified Serviceability) • Trace Configuration and Troubleshooting of Trace Configuration (Cisco Unified Serviceability) • Log Partition Monitoring • Alert Configuration (RTMT), Profile Configuration (RTMT), and Trace Collection (RTMT) Allows you to view and use the SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service. For the SOAP Call Record API, the RTMT Analysis Manager Call Record permission is controlled through this resource. For the SOAP Diagnostic Portal Database Service, the RTMT Analysis Manager Hosting Database access controlled thorough this resource.	Standard CCM Server Monitoring, Standard CCM Super Users
Standard SERVICEABILITY Administration	A serviceability administrator can access the Plugin window in Cisco Unified Communications Manager Administration and download plugins from this window.	
Standard SERVICEABILITY Administration	Allows you to administer all aspects of serviceability for the Dialed Number Analyzer.	
Standard SERVICEABILITY Administration	Allows you to view and configure all windows in Cisco Unified Serviceability and Real-Time Monitoring Tool. (Audit Trace supports viewing only.) Allows you to view and use all SOAP Serviceability AXL APIs.	
Standard SERVICEABILITY Read Only	Allows you to view all serviceability-related data for components in the Dialed Number Analyzer.	Standard CCM Read Only

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SERVICEABILITY Read Only	Allows you to view configuration in Cisco Unified Serviceability and Real-Time Monitoring Tool. (excluding audit configuration window, which is represented by the Standard Audit Log Administration role) Allows an you to view all SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service.	
Standard System Service Management	Allows you to view, activate, start, and stop services in Cisco Unified Serviceability.	



CHAPTER 5

Audit Logs

Note This chapter replaces the existing 'Audit Logs' chapter from the *Cisco Unified Serviceability Administration Guide, Release 11.5(1)*. This chapter describes how to set up audit logging and has been updated with new functionality for this Service Update (SU) release.

- Audit Logs, page 39

Audit Logs

With audit logging, configuration changes to the system get logged in separate log files for auditing.

Audit Logging (Standard)

When audit logging is enabled, but the detailed audit logging option is not selected, the system is configured for standard audit logging.

With standard audit logging, configuration changes to the system get logged in separate log files for auditing. The Cisco Audit Event Service, which displays under Control Center - Network Services in the serviceability GUI, monitors and logs any configuration changes to the system that are made by a user or as a result of the user action.

You access the **Audit Log Configuration** window in the serviceability GUI to configure the settings for the audit logs.

Standard audit logging contains the following parts:

- Audit logging framework - The framework comprises an API that uses an alarm library to write audit events into audit logs. An alarm catalog that is defined as GenericAlarmCatalog.xml applies for these alarms. Different system components provide their own logging.

  The following example displays an API that a Cisco Cisco Unified Communications Manager component can use to send an alarm:

```
User ID: CCMAdministratorClient IP Address: 172.19.240.207
Severity: 3
```

```
EventType: ServiceStatusUpdated
ResourceAccessed: CCMService
EventStatus: Successful
Description: CallManager Service status is stopped
```

- Audit event logging - An audit event represents any event that is required to be logged. The following example displays a sample audit event:

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is
stopped App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node
ID:sa-cm1-3
```

Tip Be aware that audit event logging is centralized and enabled by default. An alarm monitor called Syslog Audit writes the logs. By default, the logs are configured to rotate. If the AuditLogAlarmMonitor cannot write an audit event, the AuditLogAlarmMonitor logs this failure as a critical error in the syslog file. The Alert Manager reports this error as part of a SeverityMatchFound alert. The actual operation continues even if the event logging fails. All audit logs get collected, viewed, and deleted from Trace and Log Central in the Cisco Unified Real-Time Monitoring Tool.

Cisco Unified Serviceability Standard Events Logging

Cisco Unified Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service.
- Changes in trace configurations and alarm configurations.
- Changes in SNMP configurations.
- Changes in CDR management. (Cisco Cisco Unified Communications Manager only)
- Review of any report in the Serviceability Reports Archive. This log gets viewed on the reporter node. (Cisco Cisco Unified Communications Manager only)

Cisco Unified Real-Time Monitoring Tool Standard Events Loggin

Cisco Unified Real-Time Monitoring Tool logs the following events with an audit event alarm:

- Alert configuration
- Alert suspension
- E-mail configuration
- Set node alert status
- Alert addition
- Add alert action
- Clear alert
- Enable alert

- Remove alert action
- Remove alert

Cisco Unified Communications Manager Standard Events Logging

Cisco CDR Analysis and Reporting (CAR) creates audit logs for these events:

- Loader scheduling
- Daily, weekly, and monthly reports scheduling
- Mail parameters configuration
- Dial plan configuration
- Gateway configuration
- System preferences configuration
- Autopurge configuration
- Rating engine configurations for duration, time of day, and voice quality
- QoS configurations
- Automatic generation/alert of pregenerated reports configurations.
- Notification limits configuration

Cisco Unified CM Administration Standard Events Logging

The following events get logged for various components of Cisco Cisco Unified Communications Manager Administration:

- User logging (user logins and user logouts)
- User role membership updates (user added, user deleted, user role updated)
- Role updates (new roles added, deleted, or updated)
- Device updates (phones and gateways)
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, hostnames, Ethernet settings, and Cisco Cisco Unified Communications Manager server additions or deletions)

Cisco Unified Communications Self Care Portal Standard Events Logging

User logging (user login and user logout) events are logged for Cisco Unified Communications Self Care Portal.

Command-Line Interface Standard Events Logging

All commands issued via the command-line interface are logged (for both Cisco Cisco Unified Communications Manager and Cisco Unity Connection).

Cisco Unity Connection Administration Standard Events Logging

Cisco Unity Connection Administration logs the following events:

- User logging (user logins and user logouts)
- All configuration changes, including but not limited to users, contacts, call management objects, networking, system settings, and telephony
- Task management (enabling or disabling a task)
- Bulk Administration Tool (bulk creates, bulk deletes)
- Custom Keypad Map (map updates)

Cisco Personal Communications Assistant (Cisco PCA) Standard Events Logging

The Cisco Personal Communications Assistant client logs the following events:

- User logging (user logins and user logouts)
- All configuration changes made via the Messaging Assistant

Cisco Unity Connection Serviceability Standard Events Logging

Cisco Unity Connection Serviceability logs the following events:

- User logging (user logins and user logouts).
- All configuration changes.
- Activating, deactivating, starting or stopping services.

Cisco Unity Connection Clients that Use the Representational State Transfer APIs Events Logging

Cisco Unity Connection clients that use the Representational State Transfer (REST) APIs log the following events:

- User logging (user API authentication).
- API calls that utilize Cisco Unity Connection Provisioning Interface.

Audit Logging (Detailed)

Detailed audit logging is an optional feature that logs additional configuration modifications that are not stored in standard (default) audit logs. In addition to all of the information that is stored in standard audit logs, detailed audit logging also includes configuration items that were added, updated, and deleted, including the modified values. Detailed audit logging is disabled by default, but you can enable it in the **Audit Log Configuration** window.

Audit Log Types

System Audit Logs

System audit logs track activities such as the creation, modification, or deletion of Linux OS users, log tampering, and any changes to file or directory permissions. This type of audit log is disabled by default due to the high volume of data gathered. To enable this function, you must manually enable utils auditd using the CLI. After you have enabled the system audit log feature, you can collect, view, download, or delete selected logs through Trace & Log Central from the Real-Time Monitoring Tool. System audit logs take on the format of `vos-audit.log`.

For information about how to enable this feature, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. For information about how to access collected logs from the Real-Time Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* .

Application Audit Logs

The Application Audit logs monitor and record any configuration changes to the system that were made by a user or as a result of the user action.

Note The Application Audit Logs (Linux auditd) can be enabled or disabled only through the CLI. Other than the collection of vos-audit.log through the Real-Time Monitoring Tool, you can not change any settings for this type of audit log.

Database Audit Logs

Database Audit Logs track all activities associated with access to the Informix Database, such as logins.

Audit Log Configuration Task Flow

Complete the following tasks to configure audit logging.

Procedure

	Command or Action	Purpose
Step 1	Set up Audit Logging, on page 44	Set up your audit log configuration in the Audit Log Configuration window. You can configure whether you want to use remote audit logging and whether you want the Detailed Audit Logging option.
Step 2	Configure Remote Audit Log Transfer Protocol, on page 44	Optional. If you have remote audit logging configured, configure the transfer protocol. The system default in normal operating mode is UDP, but you can also configure TCP.
Step 3	Configure Email Server for Alert Notifications, on page 45	Optional. In RTMT, set up the email server for email alerts.

	Command or Action	Purpose
Step 4	Enable Email Alerts, on page 45	Optional. If you have remote audit logging configured with TCP, set up the email notification for the **TCPRemoteSyslogDeliveryFailed** alert.
Step 5	Configure Remote Audit Logging for Platform Logs, on page 46	Set up remote audit logging for platform audit logs and remote server logs. For these types of audit logs, you must configure a FileBeat client and external logstash server.

Set up Audit Logging

Before You Begin

For remote audit logging, you must have already set up your remote syslog server and configured IPSec between each cluster node and the remote syslog server, including connections to any gateways in between. For IPSec configuration, see the *Cisco IOS Security Configuration Guide*.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Audit Log Configuration**.

Step 2 From the **Server** drop-down menu, select any server in the cluster and click **Go**.

Step 3 To log all cluster nodes, check the **Apply to All Nodes** check box.

Step 4 In the **Server Name** field, enter the IP Address or fully qualified domain name of the remote syslog server.

Step 5 Optional. To log configuration updates, including items that were modified, and the modified values, check the **Detailed Audit Logging** check box.

Step 6 Complete the remaining fields in the **Audit Log Configuration** window. For help with the fields and their descriptions, see the online help.

Step 7 Click **Save**.

What to Do Next

Configure Remote Audit Log Transfer Protocol, on page 44

Configure Remote Audit Log Transfer Protocol

Use this procedure to change the transfer protocol for remote audit logs. The system default is UDP , but you can reconfigure to TCP.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils remotesyslog show protocol** command to confirm which protocol is configured.

Step 3 If you need to change the protocol on this node, do the following:

- To configure TCP, run the **utils remotesyslog set protocol tcp** command.
- To configure UDP, run the **utils remotesyslog set protocol udp** command.

Step 4 If you changed the protocol, restart the node.

Step 5 Repeat this procedure for all Cisco Unified Communications Manager and IM and Presence Service cluster nodes.

What to Do Next

Configure Email Server for Alert Notifications, on page 45

Configure Email Server for Alert Notifications

Use this procedure to set up your email server for alert notifications.

Procedure

Step 1 In the Real-Time Monitoring Tool's System window, click **Alert Central**.

Step 2 Choose **System** > **Tools** > **Alert** > **Config Email Server**.

Step 3 In the **Mail Server Configuration** popup, enter the details for the mail server.

Step 4 Click **OK**.

What to Do Next

Enable Email Alerts, on page 45

Enable Email Alerts

If you have remote audit logging with TCP configured, use this procedure to set up an email alert for the **TCPRemoteSyslogDeliveryFailed** alert to notify you of transmission failures.

Procedure

Step 1 In the Real-Time Monitoring Tool **System** area, click **Alert Central**.

Step 2 In the **Alert Central** window, select **TCPRemoteSyslogDeliveryFailed**.

Step 3 Choose **System** > **Tools** > **Alert** > **Config Alert Action**.

Step 4 In the **Alert Action** popup, select **Default** and click **Edit**.

Step 5 In the **Alert Action** popup, **Add** a recipient.

Step 6 In the popup window, enter the address where you want to send email alerts and click **OK**.

Step 7 In the **Alert Action** popup, make sure that the address appears under **Recipients** and that the **Enable** check box is checked.

Step 8 Click **OK**.

Configure Remote Audit Logging for Platform Logs

Complete these tasks to add remote audit logging support for platform audit logs, remote support logs, and Bulk Administration csv files. For these types of logs, the FileBeat client and logstash server get used.

Before You Begin

Make sure that you have set up an external logstash server.

Procedure

	Command or Action	Purpose
Step 1	Configure Logstash Server Information, on page 46	Configure the FileBeat client with the external logstash server details, such as IP addresses, ports and file types.
Step 2	Configure the FileBeat Client, on page 47	Enable the FileBeat client for remote audit logging.

Configure Logstash Server Information

Use this procedure to configure the FileBeat client with the external logstash server information, such as IP address, port number, and downloadable file types.

Before You Begin

Make sure that you have set up your external logstash server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat configure** command.

Step 3 Follow the prompts to configure the logstash server details.

Configure the FileBeat Client

Use this procedure to enable or disable the FileBeat client for uploads of platform audit logs, remote support logs, and Bulk Administration csv files.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat status** command to confirm whether the FileBeat client is enabled.

Step 3 Run one of the following commands:

- To enable the client, run the **utils FileBeat enable** command.
- To disable the client, run the **utils FileBeat disable** command.

Step 4 Repeat this procedure on each node.
Do not run any of these commands on all nodes simultaneously.

Audit Log Configuration Settings

Before You Begin

Be aware that only a user with an audit role can change the audit log settings. By default, for Cisco Cisco Unified Communications Manager, the CCMAdministrator possesses the audit role after fresh installs and upgrades. The CCMAdministrator can assign any user that has auditing privileges to the Standard Audit Users group in the User Group Configuration window in Cisco Cisco Unified Communications Manager Administration. If you want to do so, you can then remove CCMAdministrator from the Standard Audit Users group.

For Cisco Unity Connection, the application administration account that was created during installation has the Audit Administrator role and can assign other administrative users to the role. You can also remove the Audit Administrator role from this account.

The Standard Audit Log Configuration role is to provide the ability to delete audit logs and to read/update access to Cisco Unified Real-Time Monitoring Tool, IM and Presence Real-Time Monitoring Tool, Trace Collection Tool, Real-Time Monitoring Tool (RTMT) Alert Configuration, Control Center - Network Services in the serviceability user interface, RTMT Profile Saving, Audit Configuration in the serviceability user interface, and a resource that is called Audit Traces.

The Standard Audit Log Configuration role is to provide the ability to delete audit logs and to read/update access to Cisco Unified RTMT, Trace Collection Tool, RTMT Alert Configuration, Control Center - Network Services in Cisco Unified Serviceability, RTMT Profile Saving, Audit Configuration in Cisco Unified Serviceability, and a resource that is called Audit Traces.

The Audit Administrator role in Cisco Unity Connection provides the ability to view, download and delete audit logs in Cisco Unified RTMT.

For information on roles, users, and user groups in Cisco Cisco Unified Communications Manager, refer to the *Cisco Cisco Unified Communications Manager Administration Guide*.

For information on roles and users in Cisco Unity Connection, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

The following table describes the settings that you can configure in the Audit Log Configuration window in Cisco Unified Serviceability.

Table 3: Audit Log Configuration Settings

Field	Description
Select Server	
Server	Choose the server (node) where you want to configure audit logs; then, click **Go**.
Apply to All Nodes	If you want to apply the audit log configuration to all nodes in the cluster, check the **Apply to all Nodes** check box.
Application Audit Log Settings	
Enable Audit Log	When you check this check box, an audit log gets created for the application audit log. For Cisco Cisco Unified Communications Manager, the application audit log supports configuration updates for Cisco Cisco Unified Communications Manager user interfaces, such as Cisco Cisco Unified Communications Manager Administration, Cisco Unified RTMT, Cisco Cisco Unified Communications Manager CDR Analysis and Reporting, and Cisco Unified Serviceability. For Cisco Unity Connection, the application audit log supports configuration updates for Cisco Unity Connection user interfaces, including Cisco Unity Connection Administration, Cisco Unity Connection Serviceability, Cisco Personal Communications Assistant, and clients that use the Connection REST APIs. This setting displays as enabled by default. **Note** The Network Service Audit Event Service must be running.

Field	Description
Enable Purging	The Log Partition Monitor (LPM) looks at the Enable Purging option to determine whether it needs to purge audit logs. When you check this check box, LPM purges all the audit log files in RTMT whenever the common partition disk usage goes above the high water mark; however, you can disable purging by unchecking the check box. If purging is disabled, the number of audit logs continues to increase until the disk is full. This action could cause a disruption of the system. A message that describes the risk of disabling the purge displays when you uncheck the Enable Purging check box. Be aware that this option is available for audit logs in an active partition. If the audit logs reside in an inactive partition, the audit logs get purged when the disk usage goes above the high water mark. You can access the audit logs by choosing **Trace and Log Central** > **Audit Logs** in RTMT. **Note** The Network Service Cisco Log Partitions Monitoring tool must be running.
Enable Log Rotation	The system reads this option to determine whether it needs to rotate the audit log files or it needs to continue to create new files. The maximum number of files cannot exceed 5000. When the Enable Rotation check box is checked, the system begins to overwrite the oldest audit log files after the maximum number of files is reached. **Tip** When log rotation is disabled (unchecked), audit log ignores the Maximum No. of Files setting.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. The default setting specifies 250. The maximum number specifies 5000.
Maximum File Size	Enter the maximum file size for the audit log. The file size value must remain between 1 MB and 10 MB. You must specify a number between 1 and 10.
Database Audit Log Filter Settings	
Enable Audit Log	When you check this check box, an audit log gets created for the Cisco Cisco Unified Communications Manager and Cisco Unity Connection databases. Use this setting in conjunction with the Debug Audit Level setting, which allows you create a log for certain aspects of the database.

Field	Description
Debug Audit Level	This setting allows you to choose which aspects of the database you want to audit in the log. From the drop-down list box, choose one of the following options. Be aware that each audit log filter level is cumulative. • **Schema** - Tracks changes to the setup of the audit log database (for example, the columns and rows in the database tables). • **Administrative Tasks** - Tracks all administrative changes to the Cisco Cisco Unified Communications Manager system (for example, any changes to maintain the system) plus all **Schema** changes. **Tip** Most administrators will leave the Administrative Tasks setting disabled. For users who want auditing, use the Database Updates level. • **Database Updates** - Tracks all changes to the database plus all **schema** changes and all **administrative tasks** changes. • **Database Reads** - Tracks every read to the system, plus all schema changes, administrative tasks changes, and database updates changes. **Tip** Choose the Database Reads level only when you want to get a quick look at the Cisco Cisco Unified Communications Manager or Cisco Unity Connection system. This level uses significant amounts of system resources and should be used only for a short time.
Enable Audit Log Rotation	The system reads this option to determine whether it needs to rotate the database audit log files or it needs to continue to create new files. When the Audit Enable Rotation option check box is checked, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached. When this setting check box is unchecked, audit log ignores the Maximum No. of Files setting.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. Ensure that the value that you enter for the Maximum No. of Files setting is greater than the value that you enter for the No. of Files Deleted on Log Rotation setting. You can enter a number from 4 (minimum) to 40 (maximum).
No. of Files Deleted on Log Rotation	Enter the maximum number of files that the system can delete when database audit log rotation occurs. The minimum that you can enter in this field is 1. The maximum value is 2 numbers less than the value that you enter for the Max No. of Files setting; for example, if you enter 40 in the Maximum No. of Files field, the highest number that you can enter in the No. of Files Deleted on Log Rotation field is 38.

Caution When enabled, database logging can generate large amounts of data in a short period, particularly if the debug audit level is set to **Database Updates** or **Database Reads**. This can result in a significant performance impact during heavy usage periods. In general, we recommend that you keep database logging disabled. If you do need to enable logging to track changes in the database, we recommend that you do so only for short periods of time, by using the **Database Updates** level. Similarly, administrative logging does impact on the overall performance of the web user interface, especially when polling database entries (for example, pulling up 250 devices from the database).