



Enterprise Chat and Email Administrator's Guide, Release 12.0(1) ES1

For Packaged Contact Center Enterprise

First Published: January 11, 2019

Last Updated: August 30, 2019

Americas Headquarters

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Enterprise Chat and Email Administrator's Guide: For Packaged Contact Center Enterprise. August 29, 2019

©2016-2019 Cisco Systems, Inc. All rights reserved.

Contents

- Preface12**
 - About This Guide 13
 - Change History 13
 - Related Documents 14
 - Communications, Services, and Additional Information 14
 - Cisco Bug Search Tool 14
 - Field Alerts and Field Notices 15
 - Documentation Feedback 15
 - Document Conventions 15

- Chapter 1: Console Basics16**
 - Important Administration Tasks 17
 - Key Terms and Concepts 17
 - Sharing of Business Objects 20
 - ECE Administration Space 20
 - At the Partition Level 20
 - At the Department Level 20
 - Navigating the Console 21

- Chapter 2: Packaged CCE Integration.....23**
 - About Packaged CCE Integration 24
 - Configuring Integration 24
 - Importing Data 26
 - Importing Media Routing Domains (MRDs) 26
 - Importing Users 27

- Chapter 3: Services29**
 - About Services, Service Processes, and Service Instances 30
 - Services 30

Unified CCE	30
Email Services	31
General Services	31
Workflow Services	31
Service Processes	32
Service Instances	32
Managing Service Processes	32
Creating Service Processes	32
Deleting Service Processes	33
Increasing the Number of Instances for Service Processes	33
Starting Service Processes	33
Stopping Service Processes	34
Managing Service Instances	34
Creating Service Instances	34
Deleting Service Instances	35
Starting Service Instances	36
Stopping Service Instances	36
Adding Aliases to Retriever Instances	37
Configuring an EAAS Service Instance	37
Configuring the MR Connection Port for an EAAS Service Instance	37
Configuring Security Settings for an EAAS Service Instance	37
Configuring an EAMS Service Instance	39
Configuring Peripheral Gateway and CTI Server Details	39
Configuring Security Settings for an EAMS Service Instance	40
Configuring Context Service for ECE	42

Chapter 4: Settings 44

About Settings	45
Settings to Configure After Installation	45
Mandatory Settings	45
Optional Settings	46
Configuring Settings	46
Configuring Partition Settings	46
Configuring Department Settings	46
Configuring App Settings for a Department	46
Configuring Language Settings for a Department	47
Chat Settings	47

Email Settings	47
Common Partition Settings	48
To: Address for Notifications from Services	48
From: Address for Notifications from Services	48
Installation Name	48
Web Server URL or Load Balancer URL	49
Maximum Number of Records to Display for Search.	49
Maximum Number of Records to Display for NAS Search	49
Common Settings for Departments.	50
Number of Activities Per Page	50
Date and Time Format.	50
Date Format.	51
Business Calendar Timezone	51
Agent Inbox Preference.	55
Refresh Interval (Seconds)	55
Number of Activities to be Monitored for Service Level	55
Chat - Daily Service Level Timezone.	55
Service Email and Chat Activities at the Same Time	59
Service Email and Phone Activities at the Same Time	59
Service Chat and Phone Activities at the Same Time.	60
Integration Settings	60
Proactive Monitoring Refresh Interval (Seconds).	60
Allow Transfer of Activities to Integrated Queues in Other Departments	60
Reason Code for Agent Not Ready	61
Maximum Wait Time for Login Response From UCCE (Seconds)	61
Enable Chat Queueing.	61
Chat Watchdog Interval (seconds)	62
Allow Transferring Email Activities to Agents Who Are Not Available.	62
Allow Transferring Chats to Agents Who Are Not Available	62
Allow Transferring Emails to Agents Who Are Not Logged in	62
Allow Supervisor to Join an Ongoing Chat Session	63
Agent Availability Settings After Completion of Call	63
Mark Agent Ready After Completion of Call	63
Event Reason Code to Track Agent State	63
Starvation Time for Activities.	64
Concurrent Task Limit Mappings by Media.	64
Media Class Names.	65

Partition Security Settings	65
Allow Users to Change Password	65
Inactive Time Out (Minutes)	65
Session Time Out (Minutes)	66
Allow Local Login for Partition Administrators	66
Customer Departmentalization	66
Password Complexity Policy	67
Security Settings for Cookies	67
Secure the Cookies Created by Application for Customer Websites	68
Departments Security Settings	68
Unsuccessful Attempts Time Frame	68
Unsuccessful Attempts Time Unit	68
Maximum Inactivity Time Unit	69
Maximum Inactivity Time Frame	69
Maximum Number of Unsuccessful Attempts	69
Maximum Number of Unsuccessful Timed Attempts	70
Logger Settings	70
Maximum Backups of Log Files	70
Default Size in MB	70
Default Log Level	71
Encrypt Log Files	71
Login Name Minimum Length	71
Login Password Case Sensitive	72
Password Life Time	72
Password Life Time Unit	72
Allow Users to Change Password	73
Unsuccessful Attempts Time Frame	73
Unsuccessful Attempts Time Unit	73
Maximum Number of Unsuccessful Timed Attempts	74
Maximum Number of Unsuccessful Attempts	74
Maximum Inactivity Time Frame	74
Maximum Inactivity Time Unit	75
Language Settings	75
KB Primary Language	75
Custom Language Label	76
Ignore Words with Only Upper Case Letters	76
Ignore Words with a Mixture of Upper and Lower Case Letters	76

Ignore Words with Only Numbers or Special Characters	76
Ignore Words that Contain Numbers	77
Ignore Web Addresses and File Names	77
Auto Spellcheck	77
Preferred Dictionary of the User	78
Auto Blockcheck	78
Split Contracted Words	78
Include Original Message Text During Spell Check	79
Chat - Auto Blockcheck	79
Chat - Auto Spellcheck	79

Chapter 5: Users.....80

About Users, Groups, Roles, and Actions	81
Users	81
User Groups.	81
User Roles	81
Actions	82
Permissions	82
Important Things to Note About Picking and Pulling Activities	83
Important Things to Note About Transferring Emails	83
Important Things to Note About Transferring Chats	84
What are the Actions Assigned to the Default Roles?	86
Partition Administrator	86
Administrator.	87
Agent	89
Agent (Read Only)	95
Supervisor	96
Supervisor (Read Only).	98
Managing User Roles	99
Creating User Roles	99
Assigning User Subroles	100
Copying User Roles	101
Restoring User Roles.	102
Deleting User Roles and Subroles.	102
Managing User Groups	103
Managing Users	104
Editing Department Users	105
Assigning Manager of Users.	107

Chapter 6: Configuring Security..... 109

Cross-Origin Resource Sharing 110

Enabling Cross-Origin Resource Sharing..... 110

About File Attachments 111

Configuring Attachment Settings 111

Rich Text Content Policies 112

Enabling and Disabling Rich Text Content Policies..... 113

Exporting and Importing Rich Text Content Policies..... 114

Configuring the Rich Text Content Policy File 115

 Adding a Common Regular Expression 115

 Allowing a New Tag..... 116

 Allowing a New Attribute for a Tag..... 116

 Adding a Rule for an Attribute Value..... 116

 Adding Validation for Attributes 117

 Allowing a New CSS Property 117

 Adding a Rule for a CSS Property Value 117

 Allowing Links in the Source Attribute of an iframe Tag 118

 Using a Plain Text Policy 119

Restoring Rich Text Content Policies..... 119

Chapter 7: ECE User Single Sign-On 120

About Single Sign-On (SSO) 121

Preparing to Configure Single Sign-On 121

 Integrating with Packaged CCE 121

 Configuring an Identity Provider 121

 Importing the SSL Certificate..... 122

Configuring Single Sign-On for Agents..... 123

Configuring SSO for Partition Administrators 125

Signing in 127

Troubleshooting 128

Chapter 8: Customer Single Sign-On 129

About Customer Single Sign-On 130

Customer Single Logout	130
Planning Your Configuration	131
Customer Single Sign-On Configuration	131
Creating Identity Providers	132
Configuring Customer Single Sign-On	135
Configuring Your Website for Secure Chat	136
Chapter 9: Departments	137
About Departments	138
Configuring Activity Transfer Between Departments	138
Chapter 10: Business Calendars	139
About Business Calendars	140
Managing Shift Labels	140
Creating Shift Labels	140
Deleting Shift Labels	141
Managing Day Labels	141
Creating Day Labels	141
Deleting Day Labels	142
Managing Business Calendars	143
Setting the Time Zone	143
Creating Business Calendars	143
Deleting Business Calendars	144
Managing Daylight Saving Changes	145
Chapter 11: Codes and Classifications	146
About Classifications	147
Managing Categories	147
Creating Categories	147
Deleting Categories	148
Managing Resolution Codes	148
Creating Resolution Codes	149
Deleting Resolution Codes	149
Managing Not Ready Reason Codes	150

Creating Not Ready Reason Codes	150
Enabling and Enforcing Not Ready Reason Codes	151
Deleting Not Ready Reason Codes	151
Chapter 12: Language Options	152
Setting the Language for the User Interface	153
About Dictionaries	154
Choosing a Default Dictionary	155
Creating Dictionaries	156
Approving and Rejecting Suggested Words	156
Viewing and Adding Approved Words	157
Viewing and Adding Blocked Words	157
Chapter 13: Macros	159
About Macros	160
Creating Business Object Macros	160
Creating Combination Macros	161
Deleting Macros	162
Chapter 14: Business Objects	163
Activity Object Attributes	164
Default Attributes	164
Custom Attributes	165
Adding Attributes to Screens	168
Chapter 15: Loggers	170
About Loggers	171
List of Processes Available in the System	172
Managing Logging for Processes	172
Viewing Logging Details for Processes	173
Changing the Logging Trace Levels for Processes	174
Enabling Logging for Specific Users	174

Chapter 16: Storage Management.....177

- About Storage Management 178
 - About Purge Jobs 178
 - What Can You Purge? 178
 - Who can Manage Purge Jobs? 178
 - Planning the Schedule of Purge Jobs. 178
 - Where can I View Current Storage Usage? 179
- Creating Purge Jobs 179
- Deleting Purge Jobs 180

Preface

- ▶ [About This Guide](#)
- ▶ [Change History](#)
- ▶ [Related Documents](#)
- ▶ [Communications, Services, and Additional Information](#)
- ▶ [Field Alerts and Field Notices](#)
- ▶ [Documentation Feedback](#)
- ▶ [Document Conventions](#)

Welcome to the Enterprise Chat and Email (ECE) feature, which provides multichannel interaction software used by businesses all over the world as a core component to the Unified Contact Center Enterprise product line. ECE offers a unified suite of the industry’s best applications for chat and email interaction management to enable a blended agent for handling of web chat, email and voice interactions.

About This Guide

Enterprise Chat and Email Administrator’s Guide introduces you to the ECE Administration and helps you understand how to use it to set up and manage various business resources.

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

Change	See	Date
Update of Document		August 2019
Updated information about generating certificates for EAAS and EAMS services	“Configuring Security Settings for an EAAS Service Instance” on page 37 and “Configuring Security Settings for an EAMS Service Instance” on page 40	
Adjusted steps for importing SSL certificate for Single Sign-On	“Importing the SSL Certificate” on page 122	
Configuration information and images have been corrected for SSO for partition administrators	“Configuring SSO for Partition Administrators” on page 170	
Update of Document for Release 12.0(1) ES1		April 2019
New custom attribute data types added.	“Activity Object Attributes” on page 164	
Role management section has been added to include new role management features	“Managing User Roles” on page 99	
Configuration information and images have been corrected for SSO for partition administrators	“Configuring SSO for Partition Administrators” on page 125	
New setting Chat - Daily Service Level Timezone added	“Chat - Daily Service Level Timezone” on page 55	
“Chat Entry Point” actions renamed to “Chat Resources”	“Administrator” on page 87 , “Supervisor” on page 96 , and “Supervisor (Read Only)” on page 98	

Change	See	Date
Initial Release of Document for Release 12.0(1)		January 2019
Updated link in Related Documents section to correct URL	“Related Documents” on page 14	
Clarified value options in Service Chat and Phone Activities at the Same Time setting	“Service Chat and Phone Activities at the Same Time” on page 60	

Related Documents

The latest versions of all Cisco documentation can be found online at <https://www.cisco.com>

Subject	Link
Complete documentation for Enterprise Chat and Email, for both Cisco Unified Contact Center Enterprise (UCCE) and Cisco Packaged Contact Center Enterprise (PCCE)	https://www.cisco.com/c/en/us/support/contact-center/enterprise-chat-email-12-0-1/model.html

Communications, Services, and Additional Information

- ▶ To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- ▶ To get the business impact you’re looking for with the technologies that matter, visit [Cisco Services](#).
- ▶ To submit a service request, visit [Cisco Support](#).
- ▶ To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- ▶ To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- ▶ To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Field Alerts and Field Notices

Cisco products may be modified or key processes may be determined to be important. These are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Log into www.cisco.com and then access the tool at <https://www.cisco.com/cisco/support/notifications.html>

Documentation Feedback

To provide comments about this document, send an email message to the following address:
contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Document Conventions

This guide uses the following typographical conventions.

Convention	Indicates
<i>Italic</i>	Emphasis. Or the title of a published document.
Bold	Labels of items on the user interface, such as buttons, boxes, and lists. Or text that must be typed by the user.
Monospace	The name of a file or folder, a database table column or value, or a command.
<i>Variable</i>	User-specific text; varies from one user or installation to another.

Document conventions

1 Console Basics

- ▶ [Important Administration Tasks](#)
- ▶ [Key Terms and Concepts](#)
- ▶ [Sharing of Business Objects](#)
- ▶ [Navigating the Console](#)

The Administrator Dashboard is the main management interface in the system. It helps administrators oversee their departments and manage system settings such as security, integration with Unified CCE, and language tools. Administrators can use the Administrator Dashboard to better tailor the system for their agents' needs, such as setting the department's time zone, or configuring the department's dictionary.

Important Administration Tasks

All business resources are set up and managed in the Administrator Dashboard. Some important tasks performed in this console include managing:

- ▶ Settings at the partition level and department level
- ▶ Integration with Cisco Unified CCE
- ▶ Loggers, Hosts, and Services
- ▶ Languages
- ▶ Custom Attributes
- ▶ User accounts
- ▶ Business calendars
- ▶ Chat infrastructure
- ▶ Email infrastructure
- ▶ Attachments
- ▶ Single Sign-On configurations
- ▶ Data adapters
- ▶ Classifications
- ▶ Dictionaries
- ▶ Macros

The next section describes each of these concepts in detail.

Key Terms and Concepts

Partitions and Departments

When the application is installed, a partition is created by the installation program, with one department in it. This department is called `Service` and can be renamed. The partition itself is labeled as `Partition` in the Administrator Dashboard. Note that departments are subordinate to the partition in the permissions hierarchy.

You can create additional departments to:

- ▶ Mirror your company's organization
- ▶ Create units with independent business processes

Settings

Settings are selective properties of business objects and are used to manage how the system works. For example, security settings help you configure the following properties of user passwords - the expiry time period for passwords, the characters allowed in passwords, and so on.

For more information, see [“Settings” on page 44](#).

Users

A user is an individual—an administrator, supervisor, or agent—possessing a distinct identification which is used to log in to Enterprise Chat and Email (ECE) in order to perform specific functions. Users are assigned roles and permissions, which enable them to perform various tasks. To make it easier to administer a large number of users, users can be organized into named groups.

Users consist of the following levels:

- ▶ **Partition level user:** This user is typically the administrator of the system who manages the business partition resources such as: services, departments, and so on.
- ▶ **Department level users:** Department level users have many different types of functions in the system. For example, the administrator manages resources such as, chat infrastructure, email infrastructure, and so on. while the agents handle customer interactions such as chat, emails, and so on.

For more information, see [“Users” on page 124](#).

User Roles

A role is a set of permissible actions for various business resources. An agent’s role, for instance, would include actions such as “Edit customer,” and “Add notes.” You can assign these roles to your employees as per the needs of your organization. To ease your task, the system comes with some default user roles. You can use these, and if required, reconfigure them to suit your needs. You can assign one or more roles to a group of users or an individual user.

For more information, see [“Users” on page 124](#).

User Groups

User groups are a collection of users that share similar functions or roles in the system. Groups make it much easier to manage user accounts. Like users, user groups can also be created in a department.

A standard user group called **All Users in** *Department_Name* is created in each department. Every new user added to the department is then automatically included in this group.

For more information, see [“Users” on page 124](#).

Calendars

Business calendars allow administrators to set up working and non-working hours and days for employees in their department. To create a business calendar, it is essential to first create shifts and day labels.

- ▶ **Shift labels:** According to the working hours of your company, you can organize various shifts for agents in your department. It also allows you to create shifts for holidays and extra working hours.
- ▶ **Day labels:** Day labels enable you to assign time slots to the shifts that you have created in the Shift label. You cannot create day labels, if you have not created shift labels first.

- ▶ **Calendars:** Use the day labels to form a calendar for the work days in a week. You can also specify exceptional days, such as holidays or an extra working day. Please note that you can have only one active calendar for each department.

For more information, see [“Business Calendars” on page 139](#).

Classifications

Classification is a systematic arrangement of resources comprising of categories and resolution codes. You can create and assign classifications to incoming activities or to knowledge base articles. Classifications are of two types:

- ▶ **Categories:** Categories are keywords or phrases that help you keep track of different types of activities.
- ▶ **Resolution codes:** Resolution codes are keywords or phrases that help you keep track of how different activities were fixed.

For more information, see [“Codes and Classifications” on page 146](#).

Dictionaries

Dictionaries refer to a list of words stored in the system for reference. Agents use dictionaries to check spellings in outgoing emails. Each department comes with multiple predefined dictionaries and one of them is configured as the default dictionary. A department can have only one default dictionary and it can be changed according to the business requirements.

For more information, see [“Language Options” on page 152](#).

Macros

Macros are shortcuts to perform oft-repeated tasks, such as, inserting customer names in emails, and so on. Macros save the response time to customer queries. Instead of repeatedly typing the frequently used sentences or phrases, users can simply add the appropriate macro. When the mail reaches the customer, the macro expands into the whole text. Macros are of two types - business object macros and combination macros.

You can create business object macros for:

- ▶ Activity data
- ▶ Case data
- ▶ Chat session data
- ▶ Contact person data
- ▶ Contact point data
- ▶ Customer data
- ▶ Email address contact point data
- ▶ Phone address data
- ▶ Postal address data
- ▶ User data
- ▶ Website data

You can create combination macros with multiple definitions. That is, you can combine multiple macros within a single macro. Multiple macros can be selected from business objects macros to create a combination macro.

For more information, see [“Macros” on page 159](#).

Sharing of Business Objects

This section lists the business objects available at different levels in the system and how they are shared in different consoles.

ECE Administration Space

At the Partition Level

The following objects are common for the entire application and all departments, and are managed by the partition administrators.

- ▶ Settings: Partition and department settings.
- ▶ Integration options: Integrate with Unified CCE.
- ▶ Security configuration: Cross-Origin Resource Sharing (CORS), Single-Sign On (SSO), rich text content policies, password policy.
- ▶ Service Instances: All departments in an installation use common services that are managed by partition administrators.
- ▶ Service Processes
- ▶ Loggers
- ▶ Language Settings: Set at Partition level and are available to users in all departments.

At the Department Level

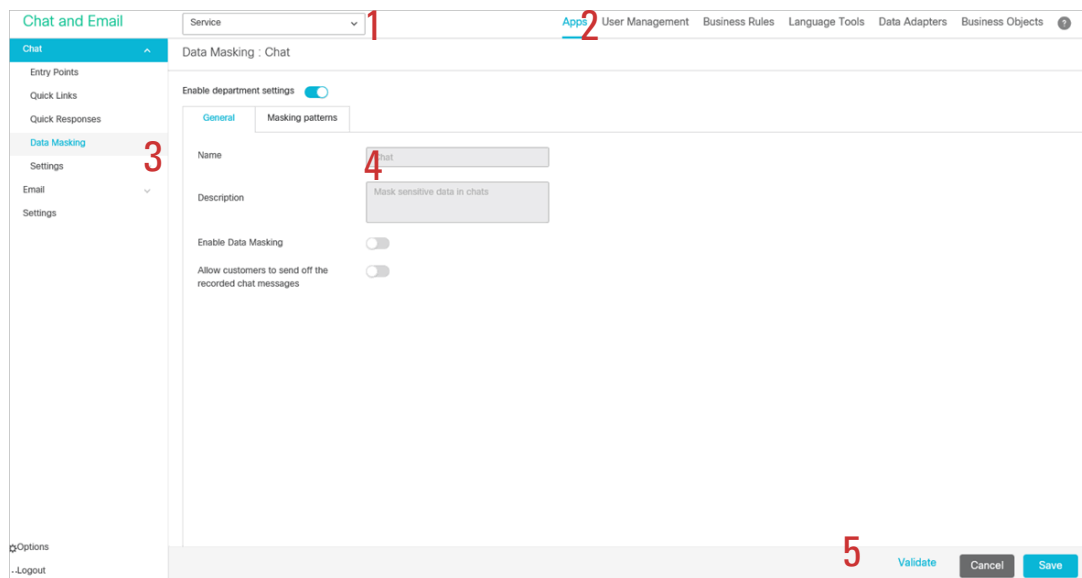
Access to these objects is controlled by roles and permissions.

- ▶ Settings
- ▶ Business calendars
- ▶ Classifications
- ▶ Dictionaries
- ▶ Macros
- ▶ Screen attributes

Navigating the Console

The console interface contains multiple areas, each containing different functions that follow a particular logical process. These areas adjust and update as you navigate through the console and click different options in the console menus. Therefore, when navigating the console, it is important to keep a step-by-step approach in mind.

The image below marks the different functional areas of the console and the order in which they should be accessed when making any modifications to the application.



Elements of the Administrator Dashboard available in a department

These items are displayed as follows:

- 1. Partition and Department menu:** This dropdown menu permits switching between departments or partitions, such as changing from Partition to department. You can choose departments to be adjusted individually, or adjust them all at once via the partition.
- 2. Top Menu:** The top-level navigation menu. The options contained here change depending on the department or partition selected prior. Clicking an option in the Top menu changes the available options displayed in the Left menu.
- 3. Left Menu:** Tools and settings contained within the Top menu options appear here. Once you have selected an option from the Top menu, use this menu to navigate to through the different sections of the application you can configure.
- 4. Workspace Area:** Upon selecting an option from the Left menu, the space in the center of the screen refreshes. Any modifications or changes can be made here.
- 5. Workspace Toolbar:** Permits you to save or cancel any changes that you have made. Note that there may be other buttons available here, depending on the workspace options you previously selected. Remember to save your changes before moving on.

The console follows a particular logic path when it comes to navigation and displaying information. When working in the console, you should follow the process of navigating the console in the order of these different sections.

In most instances, you start in the upper left section of the desktop to verify that you are working in the correct department or at the partition level. Next, you want to select an option from the Top menu and navigate the Left menu to select the setting or configuration you wish to adjust. Doing so refreshes Workspace Area, where you can select the individual functions of the configuration and make your necessary adjustments. When you are finished with your changes, use the buttons in the Workspace Toolbar to finalize your modifications.

Packaged CCE Integration

- ▶ [About Packaged CCE Integration](#)
- ▶ [Configuring Integration](#)
- ▶ [Importing Data](#)

About Packaged CCE Integration

The process of integrating ECE with Cisco Packaged CCE can vary based on how ECE was installed. Some of the steps listed below may have been performed already during the installation process and may not be necessary. For more information, see *Enterprise Chat and Email Installation Guide*.

Configuring Integration

To integrate ECE with Unified CCE:

1. In the partition-level Top menu, click the **Integration** option.
2. In the Left menu, navigate to **Unified CCE > Unified CCE**.
3. In the Unified CCE Details space, on the AWDB Details tab, provide information for the following fields under the Primary AWDB section:
 - **Authentication:** From the dropdown menu, select the desired authentication type. Options include: **SQL Server Authentication** and **Windows Authentication**.
 - **Unified CCE Administration Host Name:** The server name or IP address of the host on which Packaged CCE or Unified CCE is installed.
 - **Active:** Click this toggle to enable the configuration.
 - **SQL Server Database Name:** The name of the AWDB database.
 - **Port Number:** Set the value to match the database port configured in MSSQL for this database. By default the value is set to 1433.
 - **Database Administrator Login Name:** The database administrator's user name.
 - **Database Administrator Login Password:** The database administrator's password.

- **Maximum Capacity:** The maximum number of allowed connections to be made to the AWDB. By default, this is set to 360.


The screenshot displays the 'Unified CCE Details' configuration page. The 'Primary AWDB' section is active, showing the following fields:


- Authentication*: SQL Server Authentication
- Unified CCE Administration Host Name*: 10.10.19.70
- Active:
- SQL Server Database Name*: na_awdb
- Port Number*: 1433
- Database Administrator Login Name*: sa
- Database Administrator Login Password*: *****
- Maximum Capacity*: 360

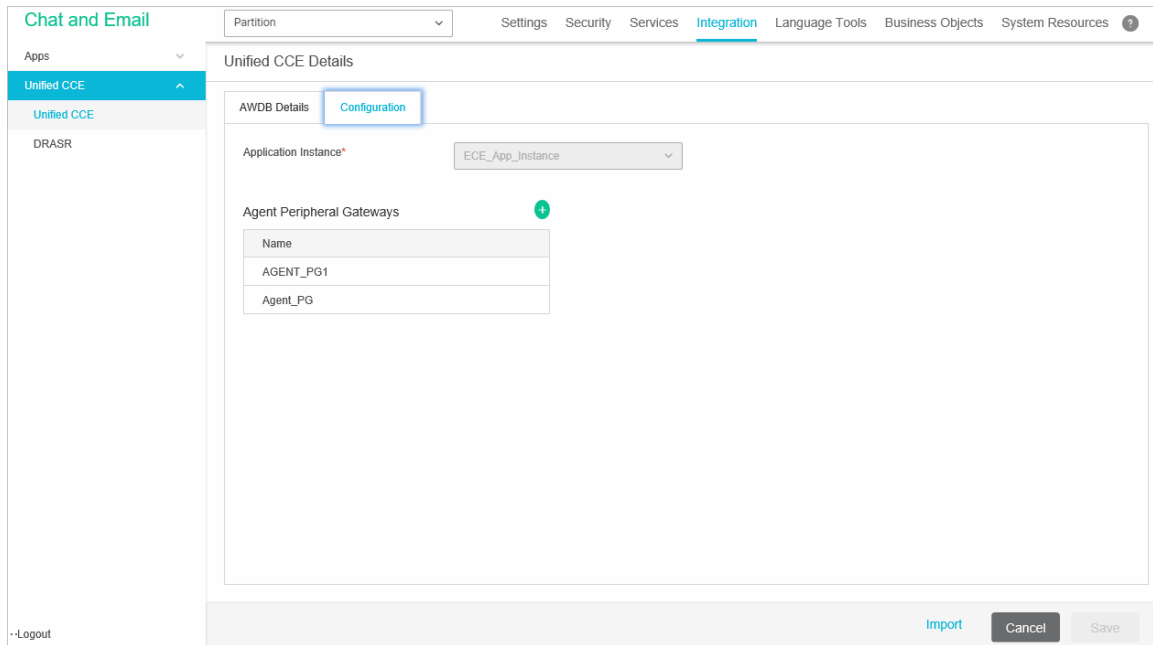
The 'Secondary AWDB' section is currently empty. At the bottom of the form, there are buttons for 'Import', 'Cancel', and 'Save'. The 'Save' button is currently greyed out.

Provide the primary AWDB server details

4. If you have a secondary AWDB database and wish to apply it to your integration, click the **Secondary AWDB** section and provide the necessary details.
5. Click the **Save** button. Note that the Save button only becomes available if the inputted information is correct - incorrect information causes it to be greyed out and inaccessible.
6. Next, select the **Configuration** tab and set the following:
 - **Application Instance:** Select an instance from the dropdown field.

- **Agent Peripheral Gateways:** Click the **Search and Add**  button to add any desired gateways for agent peripherals.

 **Important:** When you save your changes, your system is permanently connected to your Unified CCE installation. This cannot be undone.



The screenshot shows the 'Unified CCE Details' configuration page. The 'Configuration' tab is active. The 'Application Instance' is set to 'ECE_App_Instance'. Under 'Agent Peripheral Gateways', a table lists the following gateways:

Name
AGENT_PG1
Agent_PG

At the bottom right of the configuration area, there are buttons for 'Import', 'Cancel', and 'Save'.

Provide configuration details

7. Click the **Save** button. Your system is now connected with Unified CCE. To complete the integration, you must import the MRDs and users from the Unified CCE system. For more information, see [“Importing Data”](#) on page 26.

Importing Data


Before the system can become fully integrated with your Unified CCE deployment, data from the Unified CCE must be imported to the application. The following objects can be imported from Unified CCE:

- ▶ **Media Routing Domains (MRDs):** These are shown as queues upon importing to a selected department.
- ▶ **Users:** These are shown as users upon importing to a selected department.

Importing Media Routing Domains (MRDs)

The MRDs available for importing are decided based on the media classes configured in the partition level setting: Media Class Names ([page 65](#)). If you do not see the correct MRDs available for importing, check to make sure that the Media Classes names configured in the setting match the configuration in Unified CCE. Note that media class names are case sensitive.

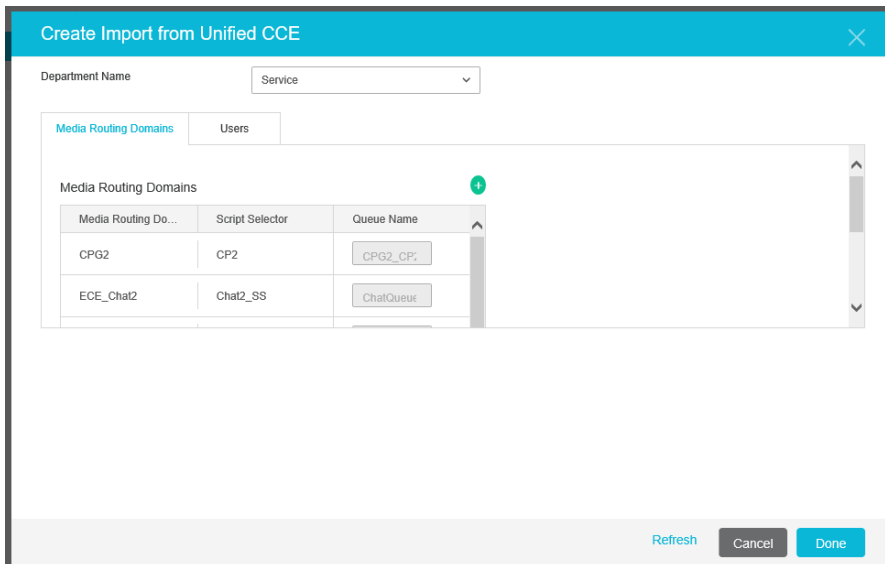
To import MRDs:

1. In the partition-level Top menu, click the Integration option.
2. In the Left menu, navigate to **Unified CCE > Unified CCE**.
3. In the Unified CCE Details space, click the **Import** button. The Create Import from Unified CCE window appears.
4. Select the department to which you are importing the MRDs from the Department Name dropdown.
5. Under the Media Routing Domains tab, click the **Search and Add**  button and select the MRDs you wish to import.



Important: Any MRDs without script selectors or MRDs that have already been imported are not shown.

When an MRD is added to the system, a queue is created. In the import window, you can change the names of the queues to how you want them to appear in the application.



Media Routing Do...	Script Selector	Queue Name
CPG2	CP2	CPG2_CP2
ECE_Chat2	Chat2_SS	ChatQueue


Import MRDs

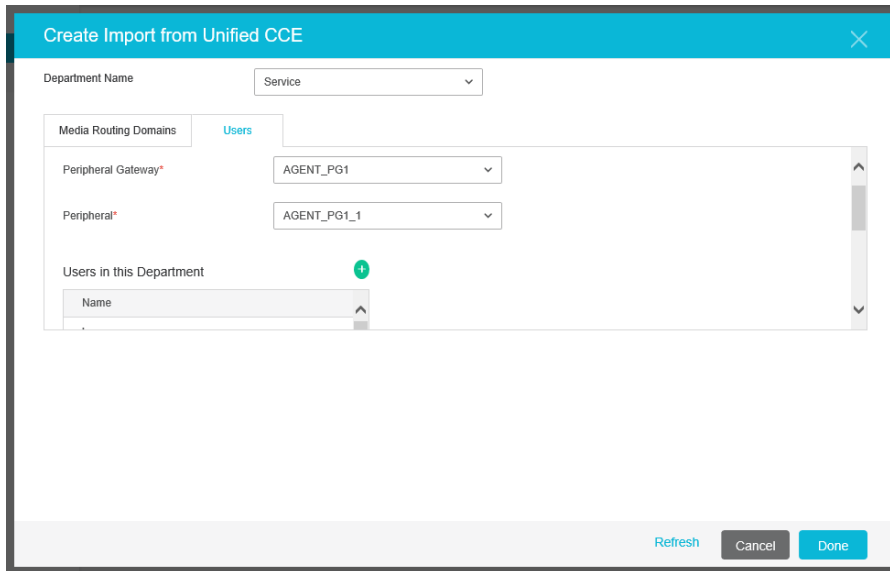
6. Click the **Done** button.

Importing Users

To import Unified CCE users:

1. In the partition-level Top menu, click the **Integration** option.
2. In the Left menu, navigate to **Unified CCE > Unified CCE**.
3. In the Unified CCE Details space, click the **Import** button. The Create Import from Unified CCE window appears.
4. Select the department to which you are importing the users from the Department Name dropdown.

5. In the Users tab, set the following:
 - Select the peripheral gateway from the dropdown.
 - Select the appropriate peripheral.
 - Select the users from the Users in this Department list that you wish to import. If a desired user does not appear in this list, click the **Add and Select**  button and then add their name in the Add Users in this Department pop-up window.



Import users

6. Click the **Done** button.

Once users have been imported to ECE, they can log into the application using their Unified CCE login credentials. The login credentials of a user in ECE is case-sensitive and must match their Unified CCE credentials.
7. Newly imported users may still need to have user roles assigned. For more information about assigning user roles, see [“Editing Department Users”](#) on page 105.

3 Services

- ▶ [About Services, Service Processes, and Service Instances](#)
- ▶ [Managing Service Processes](#)
- ▶ [Managing Service Instances](#)
- ▶ [Configuring an EAAS Service Instance](#)
- ▶ [Configuring an EAMS Service Instance](#)
- ▶ [Configuring Context Service for ECE](#)

About Services, Service Processes, and Service Instances

Services

Services accomplish specialized functions within the system. For example, a dispatcher service is responsible for sending out emails. Similarly other services perform varied functions for the system. Each service, has a service process and a corresponding service instance. Multiple processes and instances can be created for some of the services.

Services are of following types.

- ▶ Unified CCE
 - Context Service
 - EAAS
 - EAMS
- ▶ Email services
 - Dispatcher service
 - Retriever service
- ▶ General service
 - Archive (Enterprise) service
 - Report service
 - Scheduler service
- ▶ Workflow services
 - Activity Pushback service
 - Alarm service
 - Workflow Cache service
 - Workflow Engine service

Unified CCE

- ▶ **Context Service:** In addition to the standard services, the application comes equipped with the Context Service service. This service allows for the synchronization of specific activity and customer information between the ECE database and the Cisco cloud context service database. The application must be registered and integrated with Unified CCE before the Context Service can be properly configured.

Administrators can use the **Factory Reset** option to reset and reestablish the connection between ECE and Context Service. This may be required when significant updates are made to Context Service. Click this button only when directed to do so by Cisco support. No information is lost from Context Service when you use the factory reset capability.

- ▶ **EAAS:** The external agent assignment service (EAAS) routes email, chat, callback, and delayed callback activity requests to Unified CCE. EAAS sends a request to Unified CCE for every activity that arrives into an external assignment queue, for the identification of an agent who is available to handle the given activity.

If the EAAS service is not running, customers cannot start the chat, callback, and delayed callback sessions and the off hours page is displayed to them. This service can have only one process and instance and neither can be deleted.

- ▶ **EAMS:** The external agent message service (EAMS) initiates and maintains a reliable channel of communication with the Agent Peripheral Gateway (PG)/ARM interface of Unified CCE. Each instance of this service is dedicated to communicating with an Agent PG, and reports the current state of agents and tasks to the appropriate Agent PG (i.e. the Agent PG to which the relevant agent belongs). These events are then used by Unified CCE for reporting purposes.

Email Services

- ▶ **Dispatcher service:** This service turns the messages that agents write into emails and sends them out of your Mail system. The dispatcher service acts as a client that communicates with SMTP or ESMTP servers.
- ▶ **Retriever service:** This service is a POP3 or IMAP client that fetches incoming emails from servers. It then turns them into messages that agents can view in their mailbox.

General Services

- ▶ **Archive (Enterprise) service:** The application uses a partitioning feature provided by the databases to manage growth of high volume objects in active and reports databases. When the application is installed, two partitions are created for the objects in these databases. Groups comprised of multiple partitioning steps are scheduled to run daily, weekly, and monthly. Every time these groups are run, new partitions are added. This ensures that there are always additional partitions available.

A notification email about the success or failure to add a new partition is sent to the email address specified in the partition level setting “To: address for notifications from services”. If a step within group fails, the service attempts to resume the group from same step the next day until it succeeds.
- ▶ **Scheduler service:** This service schedules the messaging and reminder system.

Workflow Services

- ▶ **Activity Pushback service:** This service is a continuous service that pushes agents’ unpinned activities, back into the queue after they have logged out. Those activities get reassigned to other users in the queue.
- ▶ **Alarm service:** This service runs at specific time intervals. While processing a workflow, it determines if any alarm conditions are met. It then performs the relevant actions including sending out any configured notifications or alarms to the user.
- ▶ **Workflow Cache service:** This service maintains and updates the Rules Cache, KB Cache, and Queue Cache in the system. These caches are accessed by all rules engine instances before executing rules.
- ▶ **Workflow Engine service:** This service is the main Rules engine. It uses the cache produced by Rules Cache service, and applies rules on activities on the basis of workflows. This service handles the general, inbound, and outbound workflows.

Service Processes

At least one service process for each service should be running to enable the basic functioning of the system. Service processes can be set to start automatically, or can be started manually by the system administrator.

Service Instances

Service instances are derivatives of service processes. Configure service instances within the business partition to accomplish specific functions. For example, in an installation that is used to manage five different email aliases you could configure two service instances of the retriever service process and assign three aliases to one instance and two aliases to the other.

Managing Service Processes

For each service, a service process is provided in the system. In addition to these you can create new service processes. You have to start a service process before the system can use that process.

Creating Service Processes

Before creating a service process, estimate your system requirements well. Depending on your needs, you can create the number and type of service processes you require.


To create a service process:

1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to create a new process.
3. In the workspace dropdown, click the **Processes** option.
4. Click the **New** button.
5. In the Create Process space, under the General tab, provide the following details.
 - **Name:** Type a name for the process. This is required information.
 - **Maximum Number of Instances:** Type the maximum number of instances this service process can have. This option is available only for those services that can have more than one instance.
 - **Description:** Provide a brief description.
 - **Start type:** From the dropdown list, select a start type for the service process. The following three options are available:
 - **Manual:** The service process has to be started manually by the system administrator.
 - **Automatic:** The service process is started automatically by the system when the application is started.
6. Click the **Save** button

Deleting Service Processes

The system allows you to delete certain service processes that are not required in the system. Before you delete the service process, make sure it is not running. Not all service processes in the system can be deleted.

To delete a service process:

1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to delete a process.
3. In the workspace, if the process is running, select the service process and stop the service process.
4. Hover your mouse over the process and click the **Delete**  button.

Increasing the Number of Instances for Service Processes

The system allows you to create more than one instance of certain service processes to help increase performance. As a system administrator you can create these instances. The following services can have more than one instance:

- ▶ Email services: Retriever and Dispatcher
- ▶ Workflow service: Workflow Engine
- ▶ External Agent Message Service (EAMS)

You can also set the maximum number of service instances that can be created for each of the above service processes.

To increase the number of instances for a service process:

1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to increase the number of service instances.
3. Process space, under the General tab go to the **Maximum number of instances** field, and type the maximum number of instances this service process can have.
4. Click the **Save** button.
5. Stop and start the service process.

Starting Service Processes

Unless a service process is configured to start automatically when a system is running, you have to manually start the particular process when you require it. Every time you start the service process, you need to manually start the instances for that service.

To start a service process:

1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to start a process.
3. Browse to the process and click the checkbox next to it.

4. Click the **Actions** button and select **Start** option.

The process starts on the selected hosts.

Stopping Service Processes

Stop the service process if it is not needed. This frees up system resources. Sometimes you may be required to stop and start a service process after making changes to its properties. For example, when you increase or decrease the number of service instances that can be associated with a particular service process, you must stop and start that service process.

To stop a service process:

1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to stop a process.
3. Browse to the process and click the checkbox next to it.
4. Click the **Actions** button and select **Stop** option.

The process stops working on the selected hosts.



Important: Once the service process is stopped, all service instances also stop.

Managing Service Instances

Service instances are specific to the business partition. You can manage all the activities related to instances from the business partition. You can also create and delete instances as required.

Creating Service Instances

By default, one service instance is provided for each service in the system. The system allows you to create additional service instances for certain services. The services that can have more than one instance running at a time are:


- ▶ Email services: Retriever and Dispatcher
- ▶ Workflow service: Workflow Engine
- ▶ External Agent Assignment Service (EAAS)
- ▶ External Agent Message Service (EAMS)

To create a service instance:

1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to create a new instance.
3. Click the **New** button.

4. In the Create Instance space, under to the General tab and provide the following details.
 - **Name:** Type a name for the instance. This is required information.
 - **Description:** Provide a brief description.
 - **Start type:** From the dropdown list, select a start type for the instance. The following two options are available.
 - **Manual:** The service instance has to be started manually by the system administrator.
 - **Automatic:** The service instance is started automatically by the system when the application is started.
 - **Use Process:** Select the process to which the service instance is applied from the dropdown.

Create a new instance

5. For retriever service instances, there is an additional Input tab. Under the Input tab, click the **Search and Add**  button to select an available email alias and add it to the retriever instance. For more details, see [“Adding Aliases to Retriever Instances” on page 37](#).
6. For the EAAS Service, refer to the following section for more details: [“Configuring an EAAS Service Instance” on page 37](#).
7. For the EAMS, refer to the following section for more details: [“Configuring an EAMS Service Instance” on page 39](#)
8. Click the **Save** button.




Important: The number of instances for a given service should tally with the maximum number of instances defined for the service process in Shared Resources. For details, refer to the following section: [“Increasing the Number of Instances for Service Processes” on page 33](#).

Deleting Service Instances

You can delete a service instance if it is not required anymore or occupies system resources.

To delete a service instance:

1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to delete an instance.

3. In the workspace, if the instance is running, select the service process and stop the service instance.
4. Hover your mouse over the instance and click the **Delete**  button.

Starting Service Instances

Unless a service instance is configured to start automatically when a system is running, you have to manually start the particular instance when you require it. Every time you start the service process, you need to manually start the instances for that service in the business partition.

When you create additional instances for a service, you can start those instances only after you do the following.

- ▶ Increase the number of instances that can be associated with the service process. And, restart the service process. For details, see [“Increasing the Number of Instances for Service Processes” on page 33](#).

To start a service instance:

1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to start an instance.
3. Browse to the instance and click the checkbox next to it.
4. Click the **Actions** button and select **Start** option.

The instance starts running.



Important: More than one service instance cannot be started on a business partition, except for Retriever, Dispatcher, EAMS, Workflow service: Workflow Engine.

Stopping Service Instances

Stop the service instance if it is not needed, freeing up system resources. Changing a server instance’s properties may also require a restart of the server instance. For example, when you add an alias to a retriever instance, you need to stop and start the retriever instance and all the dispatcher instances for the business partition.

To stop a service instance:


1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to stop an instance.
3. Browse to the instance and click the checkbox next to it.
4. Click the **Actions** button, click the **Stop** option.

The instance stops running.

Adding Aliases to Retriever Instances

You can start the retriever instance only after you add an alias to the retriever instance. A retriever instance can have any number of aliases, but one alias can be associated with only one instance.

To add aliases to a retriever instance:

1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, navigate to **Email > Retriever**.
3. In the Retriever space, click the dropdown menu and select the **Instances** option.
4. Click the Retriever instance you want to use and click the **Input** tab.
5. Under the Input tab, click the **Search and Add**  button to select an available email alias and add it to the retriever instance.
6. Click the **Save** button.
7. Stop and start the retriever instance. The retriever picks emails from the alias only after you restart the retriever instance.

Configuring an EAAS Service Instance

In addition to the standard fields mentioned in the [“Creating Service Instances” on page 34](#), the EAAS service instance has additional configuration steps to improve the quality and security of the connection.

Configuring the MR Connection Port for an EAAS Service Instance

This is the port used by ECE when initializing a server socket connection with Unified CCE to listen to incoming connections from the Media Routing Peripheral Gateway (MR PG) of Unified CCE and is a pre-requisite for sending new activity requests for routing through Unified CCE.

The port number entered here should match the corresponding value that is entered at the time of setting up the Media Routing Peripheral Interface Manager (MR PIM) in Unified CCE. Use a port number greater than 2000.

Enter this value manually *after* starting ECE, and *before* starting the EAAS process and instance.

If this value is modified later (based on a modification within the MR PIM) you must restart both the service process and the instance.

Configuring Security Settings for an EAAS Service Instance

The EAAS service instance has security settings that can be configured to protect personally identifiable information that passes through the integrated system.



Important: If the application is integrated with a version prior to Packaged CCE 12.0(1), the security settings for EAAS cannot be enabled.

Before configuring security settings for an EAAS service instance, you need to:

- ▶ **Generate a security certificate for the Media Routing servers** that will be used by the instance. A certificate for the primary media routing (MR) server is mandatory and a certificate for the secondary MR server is optional. These certificates are generated and can be obtained in the Cisco Unified CCE environment. For more information, consult *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise*.
- ▶ **Generate a private key in the ECE environment.** To generate a private key:
 - In the ECE environment, open command prompt (`cmd.exe`)
 - Go to the file location: `application_server\ECE_installation_directory\Java\jdk\bin`
 - Execute the command: `keytool -genkey -keyalg RSA -alias ecesaml -keystore ecesaml.jks -validity validity_in_days`
validity_in_days indicates the number of days the certificate should be valid.
 - Provide the necessary details for the security certificate.

This generates the JKS file in the bin folder to be used in the configuration process.


To configure security settings for an EAAS service instance:

1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, navigate to **Unified CCE > EAAS**.
3. Select **Instances** from the dropdown and select the EAAS instance you wish to edit.
4. In the Edit space, under the General tab, provide the following:
 - **Name:** Type a name for the instance. This is required information.
 - **Description:** Provide a brief description.
 - **Start type:** From the dropdown list, select a start type for the instance. The following two options are available.
 - **Manual:** The service instance has to be started manually by the system administrator.
 - **Automatic:** The service instance is started automatically by the system when the application is started.
 - **Use Process:** Select the process to which the service instance is applied from the dropdown. This is automatically selected and cannot be changed.
 - **MR Connection Port:** Provide the port number for the Media Routing Peripheral Gateway.

The screenshot shows the 'Edit : EAAS-instance' configuration page in the Cisco Unified CCE Administration console. The 'General' tab is selected, and the following fields are visible:

- Name***: EAAS-instance
- Description**: This instance connects to Unified CCE Media Routing PIM to make routing decisions for entities.
- Start Type***: Manual
- Use Process***: Any Process
- MR Connection Port**: 0

Edit the general settings of the EAAS instance

5. Click the **Security** tab and provide the following:
 - **Enable Security:** Click the toggle to enable or disable the security configuration.
 - **MR Certificate:** Provide the security certificate of the primary Media Routing server.
 - **Secondary MR Certificate:** Provide the security certificate of the secondary Media Routing server.
 - **Private Key:** Provide the following details from the private key file that was generated in the ECE environment:
 - **File Name and Path:** Provide the file path of your Java Keystore File. This file will be in .jks format and contains the decryption key the application needs to access files secured by the instance.
 - **Alias name:** The unique identifier for the decryption key.
 - **Keystore password:** The password required for accessing the Java Keystore File.
 - **Key password:** The password required for accessing the Alias' decryption key.
 - **Public Key:** Provide the details to Private Key field generates a public key here. This certificate must be installed on the Unified CCE environment. For more information about installing the public key on the Unified CCE environment, consult your Cisco Unified CCE documentation.
 - **Supported Cipher Suites:** Click the **Search and Add**  button and select one or more strings of the desired cipher suite names, separated by colons. The suite names must be in TLS format. For more information about which cipher suite names are accepted, consult your Cisco Unified CCE documentation.
6. Click the **Save** button. You must restart the service process and instances after saving your changes.

Configuring an EAMS Service Instance

In addition to the standard fields mentioned in the [“Creating Service Instances” on page 34](#), the EAMS service instance has additional configuration steps to improve the quality and security of the connection.

Configuring Peripheral Gateway and CTI Server Details

While configuring an EAMS service instance, under the general tab the following fields are can be configured:

- ▶ **Agent PG:** This is a required field. From the dropdown list, select the Agent PG to which the instance should connect. For auto-configured instances, this field is configured automatically and shows the name of the Agent PG that was selected in the integration wizard.

Below, provide the details of the CTI server in the following fields. For more information about obtaining this information, consult your Cisco Unified CCE documentation.

- ▶ **Primary CTI Server Address:** Provide the IP address of the primary CTI server that is used to handle call activities. This is a required field.
- ▶ **Primary CTI Server Port:** This value is governed by Unified CCE. Provide the value that was provided during the integration process. Values can range from 1 to 65535. This is a required field.
- ▶ **Secondary CTI Server Address:** Provide the IP address of the failover server. This field is not required.
- ▶ **Secondary CTI Server Port:** Provide the port number of the failover server. This field is not required.

After you have configured the required values and saved your changes, you must restart the service process and instances.

Configuring Security Settings for an EAMS Service Instance

The EAMS service instance has security settings that can be configured to protect personally identifiable information that passes through the integrated system.



Important: If the application is integrated with a version prior to Packaged CCE 12.0(1), the security settings for EAMS cannot be enabled.

Before configuring security settings for an EAMS service instance, you need to:

- ▶ **Generate a security certificate for the CTI servers** that will be used by the instance. A certificate for the primary CTI server is mandatory and a certificate for the secondary CTI server is optional. These certificates are generated and can be obtained in the Cisco Unified CCE environment. For more information, consult your Cisco Unified CCE documentation.
- ▶ **Generate a private key in the ECE environment.** To generate a private key:
 - In the ECE environment, open command prompt (`cmd.exe`)
 - Go to the file location: `application_server\ECE_installation_directory\Java\jdk\bin`
 - Execute the command: `keytool -genkey -keyalg RSA -alias ecesaml -keystore ecesaml.jks -validity validity_in_days`
validity_in_days indicates the number of days the certificate should be valid.
 - Provide the necessary details for the security certificate.

This generates the JKS file in the bin folder to be used in the configuration process.

To configure security settings for an EAMS instance:

1. In the partition-level Top menu, click the **Services** option.
2. In the Left menu, navigate to **Unified CCE > EAMS**.
3. Select **Instances** from the dropdown and select the EAMS instance you wish to edit.


- In the Edit space, under the General tab, provide the necessary information. For more information, see “Configuring Peripheral Gateway and CTI Server Details” on page 39.

The screenshot shows the 'Chat and Email' configuration page for instance '1'. The 'General' tab is active, displaying the following fields:

- Name***: 1
- Description**: Enter Description
- Start Type***: Manual
- Agent PG**: Agent_PG
- Primary CTI Server Address***: 10.10.10.10
- Primary CTI Server Port***: 1111
- Secondary CTI Server Address**: (empty)
- Secondary CTI Server Port**: 0
- Use Process***: Any Process

At the bottom right, there are buttons for 'Test', 'Cancel', and 'Save'. A 'Logout' link is visible at the bottom left.

Provide the necessary general details for the instance

- Click the **Security** tab and provide the following:
 - **Enable Security:** Click the toggle to enable or disable the security configuration.
 - **CTI Server Certificate:** Provide the security certificate of the primary CTI server.
 - **Secondary CTI Server Certificate:** Provide the security certificate of the secondary CTI server.
 - **Private Key:** Provide the following details from the private key file that was generated in the ECE environment:
 - **File Name and Path:** Provide the file path of your Java Keystore File. This file will be in .jks format and contains the decryption key the application needs to access files secured by the instance.
 - **Alias name:** The unique identifier for the decryption key.
 - **Keystore password:** The password required for accessing the Java Keystore File.
 - **Key password:** The password required for accessing the Alias' decryption key.
 - **Public Key:** Provide the details to Private Key field generates a public key here. This certificate must be installed on the Unified CCE environment. For more information about installing the public key on the Unified CCE environment, consult your Cisco Unified CCE documentation.
 - **Supported Cipher Suites:** Click the **Search and Add**  button and select one or more strings of the desired cipher suite names, separated by colons. The suite names must be in TLS format. For more information about which cipher suite names are accepted, consult your Cisco Unified CCE documentation.
- After you have configured the required values and saved your changes, you can click the **Test** button to verify your settings are valid and secure.

- Click the **Save** button. You must restart the service process and instances after saving your changes.

Configuring Context Service for ECE



Important: This section only applies to systems using Cisco Context Service.

The ECE application must be registered from Unified CCE or Packaged CCE before the Context Service can be properly configured. The Enterprise Chat and Email Context Service must also be registered with Finesse and Unified CCE or Packaged CCE.

Before you configure and register Context Service, integrate the ECE application with Unified CCE, HCS for Contact Center, or Packaged CCE. The application must be integrated with Unified CCE before the Context Service can be properly configured. For information about integrating the ECE application, see “[Packaged CCE Integration](#)” on page 23.

For instructions on how to configure and register Context Service for:	See the Context Service section in:
Unified CCE solutions	Cisco Unified Contact Center Enterprise Features Guide
Packaged CCE solutions	Cisco Packaged Contact Center Enterprise Features Guide
HCS for Contact Center solutions	Configuring Guide Cisco HCS for Contact Center

To configure the Context Service:

- In the partition-level Top menu, click the **Services** option.
- In the Left menu, navigate to **Unified CCE > Context Service**.
- Select Processes from the dropdown menu and select the process you wish to edit.
- In the Edit space, under the General tab, adjust the following if necessary:
 - Proxy Server URL:** When the ECE Services Server or the ECE All-In-One server (in PCCE installations) is behind a firewall and does not have direct access to the internet, a proxyURL should be provided so the server can connect to Cisco Context Service. The URL should be in the format `http://ProxyServerName:Port` or `https://ProxyServerName:Port`
- Click the **Save** button.



Important: The Context Service process must be running before the instance can be properly configured.

- Click the checkbox next to the Context Service process.
- Click the **Actions** button and select the **Start** option.
- Click the dropdown menu and select **Instances**.
- Select the Context Service instance.

10. In the Edit space, the General tab, adjust the following if necessary:
 - **Name:** Name of the Instance.
 - **Description:** Description of the Instance.
 - **Start type:** From the dropdown list, select a start type for the instance. The following two options are available.
 - **Manual:** The service instance has to be started manually by the system administrator.
 - **Automatic:** The service instance is started automatically by the system when the application is started.
11. Click the **Save** button.
12. Click the checkbox next to the Context Service instance.
13. Click the **Actions** button and select the **Start** option.



Important: Once Context Service is configured and running in ECE, if Context Service is modified on the Unified or Packaged CCE environment, the Context Service instance must be restarted.



Settings

- ▶ [About Settings](#)
- ▶ [Configuring Settings](#)
- ▶ [Common Partition Settings](#)
- ▶ [Common Settings for Departments](#)
- ▶ [Integration Settings](#)
- ▶ [Partition Security Settings](#)
- ▶ [Departments Security Settings](#)
- ▶ [Logger Settings](#)
- ▶ [Language Settings](#)

About Settings

Settings are selective properties of business objects and are used to configure the way system works. For example, security settings help you to configure the following properties of user password - the expiry time period for passwords, the characters allowed in passwords, and so on. Some settings can only be managed at the global level while others can be set at the department level.

Editing permissions for select settings can be transferred from the global level to the department level. These settings can be identified by the **Editable at lower level** option next to them. Checking the box next to the option grants users editing access to that particular setting. Administrators still retain editing abilities and can revoke editing permissions at any time by going back and un-checking the option box.

There are several different types of settings that can be adjusted:

- ▶ Chat settings
- ▶ Email settings
- ▶ Common settings
- ▶ Integration settings
- ▶ Security settings
- ▶ Serviceability settings
- ▶ Logger settings
- ▶ Language settings

Settings to Configure After Installation

There are two types of these settings:

1. **Mandatory settings:** These settings must be configured before using the application.
2. **Optional settings:** These settings are not mandatory, but are helpful and configuring them is likely to be useful for your business.

Mandatory Settings

At the Partition Level

Configure the following items under **Settings > Common**. See the *Enterprise Chat and Email Administrator's Guide to Chat and Email Resources* for more information.

- ▶ To: address for notifications from services
- ▶ From: address for notifications from services
- ▶ Default SMTP server settings

At the Department Level

Configure the following setting for each department under **Email > Settings**. See the *Enterprise Chat and Email Administrator's Guide to Chat and Email Resources* for more information.

- ▶ From email address for alarm

Optional Settings

These settings are extremely helpful and configuring them is recommended, though not mandatory.

At the Partition Level

Configure the following settings under **Settings > Security**.

- ▶ Inactive time out (see [“Inactive Time Out \(Minutes\)”](#) on page 65)
- ▶ Session time out (see [“Session Time Out \(Minutes\)”](#) on page 66)

At the Department Level

Configure the following setting under **Apps > Settings**.

- ▶ Business calendar timezone (see [“Business Calendar Timezone”](#) on page 51)

Configuring Settings

Configuring Partition Settings

Partition settings can be configured via the top and left menus in the console.

To configure Partition settings:

1. In the partition-level Top menu, click the **Settings** option.
2. In the Left menu, select the **System** option if you wish to adjust your system settings. Select the **All Departments** option if you wish to change the settings for all your departments at once.

Configuring Department Settings

Settings for departments can be modified at the global level and applied to all departments in an installation. Department-level settings specific to apps and languages can also be modified for an individual department.

Configuring App Settings for a Department

To configure app settings for a department:

1. In the department-level Top menu, click the **Apps** option.

2. In the Left menu, navigate to one of the following:
 - **Chat > Settings**
 - **Email > Settings**
 - **Common Settings**
3. In the Settings space, modify all the desired settings.
4. Click the **Save** button.

Configuring Language Settings for a Department

To configure language settings for a department:

1. In the department-level Top menu, click the **Language Tools** option.
2. In the Left menu, navigate to **Settings**.
3. In the Language Settings space, modify all the desired settings.
4. Click the **Save** button.

Chat Settings

Chat settings control features such as how chat items are displayed for your agents, and how your agents receive and manage chat items.

For more information about chat settings, see the *Enterprise Chat and Email Administrator's Guide to Chat and Email Resources*.

Email Settings

Email settings control features such as inbox sorting, email alerts for agents, and managing email aliases for actions such as activity transfers.

For more information about email settings, see the *Enterprise Chat and Email Administrator's Guide to Chat and Email Resources*.

Common Partition Settings

To: Address for Notifications from Services

The Distributed Services Manager (DSM) sends out notifications whenever an error occurs during service functions; for example, Retriever, Dispatcher, and so on. Use this setting to specify the email address to which these notifications are sent by the DSM.

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: String
- ▶ Default value: —
- ▶ Minimum value: 0
- ▶ Maximum value: 255
- ▶ Editable at lower level: No

From: Address for Notifications from Services

Use this setting to specify the email address displayed in the “from” field of the service error notifications sent by the Distributed Services Manager (DSM).

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: String
- ▶ Default value: —
- ▶ Minimum value: 0
- ▶ Maximum value: 255
- ▶ Editable at lower level: No

Installation Name

The installation name creates a unique name for your Enterprise Chat and Email installation. Create an installation name by providing a 1 to 4-letter code; for example, PRD, EG, TEST, PROD, TST2, and so on. Names cannot contain spaces or special characters.

If you have more than one ECE deployment, make sure that you use a unique installation name for all your ECE installations. This installation name is then appended to the article IDs.

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: String

- ▶ Default value: —

Web Server URL or Load Balancer URL

This setting is used to manage Single Sign-On (SSO) configurations by defining the correct Web Server URL. If your installation has multiple web servers, provide the Load Balancer URL instead.

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: String
- ▶ Default value: —
- ▶ Maximum length: 100

Maximum Number of Records to Display for Search

Use this setting to specify the maximum number of search results to be displayed in the Results pane of the Search window. This setting also controls the number of results displayed in the Change Customer window that is launched from the Customer section of the information pane of the Agent Console.

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: Integer
- ▶ Default value: 100
- ▶ Minimum value: 10
- ▶ Maximum value: 500

Maximum Number of Records to Display for NAS Search

Use this setting to determine the maximum number of search results to be displayed when an agent uses new activity shortcuts (NAS) to create activities.

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: Integer
- ▶ Default value: 9
- ▶ Minimum value: 1
- ▶ Maximum value: 100

Common Settings for Departments

Number of Activities Per Page

This setting determines the number of activities that are displayed on a page in the Main Inbox of the Agent Console.

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Long
- ▶ Default value: 20
- ▶ Minimum value: 0
- ▶ Maximum value: —
- ▶ Editable at lower level: Yes

Date and Time Format

The format in which date and time is displayed in the application user interface.

- ▶ Type: Department settings group
- ▶ Subtype: Common
- ▶ Data type: Enumeration
- ▶ Default value: 09/22/2019 3:15:30 PM (shows current date and time)
- ▶ Value options:
 - 09/22/2019 3:15 PM
 - Sep/22/2019 3:15 PM
 - September 22 2019 3:15 PM
 - 2019-09-22 3:15 PM
 - 22/09/2019 3:15 PM
 - 22-09-2019 3:15 PM
 - 22 Sep 2019 3:15 PM
 - Sep 22, 2019 3:15 PM
 - 22.09.2019 3:15 PM
 - 09/22/2019 15:15
 - Sep/22/2019 15:15
 - September 22 2019 15:15
 - 2019-09-22 15:15
 - 22/09/2019 15:15
 - 22-09-2019 15:15

- 22 Sep 2019 15:15
- Sep 22, 2019 15:15
- 22.09.2019 15:15
- ▶ Editable at lower level: Yes

Date Format

The format in which dates are displayed in the application user interface.

- ▶ Type: Department settings group
- ▶ Subtype: Common
- ▶ Data type: Enumeration
- ▶ Default value: 09/22/2019 (shows current date)
- ▶ Value options:
 - 09/22/2019
 - Sep/22/2019
 - September 22 2019
 - 2019-09-22
 - 22/09/2019
 - 22-09-2019
 - 22 Sep 2019
 - Sep 22, 2019
 - 22.09.2019

Editable at lower level: Yes

Business Calendar Timezone

Use this setting to select the time zone to be used for business calendars.

- ▶ Type: Department settings group
- ▶ Subtype: General
- ▶ Data type: Enumeration
- ▶ Default value: (GMT-05:00)Eastern Standard Time (US and Canada)
- ▶ Value options:
 - (GMT-12:00) Eniwetok, Kwajalein
 - (GMT-11:00) Midway Island, Samoa
 - (GMT-10:00) Hawaii
 - (GMT-09:00) Alaska-Standard

(GMT-08:00) Alaska-Daylight
(GMT-08:00) Pacific Standard Time (US & Canada)
(GMT-07:00) Pacific Daylight Time (US & Canada)
(GMT-07:00) Arizona
(GMT-07:00) Mountain Standard Time (US & Canada)
(GMT-06:00) Mountain Daylight Time (US & Canada)
(GMT-06:00) Central America
(GMT-06:00) Central Standard Time (US & Canada)
(GMT-05:00) Central Daylight Time (US & Canada)
(GMT-06:00) Mexico City-Standard
(GMT-05:00) Mexico City-Daylight
(GMT-06:00) Saskatchewan
(GMT-05:00) Bogota, Lima, Quito
(GMT-05:00) Eastern Standard Time (US & Canada)
(GMT-04:00) Eastern Daylight Time (US & Canada)
(GMT-05:00) Indiana (East)
(GMT-04:00) Atlantic Standard Time (Canada)
(GMT-03:00) Atlantic Daylight Time (Canada)
(GMT-04:00) Caracas, La Paz
(GMT-04:00) Santiago-Standard
(GMT-03:00) Santiago-Daylight
(GMT-03:30) Newfoundland-Standard
(GMT-02:30) Newfoundland-Daylight
(GMT-03:00) Brasilia-Standard
(GMT-02:00) Brasilia-Daylight
(GMT-03:00) Buenos Aires, Georgetown
(GMT-03:00) Greenland-Standard
(GMT-02:00) Greenland-Daylight
(GMT-02:00) Mid-Atlantic Standard Time
(GMT-01:00) Mid-Atlantic Daylight Time
(GMT-01:00) Azores-Standard
(GMT) Azores-Daylight
(GMT-01:00) Cape Verde Is.
(GMT) Monrovia, Casablanca

(GMT) Greenwich Mean Time; Dublin, Edinburgh, London-Standard
(GMT+01:00) Dublin, Edinburgh, London-Daylight
(GMT+02:00) Dublin, Edinburgh, London-Double Summer
(GMT+01:00) Berlin, Stockholm, Rome, Bern, Vienna, Amsterdam-Standard
(GMT+02:00) Berlin, Stockholm, Rome, Bern, Vienna, Amsterdam- Daylight
(GMT+01:00) Prague, Belgrade, Bratislava, Ljubljana, Budapest-Standard
(GMT+02:00) Prague, Belgrade, Bratislava, Ljubljana, Budapest-Daylight
(GMT+01:00) Paris, Madrid, Brussels, Copenhagen-Standard
(GMT+02:00) Paris, Madrid, Brussels, Copenhagen-Daylight
(GMT+01:00) Lisbon, Warsaw, Sarajevo, Sofija, Skopje, Vilnius, Zagreb-Standard
(GMT+02:00) Lisbon, Warsaw, Sarajevo, Sofija, Skopje, Vilnius, Zagreb-Daylight
(GMT+01:00) West Central Africa
(GMT+02:00) Athens, Istanbul, Minsk-Standard
(GMT+03:00) Athens, Istanbul, Minsk-Daylight
(GMT+02:00) Bucharest-Standard
(GMT+02:00) Bucharest-Daylight
(GMT+02:00) Cairo-Standard
(GMT+03:00) Cairo-Daylight
(GMT+02:00) Harare, Pretoria
(GMT+02:00) Helsinki, Riga, Tallinn-Standard
(GMT+03:00) Helsinki, Riga, Tallinn-Daylight
(GMT+02:00) Israel
(GMT+03:00) Baghdad-Standard
(GMT+04:00) Baghdad-Daylight
(GMT+03:00) Kuwait, Nairobi, Riyadh
(GMT+03:00) Moscow, St. Petersburg-Standard
(GMT+04:00) Moscow, St. Petersburg-Daylight
(GMT+03:30) Tehran-Standard
(GMT+04:30) Tehran-Daylight
(GMT+04:00) Abu Dhabi, Muscat
(GMT+04:00) Baku, Tbilisi, Yerevan-Standard
(GMT+05:00) Baku, Tbilisi, Yerevan-Daylight
(GMT+04:30) Kabul
(GMT+05:00) Ekaterinburg-Standard

(GMT+06:00) Ekaterinburg-Daylight
(GMT+05:00) Islamabad, Karachi, Tashkent
(GMT+05:30) Bombay, Calcutta, Madras, New Delhi, Colombo
(GMT+05:45) Kathmandu
(GMT+06:00) Almaty, Novosibirsk-Standard
(GMT+06:00) Almaty, Novosibirsk-Daylight
(GMT+06:00) Astana, Dhaka, Sri Jayawardenepura
(GMT+06:00) Rangoon
(GMT+07:00) Bangkok, Jakarta, Hanoi
(GMT+07:00) Krasnoyarsk
(GMT+08:00) Beijing, Hong Kong, Chongqing, Urumqi
(GMT+08:00) Irkutsk, Ulaan Bataar
(GMT+08:00) Kuala Lumpur, Perth, Singapore, Taipei
(GMT+09:00) Tokyo, Osaka, Sapporo, Seoul
(GMT+09:00) Yakutsk
(GMT+09:30) Adelaide-Standard
(GMT+10:30) Adelaide-Daylight
(GMT+09:30) Darwin
(GMT+10:00) Brisbane
(GMT+10:00) Canberra, Melbourne, Sydney-Standard
(GMT+11:00) Canberra, Melbourne, Sydney-Daylight
(GMT+10:00) Guam, Port Moresby
(GMT+10:00) Hobart-Standard
(GMT+11:00) Hobart-Daylight
(GMT+10:00) Vladivostok
(GMT+11:00) Magadan, Solomon Is., New Caledonia
(GMT+12:00) Wellington, Auckland-Standard
(GMT+13:00) Wellington, Auckland-Daylight
(GMT+12:00) Fiji, Kamchatka, Marshall Is.
(GMT+13:00) Tonga

▶ Editable at lower level: No

Agent Inbox Preference

Use this setting to choose if the Chat inbox or the Main inbox is displayed when an agent logs in the Agent Console.

- ▶ Type: Department settings group
- ▶ Subtype: General
- ▶ Data type: Enumeration
- ▶ Default value: Chat
- ▶ Value options: Chat, Main
- ▶ Editable at lower level: Yes

Refresh Interval (Seconds)

Use this setting to define the time interval after which the information displayed in the monitors window (in the Supervision Console) is refreshed.

- ▶ Type: Department settings group
- ▶ Subtype: Monitoring
- ▶ Data type: Integer
- ▶ Default value: 30
- ▶ Minimum value: 10
- ▶ Maximum value: 6000
- ▶ Editable at lower level: Yes

Number of Activities to be Monitored for Service Level

Use this setting to define the number of completed activities (emails and tasks) that should be considered for calculating while calculating the service levels for emails and tasks.

- ▶ Type: Department settings group
- ▶ Subtype: Monitoring
- ▶ Data type: Integer
- ▶ Default value: 10
- ▶ Minimum value: 1
- ▶ Maximum value: 1000
- ▶ Editable at lower level: No

Chat - Daily Service Level Timezone

This setting defines the timezone for the daily service level in supervision monitors.

- ▶ Type: Department settings group
- ▶ Subtype: Monitoring
- ▶ Data type: Enumeration
- ▶ Default value: (GMT-05:00) Eastern Standard Time (US and Canada)
- ▶ Value options:
 - (GMT-12:00) Eniwetok, Kwajalein
 - (GMT-11:00) Midway Island, Samoa
 - (GMT-10:00) Hawaii
 - (GMT-09:00) Alaska-Standard
 - (GMT-08:00) Alaska-Daylight
 - (GMT-08:00) Pacific Standard Time (US & Canada)
 - (GMT-07:00) Pacific Daylight Time (US & Canada)
 - (GMT-07:00) Arizona
 - (GMT-07:00) Mountain Standard Time (US & Canada)
 - (GMT-06:00) Mountain Daylight Time (US & Canada)
 - (GMT-06:00) Central America
 - (GMT-06:00) Central Standard Time (US & Canada)
 - (GMT-05:00) Central Daylight Time (US & Canada)
 - (GMT-06:00) Mexico City-Standard
 - (GMT-05:00) Mexico City-Daylight
 - (GMT-06:00) Saskatchewan
 - (GMT-05:00) Bogota, Lima, Quito
 - (GMT-05:00) Eastern Standard Time (US & Canada)
 - (GMT-04:00) Eastern Daylight Time (US & Canada)
 - (GMT-05:00) Indiana (East)
 - (GMT-04:00) Atlantic Standard Time (Canada)
 - (GMT-03:00) Atlantic Daylight Time (Canada)
 - (GMT-04:00) Caracas, La Paz
 - (GMT-04:00) Santiago-Standard
 - (GMT-03:00) Santiago-Daylight
 - (GMT-03:30) Newfoundland-Standard
 - (GMT-02:30) Newfoundland-Daylight
 - (GMT-03:00) Brasilia-Standard
 - (GMT-02:00) Brasilia-Daylight

(GMT-03:00) Buenos Aires, Georgetown
(GMT-03:00) Greenland-Standard
(GMT-02:00) Greenland-Daylight
(GMT-02:00) Mid-Atlantic Standard Time
(GMT-01:00) Mid-Atlantic Daylight Time
(GMT-01:00) Azores-Standard
(GMT) Azores-Daylight
(GMT-01:00) Cape Verde Is.
(GMT) Monrovia, Casablanca
(GMT) Greenwich Mean Time; Dublin, Edinburgh, London-Standard
(GMT+01:00) Dublin, Edinburgh, London-Daylight
(GMT+02:00) Dublin, Edinburgh, London-Double Summer
(GMT+01:00) Berlin, Stockholm, Rome, Bern, Vienna, Amsterdam-Standard
(GMT+02:00) Berlin, Stockholm, Rome, Bern, Vienna, Amsterdam- Daylight
(GMT+01:00) Prague, Belgrade, Bratislava, Ljubljana, Budapest-Standard
(GMT+02:00) Prague, Belgrade, Bratislava, Ljubljana, Budapest-Daylight
(GMT+01:00) Paris, Madrid, Brussels, Copenhagen-Standard
(GMT+02:00) Paris, Madrid, Brussels, Copenhagen-Daylight
(GMT+01:00) Lisbon, Warsaw, Sarajevo, Sofija, Skopje, Vilnius, Zagreb-Standard
(GMT+02:00) Lisbon, Warsaw, Sarajevo, Sofija, Skopje, Vilnius, Zagreb-Daylight
(GMT+01:00) West Central Africa
(GMT+02:00) Athens, Istanbul, Minsk-Standard
(GMT+03:00) Athens, Istanbul, Minsk-Daylight
(GMT+02:00) Bucharest-Standard
(GMT+02:00) Bucharest-Daylight
(GMT+02:00) Cairo-Standard
(GMT+03:00) Cairo-Daylight
(GMT+02:00) Harare, Pretoria
(GMT+02:00) Helsinki, Riga, Tallinn-Standard
(GMT+03:00) Helsinki, Riga, Tallinn-Daylight
(GMT+02:00) Israel
(GMT+03:00) Baghdad-Standard
(GMT+04:00) Baghdad-Daylight
(GMT+03:00) Kuwait, Nairobi, Riyadh

(GMT+03:00) Moscow, St. Petersburg-Standard
(GMT+04:00) Moscow, St. Petersburg-Daylight
(GMT+03:30) Tehran-Standard
(GMT+04:30) Tehran-Daylight
(GMT+04:00) Abu Dhabi, Muscat
(GMT+04:00) Baku, Tbilisi, Yerevan-Standard
(GMT+05:00) Baku, Tbilisi, Yerevan-Daylight
(GMT+04:30) Kabul
(GMT+05:00) Ekaterinburg-Standard
(GMT+06:00) Ekaterinburg-Daylight
(GMT+05:00) Islamabad, Karachi, Tashkent
(GMT+05:30) Bombay, Calcutta, Madras, New Delhi, Colombo
(GMT+05:45) Kathmandu
(GMT+06:00) Almaty, Novosibirsk-Standard
(GMT+06:00) Almaty, Novosibirsk-Daylight
(GMT+06:00) Astana, Dhaka, Sri Jayawardenepura
(GMT+06:00) Rangoon
(GMT+07:00) Bangkok, Jakarta, Hanoi
(GMT+07:00) Krasnoyarsk
(GMT+08:00) Beijing, Hong Kong, Chongqing, Urumqi
(GMT+08:00) Irkutsk, Ulaan Bataar
(GMT+08:00) Kuala Lumpur, Perth, Singapore, Taipei
(GMT+09:00) Tokyo, Osaka, Sapporo, Seoul
(GMT+09:00) Yakutsk
(GMT+09:30) Adelaide-Standard
(GMT+10:30) Adelaide-Daylight
(GMT+09:30) Darwin
(GMT+10:00) Brisbane
(GMT+10:00) Canberra, Melbourne, Sydney-Standard
(GMT+11:00) Canberra, Melbourne, Sydney-Daylight
(GMT+10:00) Guam, Port Moresby
(GMT+10:00) Hobart-Standard
(GMT+11:00) Hobart-Daylight
(GMT+10:00) Vladivostok

(GMT+11:00) Magadan, Solomon Is., New Caledonia

(GMT+12:00) Wellington, Auckland-Standard

(GMT+13:00) Wellington, Auckland-Daylight

(GMT+12:00) Fiji, Kamchatka, Marshall Is.

(GMT+13:00) Tonga

- ▶ Can be reset at lower level: No

Service Email and Chat Activities at the Same Time

Use this setting to determine if agents can continue to work on email activities, which are already assigned to them, while they are in a chat session with a customer.

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options:
 - **Yes:** Agents can continue to respond to email activities that are already assigned to them. The Send and Send and Complete buttons are enabled for emails. However, no new emails get assigned to agents while they are in a chat session. If agents are associated with an outbound MRD, they can create outbound emails while they are in a chat session.
 - **No:** Agents cannot respond to email activities that are already assigned to them. The Send and Send and Complete buttons are disabled for emails. Also, no new emails get assigned to agents while they are in a chat session. Agents cannot create outbound emails while they are in a chat session.
- ▶ Editable at lower level: No

Service Email and Phone Activities at the Same Time

Use this setting to determine if agents can continue to work on email activities, which are already assigned to them, while they are on the phone.

- ▶ Type: Department settings group
- ▶ Subtype: CTI settings
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options:
 - **Yes:** Agents can continue to respond to email activities that are already assigned to them. The Send and Send and Complete buttons are enabled for emails. However, no new emails get assigned to agents while they are on a phone call. If agents are associated with an outbound MRD, they can create outbound emails during a phone call.

- **No:** Agents cannot respond to email activities that are already assigned to them. The Send and Send and Complete buttons are disabled for emails. Also, no new emails get assigned to agents while they are on a phone call. Agents cannot create outbound emails while they are on a phone call.
- ▶ Editable at lower level: No

Service Chat and Phone Activities at the Same Time

Use this setting to determine if agents can continue to work on chat activities, which are already assigned to them, while they are on the phone.

- ▶ Type: Department settings group
- ▶ Subtype: CTI settings
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options:
 - **Yes:** Agents can continue to respond to chat activities that are already assigned to them. The Complete button is enabled for chats. However, no new chats get assigned to agents while they are on a phone call.
 - **No:** Agents cannot respond to chat activities that are already assigned to them. The Complete button is disabled for chats. Also, no new chats get assigned to agents while they are on a phone call.
- ▶ Editable at lower level: No

Integration Settings

Proactive Monitoring Refresh Interval (Seconds)

This setting controls the interval at which the application verifies if EAAS and Listener services are running.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE Integration
- ▶ Data type: Integer
- ▶ Default value: 300
- ▶ Minimum value: 300
- ▶ Maximum value: 6000

Allow Transfer of Activities to Integrated Queues in Other Departments

Use this setting to allow users to transfer activities to mapped queues (that belong to the same Media Class) in other departments.

- ▶ Type: Partition settings group

- ▶ Subtype: Unified CCE integration
- ▶ Data type: Enumeration
- ▶ Default value: Yes
- ▶ Value options: Yes, No

Reason Code for Agent Not Ready

This is the reason code that is sent to Unified CCE when agents mark themselves unavailable. You only need to change this setting if the default reason Code 2 is currently used to track a different agent status.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE Integration
- ▶ Data type: Integer
- ▶ Default value: 2
- ▶ Minimum value: 0
- ▶ Maximum value: 32767

Maximum Wait Time for Login Response From UCCE (Seconds)

This setting refers to the maximum wait time allowed while waiting for a login response from Unified CCE. If the integrated agent is not logged in during the defined time period, a message is displayed to the agent and a timeout occurs. Timeout generally occurs because of network related issues or configuration issues.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE Integration
- ▶ Data type: Integer
- ▶ Default value: 20
- ▶ Minimum value: 20
- ▶ Maximum value: 120

Enable Chat Queueing

This allows customers to initiate new chats even when all agents are working at their maximum capacity. The chat request are then queued in Unified CCE to wait for the next available agents. The maximum time for which a chat is queued is defined by the Chat Watchdog Interval setting.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE integration
- ▶ Data type: Enumeration
- ▶ Default value: Yes

- ▶ Value options: Yes, No

Chat Watchdog Interval (seconds)

This setting controls the time interval after which the chat activity is tagged as abandoned if it could not be assigned to an agent.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE Integration
- ▶ Data type: Integer
- ▶ Default value: 70
- ▶ Minimum value: 70
- ▶ Maximum value: 12600 (3.5 hours)

Allow Transferring Email Activities to Agents Who Are Not Available

Use this setting to allow email activities to be transferred to agents who are logged in, but not marked available. If you wish to enable this setting, the Enable Autopushback setting must first be disabled, as these two settings cannot be enabled simultaneously.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE integration
- ▶ Data type: Enumeration
- ▶ Default value: Yes
- ▶ Value options: Yes, No

Allow Transferring Chats to Agents Who Are Not Available

Use this setting to allow chat activities to be transferred to agents who are logged in, but not marked available.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE integration
- ▶ Data type: Enumeration
- ▶ Default value: Yes
- ▶ Value options: Yes, No

Allow Transferring Emails to Agents Who Are Not Logged in

Use this setting to allow email activities to be transferred to agents who are not logged in. If you are wish to enable this setting, the Enable Autopushback setting must first be disabled. The two settings cannot be enabled simultaneously. For more about the Enable Autopushback setting, see Activity Assignment Settings.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE integration
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No

Allow Supervisor to Join an Ongoing Chat Session

Use this setting to allow integrated supervisors to join an ongoing chat to participate in the conversation between an integrated agent and a customer. Note that when the supervisor joins chat, messages are not logged in UCCE and the reports will not include this data.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE integration
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No

Agent Availability Settings After Completion of Call

This setting allows you to determine whether agents are automatically marked as available at the end of a call, or if the agent needs to make themselves available.

Mark Agent Ready After Completion of Call

Use this setting to adjust the default agent availability status upon completion of a call activity by clicking the toggle switch. If the value is set to **True**, the agent is automatically marked ready to receive new calls. If the value is set to **False**, agents have to make themselves available after completing each call.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE integration
- ▶ Data type: Enumeration
- ▶ Default value: True
- ▶ Value options: True, False

Event Reason Code to Track Agent State

Define the event reason code that is sent to Unified CCE to track the agent status. You need to change this setting only if the default reason code 32767 is currently used to track some other status in Finesse.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE integration

- ▶ Data type: Integer
- ▶ Default value: 32767
- ▶ Value options: -

Starvation Time for Activities

Starvation time refers to the maximum time for which the system waits to send a routing request for an activity. After the set time limit is met, the request for the waiting activity is prioritized and sent first before moving on to other call activities. Priority sequence for activities is - delayed callback, chat, and email.

For example, if the system is overloaded with multiple callback activities, and is unable to process a chat activity, then once the chat activity's starvation time period has passed, it will process this chat activity first before processing the next call activity. For more information about chat and email activities, see the *Enterprise Chat and Email Administrator's Guide to Chat and Email Resources*.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE integration
- ▶ Data type: String
- ▶ Default values:
 - Callback: 10 seconds
 - Chat: 60 seconds
 - Email: 12 hours
- ▶ Value options:
 - Callback: 10 - 120 seconds
 - Chat: 60 - 180 seconds
 - Email: 1 - 168 hours

Concurrent Task Limit Mappings by Media

This setting determines the maximum number of activities that can be assigned to an agent beyond the concurrent task limit (CTL) of the Media Routing Domain. There are three classes: the Chat media class, the Email media class, and the Outbound media class.

Note that changes made to this setting can affect how activities are transferred to agents.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE Integration
- ▶ Data type: Integer
- ▶ Default value: 1
- ▶ Minimum value: 0
- ▶ Maximum value: 2

Media Class Names

This setting refers to the names of the media classes configured in Unified CCE. If the media class names have been changed in Unified CCE from their default names, they must also be changed here to match. Note that media class names are case sensitive. For more information about chat and email, see the *Enterprise Chat and Email Administrator's Guide to Chat and Email Resources*.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE integration
- ▶ Data type: String
- ▶ Default values:
 - Voice media class: Cisco_Voice
 - Chat media class: ECE_Chat
 - Email media class: ECE_Email
 - Outbound media class: ECE_Outbound

Partition Security Settings

Allow Users to Change Password

Use this setting to determine if users should be allowed to change their password via the Password tab in the Options window available in the user consoles.

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: Enumeration
- ▶ Default value: Yes
- ▶ Value options: Yes, No
- ▶ Editable at lower level: No

Inactive Time Out (Minutes)

This setting defines the period of time after which a user session is made inactive if there is no activity from the user in the application. Users can reactivate the session by providing their password, the session then resumes from the point where it was left.

- ▶ Type: Partition settings group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 30

- ▶ Minimum: 5
- ▶ Maximum: 1440

Session Time Out (Minutes)

This setting defines the period of time for which a user session is stored in the server memory once the user session has become inactive. Once this time has elapsed, the system deletes the session from the memory. User sessions cannot be recovered once deleted, though users can create a new session by logging in with their user name and password.

- ▶ Type: Partition settings group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 60
- ▶ Minimum: 5

Maximum: 1440

Allow Local Login for Partition Administrators

This setting defines whether or not a partition administrator can log into the system locally once Single Sign-On has been enabled.

- ▶ Type: Partition settings group
- ▶ Subtype: Security
- ▶ Data type: Enumeration
- ▶ Default value: Yes
- ▶ Value options: Yes, No
- ▶ Can be reset at lower level: No

Customer Departmentalization

Customer departmentalization allows for the sharing of customer history and information across departments. If you do NOT want to share this information across departments, change the value in the dropdown to **Yes**. The default setting is **No** meaning that departments automatically share customer information and history with each other.

Note that this setting can only be changed while there is one department in the partition. Once a second department is created, this setting can no longer be configured.

- ▶ Type: Partition settings group
- ▶ Subtype: Security
- ▶ Data type: Enumeration

- ▶ Default value: No
- ▶ Value options: No, Yes

Password Complexity Policy

The Password Complexity Policy defines the password policy that is enforced for all user passwords in the system. The value of this setting is defined as a Regular Expression, containing the characters that are compliant with the password policy. This value is pre-generated and can be modified accordingly, or even deleted if you do not wish to enforce a password policy.

The Failure Message is the message that is shown to users when their password do not comply with the password policy, prompting them to provide a new, acceptable password. This message can be changed according to your preferences. You can also test a password by inputting it into the **Enter a sample password** field and clicking the **Test** button.

- ▶ Type: Partition settings group
- ▶ Subtype: Security
- ▶ Data type: String
- ▶ Default value: `((?=.*[0-9])(?=.*[a-z])[A-Z]).{8,20}`
- ▶ Default failure message: “The password does not comply with the password policy. Password should be at least of 8 characters having a mix of numbers and alphabets.”
- ▶ Minimum value: 0
- ▶ Maximum value: 1000
- ▶ Can be reset at lower level: No

Security Settings for Cookies

Enabling this setting by clicking the toggle switch secures all the cookies created by the application for the various user consoles (for example, Agent Console, Administrator Dashboard, and so on). When this setting is enabled, you must configure Secure Sockets Layer (SSL) for accessing the ECE application. For details, see the *Enterprise Chat and Email Installation Guide*.

If SSL is not configured, users will not be able to access the application. This setting can only be enabled while accessing the application using the HTTPS protocol.



Important: Changes to this setting take effect when the application is restarted.

- ▶ Type: Partition settings group
- ▶ Subtype: Security
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No

Secure the Cookies Created by Application for Customer Websites

Enabling this setting by clicking the toggle switch secures all the cookies created by the application for the customer websites.



Important: This setting must be enabled only if the customer website is secure (HTTPS).

- ▶ Type: Partition settings group
- ▶ Subtype: Security
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No

Departments Security Settings

Unsuccessful Attempts Time Frame

Use this setting to decide the time frame within which, if a user makes the defined number of unsuccessful log in attempts, his account is disabled. The maximum number of allowed unsuccessful attempts are defined in the “Maximum number of unsuccessful timed attempts” setting.

- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 0
- ▶ Minimum value: 0
- ▶ Maximum value: —
- ▶ Editable at lower level: No

Unsuccessful Attempts Time Unit

Use this setting to choose the unit of time to define the time frame in the “Unsuccessful attempts time frame” setting.

- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Enumeration
- ▶ Default value: Second
- ▶ Value options: Second, Minute, Hour, Day, Month, Year

- ▶ Editable at lower level: No

Maximum Inactivity Time Unit

Use this setting to define the unit to be used to calculate the time after which a user account is disabled, if it has not been accessed in the specified time. The actual value of time is defined in the “Maximum inactivity time frame” setting.

- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Enumeration
- ▶ Default value: Second
- ▶ Value options: Second, Minute, Hour, Day, Month, Year
- ▶ Editable at lower level: No

Maximum Inactivity Time Frame

Use this setting to decide the time after which an account is disabled, if it has not been accessed in the specified time. Use the “Maximum inactivity time unit” setting to define the time unit in seconds, minutes, hours, months, or years, for the value of this setting.

- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 0
- ▶ Minimum value: 0
- ▶ Maximum value: —
- ▶ Editable at lower level: No

Maximum Number of Unsuccessful Attempts

Use this setting to define the maximum number of unsuccessful attempts a user can make before the user account is disabled. If the value of this setting is zero, then no check is done to see the number of times the user has made unsuccessful log in attempts.

- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 0
- ▶ Minimum value: —
- ▶ Maximum value: —

- ▶ Editable at lower level: No

Maximum Number of Unsuccessful Timed Attempts

Use this setting to decide the number of login attempts a user is allowed in the defined time duration before his account is disabled. The time frame is defined in the “Unsuccessful attempts time frame” setting.

- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 0
- ▶ Minimum value: —
- ▶ Maximum value: 10
- ▶ Editable at lower level: No

Logger Settings



Important: You need to restart the application after changing the logger settings.

Maximum Backups of Log Files

This setting determines the maximum number of backup copies you want to save for the log files. After the number of back-up copies of a log file reach the specified number, the system starts deleting the oldest versions from the logs folder. You should set the value more than 50.

- ▶ Type: System Partition settings group
- ▶ Subtype: Logger
- ▶ Data type: Integer
- ▶ Default value: 100
- ▶ Minimum value: —
- ▶ Maximum value: —

Default Size in MB

Use this setting to determine the maximum size of the log files created by the application.

- ▶ Type: System Partition settings group
- ▶ Subtype: Logger

- ▶ Data type: Integer
- ▶ Default value: 5
- ▶ Minimum value: —
- ▶ Maximum value: —

Default Log Level

This setting determines the default log level of the new processes that are created in the system. This setting does not apply to the processes that have been started at least once.

- ▶ Type: System Partition settings group
- ▶ Subtype: Logger
- ▶ Data type: Enumeration
- ▶ Default value: Error
- ▶ Possible values: Fatal, Error, Warn, Info, Perf, Dbquery

Encrypt Log Files

Use this setting to encrypt the log files. By default, logs are not encrypted by the application. To decrypt the logs, a utility—`logs_decryption_utility`—is available in the Utilities folder on the services server.

- ▶ Type: System Partition settings group
- ▶ Subtype: Logger
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No

Login Name Minimum Length

Use this setting to define the minimum number of characters that a user name must have. This user name is used to log in to the application.

- ▶ Type: Department settings group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 2
- ▶ Minimum value: 2
- ▶ Maximum value: —
- ▶ Can be reset at lower level: No

Login Password Case Sensitive

Use this setting to decide if you want the user passwords to be case sensitive. When this setting is enabled, at the time of login a check is made to see if the case of the password matches exactly the password set for the user.

- ▶ Type: Department settings group
- ▶ Subtype: Security
- ▶ Data type: Enumeration
- ▶ Default value: Yes
- ▶ Value options: Yes, No
- ▶ Can be reset at lower level: No

Password Life Time

Use this setting to determine the expiry time for user passwords. The expiry time is calculated from the time the password was created for the first time or from the time the password was last changed. Use the “Password lifetime unit” setting to define the time unit in seconds, minutes, hours, months, or years, for the value of this setting.

- ▶ Type: Department settings group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 0
- ▶ Minimum value: 0
- ▶ Maximum value: —
- ▶ Can be reset at lower level: No

Password Life Time Unit

Use this setting to define the unit to be used to calculate the time after which the password expires. The actual value of time is defined in the “Password lifetime” setting.

- ▶ Type: Department settings group
- ▶ Subtype: Security
- ▶ Data type: Enumeration
- ▶ Default value: Second
- ▶ Value options: Second, Minute, Hour, Day, Month, Year
- ▶ Can be reset at lower level: No

Allow Users to Change Password

Use this setting to determine if users should be allowed to change their password from the Password tab in the Options window available in the user consoles.

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: Enumeration
- ▶ Default value: Yes
- ▶ Value options: Yes, No
- ▶ Can be reset at lower level: No

Unsuccessful Attempts Time Frame

Use this setting to decide the time frame within which, if a user makes the defined number of unsuccessful log in attempts, his account is disabled. The maximum number of allowed unsuccessful attempts are defined in the “Maximum number of unsuccessful timed attempts” setting.

- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 0
- ▶ Minimum value: 0
- ▶ Maximum value: —
- ▶ Can be reset at lower level: No

Unsuccessful Attempts Time Unit

Use this setting to choose the unit of time to define the time frame in the “Unsuccessful attempts time frame” setting.

- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Enumeration
- ▶ Default value: Second
- ▶ Value options: Second, Minute, Hour, Day, Month, Year
- ▶ Can be reset at lower level: No

Maximum Number of Unsuccessful Timed Attempts

Use this setting to decide the number of login attempts a user is allowed in the defined time duration before his account is disabled. The time frame is defined in the “Unsuccessful attempts time frame” setting.

- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 0
- ▶ Minimum value: —
- ▶ Maximum value: 10
- ▶ Can be reset at lower level: No

Maximum Number of Unsuccessful Attempts

Use this setting to define the maximum number of unsuccessful attempts a user can make before the user account is disabled. If the value of this setting is zero, then no check is done to see the number of times the user has made unsuccessful log in attempts.

- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 0
- ▶ Minimum value: —
- ▶ Maximum value: —
- ▶ Can be reset at lower level: No

Maximum Inactivity Time Frame

Use this setting to decide the time after which a account is disabled, if it has not been accessed in the specified time. Use the “Maximum inactivity time unit” setting to define the time unit in seconds, minutes, hours, months, or years, for the value of this setting.

- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 0
- ▶ Minimum value: 0
- ▶ Maximum value: —
- ▶ Can be reset at lower level: No

Maximum Inactivity Time Unit

Use this setting to define the unit to be used to calculate the time after which a user account is disabled, if it has not been accessed in the specified time. The actual value of time is defined in the “Maximum inactivity time frame” setting.


- ▶ Type: Department setting group
- ▶ Subtype: Security
- ▶ Data type: Enumeration
- ▶ Default value: Second
- ▶ Value options: Second, Minute, Hour, Day, Month, Year
- ▶ Can be reset at lower level: No

Language Settings

Many of these language settings can be managed at the Partition and Department level. These control features such as the auto spellcheck function and treatment of special characters, as well as the default language for the Knowledge Base (KB).

Note that the All Departments Language Settings are not the same as the actions and functions managed through the Language Tools option in the top menu. For more information about Language Tools and the options it contains, see [“Language Options” on page 152](#).

KB Primary Language

Designates the primary language for the Knowledge Base (KB). This setting does not appear in the Language Tools section and must be set here. To add additional languages from the language pack, click the **Search and Add**  button, then select the desired language from the popup window that appears.

- ▶ Type: Department settings group
- ▶ Subtype: Knowledge base
- ▶ Data type: Enumeration
- ▶ Default value: —
- ▶ Value options: English (US), English (UK), Arabic, Chinese (Simplified), Chinese (Traditional), Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Norwegian (Bokmal), Norwegian (Nynorsk), Portuguese, Portuguese (Brazilian), Romanian, Spanish, Swedish, Turkish
- ▶ Can be reset at lower level: Yes

Custom Language Label

This setting allows you to add a custom language to the list of languages available in the KB primary language setting.

- ▶ Type: Department settings group
- ▶ Subtype: Knowledge Base
- ▶ Data type: String
- ▶ Default value: Custom
- ▶ Minimum: 0
- ▶ Maximum: 225
- ▶ Can be reset at lower level: No

Ignore Words with Only Upper Case Letters

With this setting you can decide if the spell checker should ignore misspelled words in upper case. For example, HSBC, TESTNG, and so on.

- ▶ Type: Department settings group
- ▶ Subtype: Spell checker
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No
- ▶ Can be reset at lower level: Yes

Ignore Words with a Mixture of Upper and Lower Case Letters

With this setting you can decide if the spell checker should ignore words with unusual mixture of upper and lower case letters. For example, myFirstWord.

- ▶ Type: Department settings group
- ▶ Subtype: Spell checker
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No
- ▶ Can be reset at lower level: Yes

Ignore Words with Only Numbers or Special Characters

With this setting you can decide if the spell checker should ignore words with digits in them. For example, 1234.

- ▶ Type: Department settings group

- ▶ Subtype: Spell checker
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No
- ▶ Can be reset at lower level: Yes

Ignore Words that Contain Numbers

With this setting you can decide if the spell checker should ignore words that have a mix of letters and digits. For example, name123, 123test!, and so on.

- ▶ Type: Department settings group
- ▶ Subtype: Spell checker
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No
- ▶ Can be reset at lower level: Yes

Ignore Web Addresses and File Names

With this setting you can decide if the spell checker should ignore internet addresses and file names. For example, www.company.com, alias@companyname.com, text.pdf, and so on.

- ▶ Type: Department settings group
- ▶ Subtype: Spell checker
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No
- ▶ Can be reset at lower level: Yes

Auto Spellcheck

Use this setting to enable automatic spell check for emails, tasks, and so on. This setting is not used for chat activities. For chat, use the [Chat - Auto Spellcheck](#) setting.

- ▶ Type: Department settings group
- ▶ Subtype: Spell checker
- ▶ Data type: Enumeration
- ▶ Default value: Enable
- ▶ Value options: Disable, Enable

- ▶ Can be reset at lower level: Yes

Preferred Dictionary of the User

With this setting you can choose the dictionary that the spell checker should use.

- ▶ Type: Department settings group
- ▶ Subtype: Spell checker
- ▶ Data type: String
- ▶ Default value: —
- ▶ Value options: Danish Dictionary, Swedish Dictionary, Finnish Dictionary, Norwegian (Bokmaal) Dictionary, Italian Dictionary, Dutch Dictionary, Portuguese Dictionary, French Dictionary, Spanish Dictionary, German Dictionary, English (UK) Dictionary, English (US) Dictionary
- ▶ Can be reset at lower level: Yes

Auto Blockcheck

Use this setting to check the content of emails, tasks, etc for blocked words. This setting is not used for chat activities. For chat, use the [Chat - Auto Blockcheck](#) setting. The list of blocked words is set from the Dictionaries node in the Administrator Dashboard. For details, see [“Viewing and Adding Blocked Words” on page 157](#).

- ▶ Type: Department settings group
- ▶ Subtype: Spell checker
- ▶ Data type: Enumeration
- ▶ Default value: Enable
- ▶ Value options: Enable, Disable
- ▶ Can be reset at lower level: No

Split Contracted Words

The spelling checker considers correct contracted words as misspelled while using the French and Italian dictionaries. Configure the value of this setting to **Yes** to ensure that contracted words in these languages are not misidentified by the spelling checker. This setting affects only French and Italian.

- ▶ Type: Department settings group
- ▶ Subtype: Spell checker
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No
- ▶ Can be reset at lower level: Yes

Include Original Message Text During Spell Check

Use this setting to decide if the content of the original email message should be checked when the spelling checker is run.

- ▶ Type: Department settings group
- ▶ Subtype: Spell checker
- ▶ Data type: Enumeration
- ▶ Default value: No
- ▶ Value options: Yes, No
- ▶ Can be reset at lower level: Yes

Chat - Auto Blockcheck

Use this setting to check the chat messages for blocked words. The list of blocked words is set from the Dictionaries node in the Administrator Dashboard. For details, see [“Viewing and Adding Blocked Words” on page 157](#).

- ▶ Type: Department settings group
- ▶ Subtype: Spell checker
- ▶ Data type: Enumeration
- ▶ Default value: Enable
- ▶ Value options: Enable, Disable
- ▶ Can be reset at lower level: Yes

Chat - Auto Spellcheck

Use this setting to enable automatic spell check for chats. This setting is not used for emails, tasks, and so on.

- ▶ Type: Department settings group
- ▶ Subtype: Spell checker
- ▶ Data type: Enumeration
- ▶ Default value: Disable
- ▶ Value options: Disable, Enable
- ▶ Can be reset at lower level: Yes

5 Users

- ▶ [About Users, Groups, Roles, and Actions](#)
- ▶ [What are the Actions Assigned to the Default Roles?](#)
- ▶ [Managing User Roles](#)
- ▶ [Managing User Groups](#)
- ▶ [Managing Users](#)

About Users, Groups, Roles, and Actions

Users

A user is an individual—an administrator, manager, or agent—who has a distinct identification which she uses to log in to the application to perform specific functions. Users are assigned roles and permissions, which enable them to perform various tasks. To make it easier to administer a large number of users, users can be organized into named groups.

A specific type of administrator is created during the installation. The first business user, created during installation, is a user called **Partition Administrator**. This user manages global users and settings and can create department-level users to manage department resources.

Department-level users consist of agents and supervisors. Agents handle direct customer interactions, such as chat, email, phone calls, and so on and report to supervisors who can monitor and review those interactions.

Note that department users cannot be directly created in ECE and must be imported from their associated Media Routing Domain (MRD). For more information, see [“Importing Media Routing Domains \(MRDs\)” on page 26](#).

If an ECE user’s attributes are modified in Unified CCE, when the ECE user is selected in the Administrator Dashboard, the modifications are automatically retrieved and synchronized in ECE.

User Groups

User groups are a collection of users that share similar functions or roles in the system. Groups make it much easier to manage user accounts. User groups cannot be created manually in ECE, they can only be created by importing MRDs and users.

A standard user group called All Users in *Department_Name* is created in each department. Every new user in the department is automatically included in this group. You should not use this user group to manage activity routing through workflows and pull and transfer permissions on other users, user groups, and queues.

Each user group is mapped to a Unified CCE skill group. Activities to users in this group are assigned from Unified CCE queues only. For more details on these queues, see *Enterprise Chat and EMail Administrator’s Guide to Routing and Workflows*. For user groups that map to a skill group, the agent list for the skill group is administered and managed in Unified CCE. You cannot add users to this group from ECE.

User Roles

A role is a set of permissible actions for various business resources. An agent’s role, for instance, would include actions such as “View Agent Console” and “Add notes.” The system comes with some default user roles and templates for roles. You can assign one or more roles to a group of users or an individual user.

The default user roles are:

- ▶ **Administrator:** The administrator is the manager of system and has access to the Administrator Dashboard. The administrator is automatically created while installing the application. Additional administrators in ECE can be created when an administrator from Unified CCE logs in to the ECE Administrator Dashboard.

- ▶ **Agent:** An agent is a person who handles customer queries, who is directly in contact with the customer. The agent has access to the Agent Console. Agents are imported into the system by the administrator from Unified CCE.
- ▶ **Agent (Read Only):** An agent (read only) has access to the Agent Console, but is not able to compose replies for the customer queries. A read-only agent can only view them. This role can be assigned to trainees.
- ▶ **Supervisor:** A supervisor has access to the Supervision Console, and creates monitors for queues, user groups, and users in a department. They can also create and run reports from the Reports Console.
- ▶ **Supervisor (Read Only):** A user with the supervisor (read only) role can create and run monitors. Such a user cannot create reports, but can run the reports for which the user has view and run permissions.

The screenshot shows the 'User Management' section of the 'Chat and Email' application. A sidebar on the left contains 'Users', 'User Groups', and 'Roles' (which is selected). The main area displays a table of roles with columns for Name, Description, and Actions. A 'New' button is visible in the top right corner of the table area.

Name	Description	Actions
Supervisor	Role for supervisors	...
Agent	Role for agents	...
Agent (Read Only)	Role for agents with read-only functions	...
Supervisor (Read Only)	Role for supervisors with read-only functions	...
Administrator	Role for administrators	...
Copy of Administrator	Role for administrators 21212	...

Selecting user roles

Actions

When selecting a role for a users, you must consider the work that the person with that role can handle. Actions define this work. All default user roles have already been assigned certain actions. You can view these actions by clicking on any role and you can use these actions to create new roles. For more information about actions that are assigned to roles, see [“What are the Actions Assigned to the Default Roles?”](#) on page 86.

Permissions

Permissions allow you to give users access to particular business objects, such as KB folders, queues, and so on. To be able to give a permission, the user must first be assigned the appropriate action associated with the object. For example, for KB folders if you want to give the “View Folder” permission to a user, you have to make sure that the user is first assigned the “View Folder” action.



Important: Partition administrators that are created in ECE when an administrator accesses the application through the Cisco administrator’s console, cannot change permissions of users in the ECE application. These users must use an ECE administrator account that was created during the installation or imported. For more information, see *Enterprise Chat and Email Administrator’s Guide to Administration Console*.

Important Things to Note About Picking and Pulling Activities

Emails

- ▶ Agents can pick emails from other agents that belong to the same set of skill groups.
- ▶ Only agents who are part of a skill group that is associated with the queue can pick or pull from that queue.
- ▶ Only agents who match the attributes of a Precision Queue (PQ) that is associated with the ECE queue can pick or pull from that queue.
- ▶ Based on the **Maximum Assignment Beyond Concurrent Task Limit** setting, agents who have reached their concurrent task limit can pick additional activities. The maximum number of activities is defined as part of the setting.



Important: If the application is integrated with a version prior to Packaged CCE 12.0(1), agents cannot pick activities beyond the concurrent task limit.

- ▶ When working on a non-interruptible chat or voice call:
 - Agents can pick or pull interruptible emails from queues and other agents.
 - Agents cannot pick or pull non-interruptible emails from queues or other agents.



Important: If the application is integrated with a version prior to Packaged CCE 12.0(1), agents cannot pick activities while working on non-interruptible chats or voice calls.

- ▶ Agents with the Administrator Role can pick from the Default exception queue.



Important: Emails with exception keywords that are routed to the Default exception queue should not be transferred to other queues. These emails cannot be picked or pulled upon being transferred to other queues.

Chats

- ▶ Agents are assigned chats by the system automatically. They cannot pull chat activities from queues. Pick does not apply to chats.

Important Things to Note About Transferring Emails

- ▶ Multiple emails can be selected and transferred to another user or queue at the same time, so long as the emails are new and have no draft responses. If an email has any draft responses, or is not a new incoming email, it must be transferred individually.
- ▶ Outbound emails created by agents can only be transferred to users and not to queues.



Important: For installations that have upgraded from a version prior to 12.0(1), a routing script must be applied to the Pick/Pull node for the outbound MRD in order for agents to pick, pull, or transfer outbound emails. For more information about the script, see the *Scripting and Media Routing Guide for Cisco Unified CCE*.

- ▶ Disabled users are not listed in the list of users to whom you can transfer activities.

- ▶ You can transfer activities only if you have the Transfer action. For more information about actions, see [“Actions” on page 82](#).

Transferring to Queues:

- ▶ An email can be transferred to any queue that belong to the same media class. From there, the activity is routed based on the queue-to-script mapping.

Transferring to Agents:

- ▶ Agents can transfer emails to other agents that belong to the same set of skill groups.
- ▶ Based on the **Maximum Task Limit** setting, agents can transfer additional activities to agents who have reached their concurrent task limit. The maximum number of activities is defined as part of the setting.
- ▶ Emails cannot be transferred to departments directly. If the **Allow Transfer of Activities to Integrated Queues in Other Departments** ([page 60](#)) setting is enabled, agents can transfer activities to queues of other departments.
- ▶ If the **Allow email transfer to agents who are not available** ([page 62](#)) setting is enabled, agents can transfer activities to other agents who are not available to work on new activities. To be able to transfer an email to an agent, the agent must be logged in to the application, should not have met the concurrent task limit, and should not be working on a non-interruptible activity. If these requirements are not met, the agent is not displayed in the Transfer Activities window.
- ▶ If the **Allow email transfer to agents who are not logged in** ([page 62](#)) setting is enabled, agents can transfer activities to other integrated agents who are not logged in to the application. To be able to transfer an email to an agent, the agent should not have met the concurrent task limit. If this requirement is not met, the agent is not displayed in the Transfer Activities window.
- ▶ An agent can transfer interruptible email activities to another agent. An agent cannot transfer non-interruptible email activities to another agent. The concurrent task limit of the agent is considered in these instances.

Important Things to Note About Transferring Chats

- ▶ Only one chat activity can be transferred at a time.
- ▶ Only open chat activities, in which the customer has not left the chat session, can be transferred.
- ▶ Disabled users are not listed in the list of users to whom you can transfer activities.
- ▶ You can transfer activities only if you have the Transfer action. For more information about actions and permissions, see the *Enterprise Chat and Email Administrator’s Guide to the Administration Console*.

Transferring Chats to Queues:

- ▶ Only agents who match the attributes of a Precision Queue (PQ) that is associated with an ECE queue can transfer chats to that queue.
- ▶ Chats cannot be transferred to departments directly. If the **Allow Transfer of Activities to Integrated Queues in Other Departments** ([page 60](#)) setting is enabled, agents can transfer activities to queues of other departments.
- ▶ A chat can be transferred to any queue that belong to the same media class. From there, the activity is routed based on the queue-to-script mapping.

- ▶ To be able to transfer a chat to a queue, at least one agent who can receive work from that queue must be logged in, must be available, and must not have met the concurrent task limit. The queue must also not be at its maximum task limit.

Transferring Chats to Agents:

Agents who do not meet these conditions are not displayed in the transfer window.

- ▶ Agents can transfer chats to other agents that belong to the same set of skill groups.
- ▶ Only agents who are part of a skill group that is associated with a queue can transfer chats to that queue.
- ▶ The receiving agent must be logged in to the application.
- ▶ The receiving agent must be available, depending on how the **Allow chat transfer to agents who are not available** setting is configured.
- ▶ The receiving agent should not have met the concurrent task limit, unless you are working on non-interruptible chat activities. This may be affected by the **Maximum assignment beyond concurrent task limit** setting.
- ▶ Based on the **Maximum assignment beyond concurrent task limit** setting, agents can transfer additional activities to agents who have reached their concurrent task limit. The maximum number of activities is defined as part of the setting.
- ▶ If the **Allow chat transfer to agents who are not available** ([page 62](#)) setting is enabled, agents can transfer activities to other integrated agents who are not available to work on new activities. To be able to transfer a chat to an agent, the agent must be logged in to the application. Also, the agent should not be at the concurrent task limit (CTL), and the queue associated with the agent should not be at its maximum task limit (MTL). If the CTL and MTL for the agent have been reached, or if the agent is not logged in, the agent is not displayed in the Transfer Activities window.
- ▶ An agent can transfer chat activities to another agent who is working on an interruptible email activity or a non-interruptible chat activity. If the receiving agent is working on a non-interruptible voice call, only interruptible chat activities can be transferred to that agent. Agents working on non-interruptible voice calls cannot be transferred non-interruptible chats.

What are the Actions Assigned to the Default Roles?

Partition Administrator

The various actions assigned to the Partition Administrator role are listed in the following table.

Resource Name	Actions Permitted
User	Create, Own, View, Edit, Delete
User Group	Create, Own, View, Edit, Delete
User Role	Create, View, Edit, Delete
System Attribute Profiles	View, Edit
Application Security	View Application Security, Manage Application Security
Department Security	View Department Security, Manage Department Security
Monitor	Create, Edit, Delete, Run
Integration	Create, View, Edit, Delete
Report	Create, Delete, View, Run, Edit, Schedule
Activity Shortcuts	Create, Read, Edit, Delete
Department	Create, View, Own, Edit, Administer, Copy
Instance	Create, View, Edit, Delete, Start, Stop
Messaging	Create Message, Delete Message
Partition	Administer, View, Edit, Own
Preference Group	Create, View, Edit, Delete
Reference Objects	Create, View, Edit
System Resources	View Knowledge Base, View Reports, View Administration, View Tools, View System, View Supervision

Actions assigned to the Partition Administrator role

Administrator

The various actions assigned to the Administrator role are listed in the following table. Note that the actions featured here do not include all the actions of an administrator that is created when a Unified CCE administrator logs into the console.

Resource Name	Actions Permitted
User	Create, Own, View, Edit, Delete
Activity	Edit Subject, Create, Print, Complete, Unpin, Pull Selected Activities, Edit, Pull Next Activities, Transfer Activities, Add Footer, Add Greeting, Add Attachment, Add Header, Assign Classification, Add Signature, Pin
User Group	Create, Own, View, Edit, Delete
User Role	Create, View, Edit, Delete
User Attribute Profiles	Create, View, Edit, Delete
Screen Attributes Profiles	View, Edit
Department Security	View Department Security, Manage Department Security
Category	Create, View, Edit, Delete
Messaging	Create Message, Delete Message
Customer	Create, View, Edit, Delete, Change
Notes	View, Delete, Add
Preference group	View, Delete, Edit, Create
Resolution Codes	Create, View, Edit, Delete
Customer Associations	Create, View, Edit, Delete
Macro	Create, View, Edit, Delete
Business Objects	Create, View, Edit, Delete
Case	Edit, Print, Close, Unarchive
Filter Folder	Create, Delete, Share Inbox Folder
Monitors	Create, Edit, Delete, Run
Reports	Create, Delete, View, Run, Edit, Schedule
Queue	Create, Own, View, Edit, Delete
Workflow	Create, View, Edit, Delete
Settings	Create, View, Edit, Delete
Shift Label	Create, View, Edit, Delete
Day Label	Create, View, Edit, Delete
Calendar	Create, View, Edit, Delete

Resource Name	Actions Permitted
Dictionary	Create, View, Edit, Delete
Saved Search	Create, Edit, Delete
Service Levels	Create, Read, Edit, Delete
Product Catalog	Create, View, Edit, Delete
Alias	Create, View, Edit, Delete
Blocked Addresses	Create, View, Edit, Delete
Delivery Exceptions	Create, View, Edit, Delete
Transfer Codes	View, Edit
Text Editor	Edit HTML source in reply pane, Edit HTML source for articles
Blocked File Extensions	Create, View, Edit, Delete
Chat	Complete Chat Activity, Leave Chat Activity, Transfer Chat Activity
Email	Send Email, Resubmit supervised emails, Reject emails for supervision, Send and Complete Email, Edit Reply Type, Edit From field, Edit Reply To field, Edit To field, Edit CC field, Edit BCC field, Accept emails for supervision
Chat Resources	Create, View, Edit, Delete
Chat Template Set	Create, View, Edit, Delete
Blocked Attachment	Restore
Incoming Attachment	Delete

Actions assigned to the Administrator role

Agent

The various actions assigned to the Agent role are listed in the following table.

Resource Name	Actions Permitted
System Resource	View Agent Note: This action provides access to the Agent Console
User	View, Pull Activities, Transfer Activities
Category	View
Customer	Create, View, Edit, Delete, Change
Customer Associations	Create, View, Edit, Delete
Contact Person	Create, Edit, Delete
Contact Details	Create, Edit, Delete
Filter Folder	Create, Delete
Notes	View, Add, Delete
Resolution Codes	View
KB Folder	View Folder, Edit Article, Delete Article, Add Notes
Macro	Create, View, Edit, Delete
Product Catalog	View
Activity	Edit Subject, Create, Print, Complete, Unpin, Pull Selected Activities, Edit, Pull Next Activities, Transfer Activities, Add Footer, Add Greeting, Add Attachment, Add Header, Assign Classification, Add Signature, Pin
Case	Edit, Print, Close, Change, Create
Queue	View, Pull Activities, Transfer Activities
Personal Dictionary	Create
Chat	Complete Chat Activities, Transfer Chat Activities
Saved Search	Create, View, Edit, Delete
Email	Send Email, Resubmit supervised emails, Reject emails for supervision, Send and Complete Email, Edit Reply Type, Edit From field, Edit Reply To field, Edit To field, Edit CC field, Edit BCC field, Accept emails for supervision
Email Attachment	Restore, Delete
Incoming Attachment	Delete

Actions assigned to the Agent role

The following table describes some of the important agent actions in detail.

Resource Name	Actions Permitted	Description
Activity	Create	Enables the New Activity button in the Main Inbox toolbar.
	Complete	Enables the Complete button in the Reply pane toolbar when working on email activities, custom activities, or tasks. Also enables the Send & Complete button in the Reply pane toolbar if the Send Email action is also assigned to the agent.
	Pin	Enables the Pin/Unpin button in the in the Main Inbox toolbar.
	Unpin	Allows an agent to pull the pinned activities from other agents.
	Pull Next Activities	Enables the Pull button in the Main Inbox toolbar. To be able to pull activities using this button, the agent needs: <ul style="list-style-type: none"> ▶ Pull Activities action for routing queues. ▶ Pull Activities permission on queues. For chats, the following action is also required: <ul style="list-style-type: none"> ▶ Pull Next Chat Activity action for chats.
	Pull Selected Activities	Enables the Pick button in the Main Inbox toolbar. To be able to pull activities (other than chats) using this button, an agent needs: <ul style="list-style-type: none"> ▶ Pull Activities action for routing queues. ▶ Pull Activities action for users. ▶ Pull Activities permission on queues. ▶ Pull Activities permission on users.
	Transfer Activities	Enables the Transfer button in the Main Inbox toolbar, the Chat Inbox toolbar, and the Reply pane toolbar. To be able to transfer activities using this button, an agent needs: <ul style="list-style-type: none"> ▶ Transfer Activities action for routing queues. ▶ Transfer Activities action for users. ▶ Transfer Activities permission on queues. ▶ Transfer Activities permission on users.
	Assign Classification	Enables the Save button in the Classify section of the Information pane, so that agents can assign categories and resolution codes to activities.
Case	Edit	Allows an agent to edit the case details. Enables the Save button in the Information pane, Case section. The Case status field is enabled only if the agent has the Close Case action.
	Close Case	Allows an agent to close an open case. It enables the Close Case button in the Inbox pane toolbar (Inbox Tree pane > My Work > Cases > My Cases > Open). If the agent has the Edit case action, it also enables the Case status field in the Information pane, Case section.
	Change Case	Allows an agent to change the case of an activity and associate it with an existing case. It enables the Change Case button in the Information pane, Case section.
	Create Case	Allows an agent to create new cases. When a new case is created, the old case associated with the activity is closed and the activity is associated with the new case. It enables the Create Case button in the Information pane, Case section.

Resource Name	Actions Permitted	Description
Chat	Complete Chat Activity	Enables the Complete button in the Chat pane toolbar.
	Leave Chat Activity	Enables the Leave button in the Chat pane toolbar. Allows an agent to leave a chat without completing the activity. The activity gets completed only when the customer closes the chat session.
	Pull Next Chat Activity	Enables the Pull button. Allows an agent to pull chat activities from queues. To be able to pull chat activities the agent also needs: <ul style="list-style-type: none"> ▶ Pull Next Activities action for activities ▶ Pull Activities action for routing queues ▶ Pull Activities permission on queues
	Transfer Chat Activity	Enables the Transfer button in the Chat pane toolbar. Allows an agent to transfer chats to other agents, queues, and departments. To be able to transfer chats using this button, the agent needs: <ul style="list-style-type: none"> ▶ Transfer Activities action for routing queues ▶ Transfer Activities action for users ▶ Transfer Activities permission on queues ▶ Transfer Activities permission on users

Resource Name	Actions Permitted	Description
Customer	Create	Allows agents to create new customers. It enables the Save button when an agent creates a new customer (by clicking the New button) from the Information pane, Customer section. Agents can also create new customers while creating new activities. In the New Activity Window (which opens on clicking the New Activity button in the Inbox pane toolbar), it displays the New option in the Customer field.
	Edit	Allows an agent to edit the details of a customer. It enables the Save button in the Information pane > Customer section toolbar.
	Delete	Allows an agent to delete a customer associated with an activity. It enables the Delete button in the Information pane, Customer section toolbar.
	Change Customer	Allows an agent to change the customer associated with an activity. Displays the Change customer button in the Information pane, Customer section toolbar.
	Create Contact Person	Allows an agent to create a contact person for group and corporate customers. It enables the New button in the Information pane, Customer section toolbar when the Contact person node is selected. It is available for group and corporate customers only.
	Edit Contact Person	Allows an agent to edit the details of a contact person for group and corporate customers. It enables the Save button in the Information pane, Customer section toolbar when a contact person is selected.
	Delete Contact Person	Allows an agent to delete a contact person for group and corporate customers. It enables the Delete button in the Information pane, Customer section toolbar when a contact person is selected.
	Create Contact Details	Allows an agent to create contact details for a customer. It enables the New button in the Information pane, Customer section toolbar when the Contact details node is selected.
	Edit Contact Details	Allows an agent to edit the contact details of a customer. It enables the Save button in the Information pane, Customer section toolbar when a contact detail is selected.
	Delete Contact Details	Allows an agent to delete the contact details of a customer. It enables the Delete button in the Information pane, Customer section toolbar when a contact detail is selected.
	Create Association	Allows an agent to associate products, accounts, contracts, or other custom associations available in the system with a customer. It enables the New button in the Information pane, Customer section toolbar when an association is selected.
	Edit Association	Allows an agent to edit the associations associated with a customer. It enables the Save button in the Information pane, Customer section when an association is selected.
	Delete Association	Allows an agent to delete the associations associated with a customer. It enables the Delete button in the Information pane, Customer section when an association is selected.
	Email	Send Email
Email attachment	Restore	It allows agents to restore blocked attachments. It enables the Restore button in the View Attachments window, which opens when an agent double-clicks the Attachment icon in the Inbox List pane.
	Delete	It allows agents to delete blocked attachments. Unblocked attachments cannot be deleted. It enables the Delete button in the View Attachments window, which opens when an agent double-clicks the Attachment icon in the Inbox List pane.

Resource Name	Actions Permitted	Description
Filter Folder	Create	Enables the New and Properties buttons in the Inbox Tree pane toolbar. Using these buttons, agents can create and edit search folders and personal folders in their inbox.
	Delete	Enables the Delete button in the Inbox Tree pane toolbar. Using this button, agents can delete search folders and personal folders from their inbox.
KB Folder	View Folder	Agents can only view articles in the folders on which they have the View Folder permission. All agents have permissions to view articles in the following standard folders and it cannot be removed - headers, footers, greetings, signatures, quick links, and quick responses. But, if any folders are created under these standard folders, then administrators can select not to give View Folder permission on those folders.
	Add Notes	Allows agents to view, delete, and add notes. It enables the Notes button.
Macro	View	Allows agents to view and use macros in emails, chats, tasks, and custom activities. It enables the Add macro button in the reply pane.
Notes	View	<p>Allows an agent to view notes associated with cases, activities, customers, and customer associations. It displays the View notes option in the Notes window, which can be accessed using the Notes button from the following panes:</p> <ul style="list-style-type: none"> ▶ Main Inbox toolbar ▶ Chat Inbox toolbar ▶ Reply pane ▶ Chat pane ▶ Information pane, in the following sections: Activity, Case, History, and Customer.
	Add	<p>Allows an agent to add notes to cases, activities, customers, and customer associations. It displays the Add notes option in the Notes window, which can be accessed using the Notes button from the following panes:</p> <ul style="list-style-type: none"> ▶ Main Inbox ▶ Chat Inbox ▶ Reply pane ▶ Chat pane ▶ Information pane, in the following sections: Activity, Case, History, and Customer. <p>If an agent has the View Notes action, it also enables the Add button in the Notes window. It displays the Add notes option in the Notes window, which can be accessed using the Notes button from the following panes:</p> <ul style="list-style-type: none"> ▶ Main Inbox ▶ Chat Inbox ▶ Reply pane ▶ Chat pane ▶ Information pane, in the following sections: Activity, Case, History, and Customer.
	Delete	<p>Allows an agent to delete the notes associated with cases, activities, customers, and customer associations. It enables the Delete button in the Notes window. The Notes window can be accessed using the Notes button from the following panes:</p> <ul style="list-style-type: none"> ▶ Main Inbox ▶ Chat Inbox ▶ Reply pane ▶ Chat pane ▶ Information pane, in the following sections: Activity, Case, History, and Customer. <p>The Notes window can only be accessed by agents with the View Notes action.</p>

Resource Name	Actions Permitted	Description
Routing Queue	Pull Activities	<p>Allows agents to pull activities from routing queues. To be able to pull activities from queues, an agent needs:</p> <ul style="list-style-type: none"> ▶ Pull Next Activities or Pull Selected Activities action for activities ▶ Pull Activities permission on routing queues <p>For chats, the following action is also required:</p> <ul style="list-style-type: none"> ▶ Pull Next Chat Activity action for chats
	Transfer Activities	<p>Allows agents to transfer activities to routing queues. To be able to transfer activities to queues, an agent needs:</p> <ul style="list-style-type: none"> ▶ Transfer Activities action for activities ▶ Transfer Activities permission on queues
System Resource	View Agent Console	Allows an agent to access the Agent Console.
User	Pull Activities	<p>Allows agents to pull activities from other agents. To be able to pull activities from other agents, an agent needs:</p> <ul style="list-style-type: none"> ▶ Pull Selected Activities action for activities ▶ Pull Activities permission on users
	Transfer Activities	<p>Allows agents to transfer activities to other agents. To be able to transfer activities to other agents, an agent needs:</p> <ul style="list-style-type: none"> ▶ Transfer Activities action for activities ▶ Transfer Activities permission on users

Some important actions assigned to the Agent role

Agent (Read Only)

The various actions assigned to the Agent (Read Only) role are listed in the following table.

Resource Name	Actions Permitted
System Resource	View Agent Note: This action provides access to the Agent Console
User	View
Category	View
Customer	View
Filter Folder	Create, Delete
Notes	View
KB Folder	View
Product Catalog	View
Resolution Codes	View
Macro	View
Activity	Print
Case	Print
Queue	View

Actions assigned to the Agent (read only) role

Supervisor

The following table lists the actions that are part of the default Supervisor role that are required to perform various supervisor tasks in the Agent Console, Supervision Console, and Reports Console.

Object	Actions permitted
System Resource	View Agent, View Reports, View Supervision Note: These actions provide access to the Agent Console, Reports Console, and Supervision Console
Report	Create, Delete, View, Run, Edit, Schedule Note: With these actions, users can manage reports from the Reports Console.
Monitor	Create Edit, Delete, Run Note: With these actions, users can manage monitors from the Supervision Console.
Activities	Create, Print, Edit Subject, Pin, Complete, Edit, Transfer Activities, Unpin, Add Greetings, Add Header, Add Attachment, Add Folder, Add Signature, Assign Classification
Case	Edit, Print, Close Case, Change Case, Create Case
Categories	View
Chat	Complete Chat Activity, Leave Chat Activity, Transfer Chat Activities,
Customer	View Association, Create Association, Edit Association, Delete Contact Person, Delete Contact Details, Delete Association, Edit Contact Details, Edit Contact Person, Change Customer, View, Edit, Delete, Create, Create Contact Details, Create Contact Person
Email	Resubmit supervised email, Reject emails for supervision, Accept emails for supervision Send Email, Send and Complete Email, Edit Reply To field, Edit Reply Type, Edit From field, Edit CC field, Edit BCC field, Edit To field Note: The following actions enable the supervisor to review outbound email activities: Resubmit supervised email, Reject emails for supervision, Accept emails for supervision
Email Attachment	Delete, Restore
Filter Folder	Create, Delete, Share Inbox Folder
KB Folder	View Folder, Delete Notes, Add Notes
Macros	View
Messaging	Create Message, Delete Message
Notes	View, Add, Delete
Personal Dictionary	Personal Dictionary
Product Catalog	View
Resolution	View
Routing Queue	View, Pull Activities, Transfer Activities
Saved Search	Edit, Create, Delete
Text Editor	Edit HTML source in reply pane, Edit HTML source for articles

Object	Actions permitted
Users	View, Pull Activities, Transfer Activities
Note: The following actions are part of the Supervisor role but can be used only if the “View Administration” action is explicitly added to the Supervisor role.	
Alias	Create, View, Edit, Delete
Blocked Address	Create, View, Edit, Delete
Blocked File Extension	Create, View, Edit, Delete
Delivery Exceptions	Create, View, Edit, Delete
Chat Resources	Create, View, Edit, Delete
Chat Template Set	Create, View, Edit, Delete

Actions assigned to the Supervisor role

Supervisor (Read Only)

The various actions assigned to the Supervisor (Read Only) role are listed in the following table.

Resource Names	Actions Permitted
System Resource	View Agent, View Reports, View Supervision Note: These actions provide access to the Agent Console, Reports Console, and Supervision Console
User	View
Customer	View
Association	View
Aliases	View
Blocked Address	View
Blocked File Extension	View
Chat Resources	Create, View, Edit, Delete
Chat Template Set	Create, View, Edit, Delete
Inbox Folder	Create, Delete
Delivery Exceptions	View
Categories	View
Filter Folder	View
Notes	View
Product Catalog	View
Resolution Codes	View
KB Folder	View
Macro	View
Activity	Print
Case	Print
Monitor	Create, Edit, Delete, Run
Reports	View, Run
Queue	View

Actions assigned to the Supervisor (read only) role

Managing User Roles

This section talks about:

- ▶ [“Creating User Roles” on page 99](#)
- ▶ [“Assigning User Subroles” on page 100](#)
- ▶ [“Copying User Roles” on page 101](#)
- ▶ [“Restoring User Roles” on page 102](#)
- ▶ [“Deleting User Roles and Subroles” on page 102](#)

Creating User Roles

To create a user role:

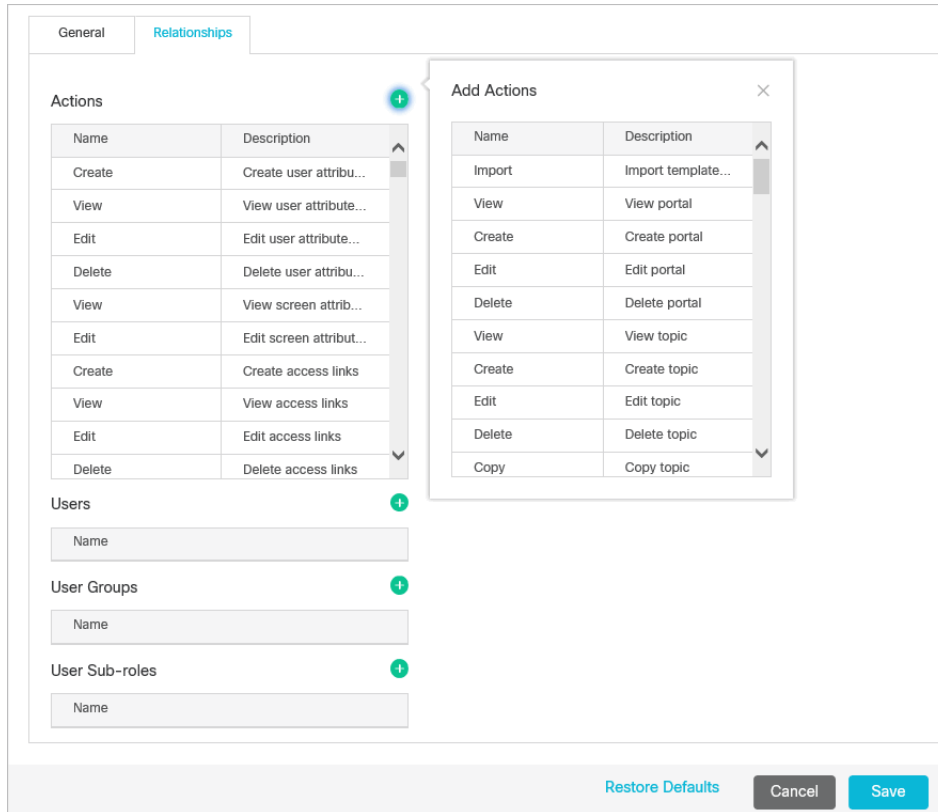
1. In the department-level Top menu, click the **User Management** option.
2. In the Left menu, navigate to **Roles**.
3. Click the **New** button.
4. In the Create Role space, on the General tab, set the following:
 - **Name:** Provide a name for the role
 - **Description:** Provide a brief description.
 - **Template:** From the dropdown list, select an available template.

The screenshot shows a 'Create Role' dialog box with two tabs: 'General' (selected) and 'Relationships'. The 'General' tab contains three input fields: 'Name*' with the value 'NewRole', 'Description' with the value 'New Role based on Administration.', and 'Template*' with a dropdown menu showing 'Administrator Template'. At the bottom right of the dialog, there are three buttons: 'Restore Defaults' (light blue), 'Cancel' (grey), and 'Save' (teal).

Create new role

5. Click the **Save** button. This enables the Relationships tab.
6. Next, go to the **Relationships** tab and do the following.
 - a. In the Actions section, select the actions for the role. The Actions section shows the list of actions associated with the template. You can customize the role by adding or removing actions. If you feel you want to go back to the original list of actions, you can restore the role to its default state.

- b. Go to the User groups section, and assign the role to user groups. You can also choose to assign roles to users individually; however, it is recommended that you assign roles to user groups. It helps you manage your users better.
- c. Next go to the Users section, and assign the role to users.
- d. Now go to the User subroles section, and select the roles you want to associate with this role as subroles. You can even set default roles as subroles. To know more about subroles, see [“Assigning User Subroles” on page 100](#).



Add actions, user groups, users, and sub-roles to the roles

7. Click the **Save** button to save the role that you have created.

Assigning User Subroles

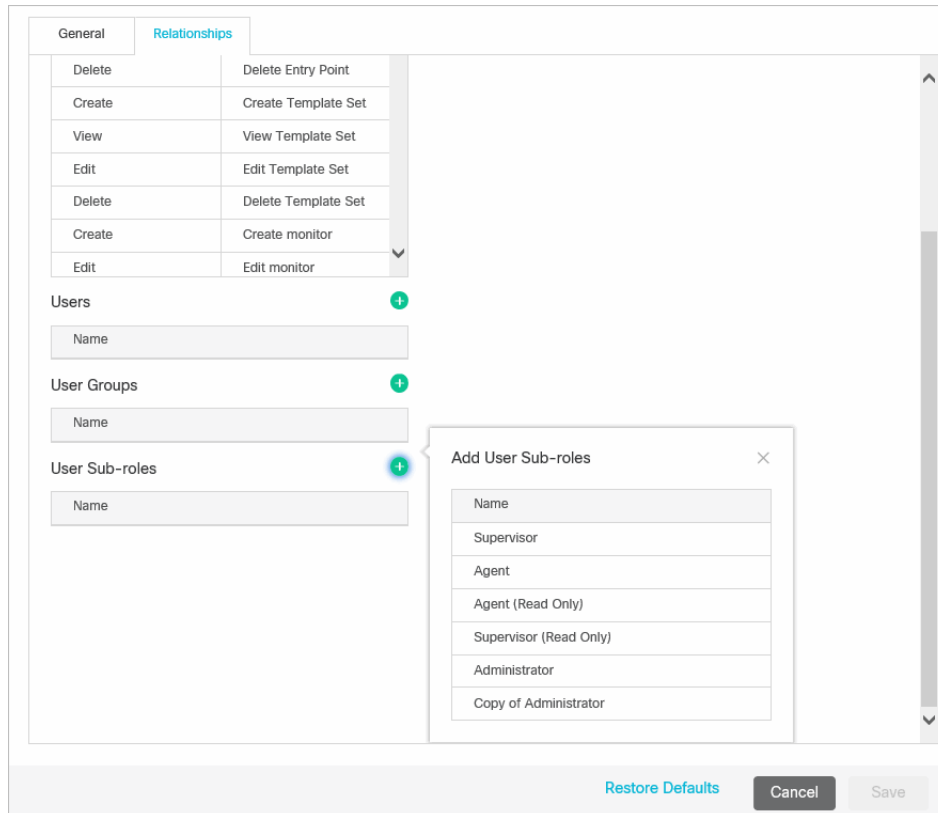
A subrole is a subset of actions required by a user to function in the system. It is an advanced feature of user management and it helps you manage user actions in a better way. You can create task-based roles and use these roles as subroles of bigger roles in the system. For example, you want your supervisor and administrator to have some common actions. Instead of assigning individual actions to the user, you can create a role, with those actions, and associate that role as a sub role to the supervisor and administrator role.

A role can be a subrole of more than one roles.

To create a subrole:

1. In the department-level Top menu, click the **User Management** option.

2. In the Left menu, navigate to **Roles**.
3. Select the role for which you want to assign a subrole.
4. Go to Relationships tab. In the User subroles section, click the **Add +** button and select from the available roles.



Select subroles

When a role with subroles is assigned, all its subroles are automatically assigned to the users.

Copying User Roles

When you copy a role, the description of the role and the actions and user subroles associated with the role are copied. The copied role is not assigned to any users or user groups.

To copy a role:

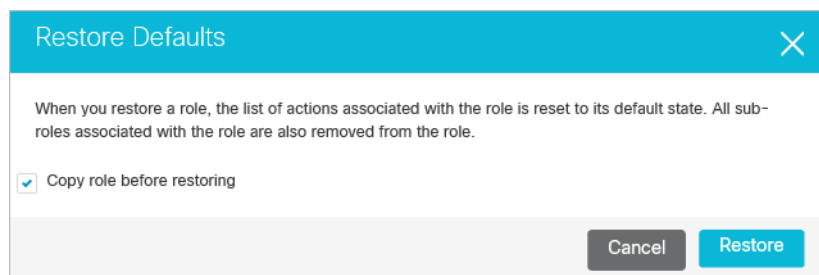
1. In the department-level Top menu, click the **User Management** option.
2. In the Left menu, navigate to **Roles**.
3. Click the **Assistance** button in the Actions column next to the role you wish to copy.
4. Select the **Create Copy** option.

Restoring User Roles

When you restore a role, the list of actions associated with the role is reset to its default state.

To restore a role:

1. In the department-level Top menu, click the **User Management** option.
2. In the Left menu, navigate to **Roles**.
3. In the Roles space, select the role you want to restore to its default state.
4. In the Edit Role workspace, click the **Restore Defaults** button.
5. In the window that appears, perform the following:
 - Click the **Copy role before restoring** box to create a copy of the role along with all sub-roles assigned to it.
 - Click the **Restore** button to restore the defaults of the role.



Restore the defaults of the role

Deleting User Roles and Subroles

Delete the user roles that are not needed anymore. Before deleting a role, make sure that it is not assigned to any user. The system does not check to see if the role is in use or not.

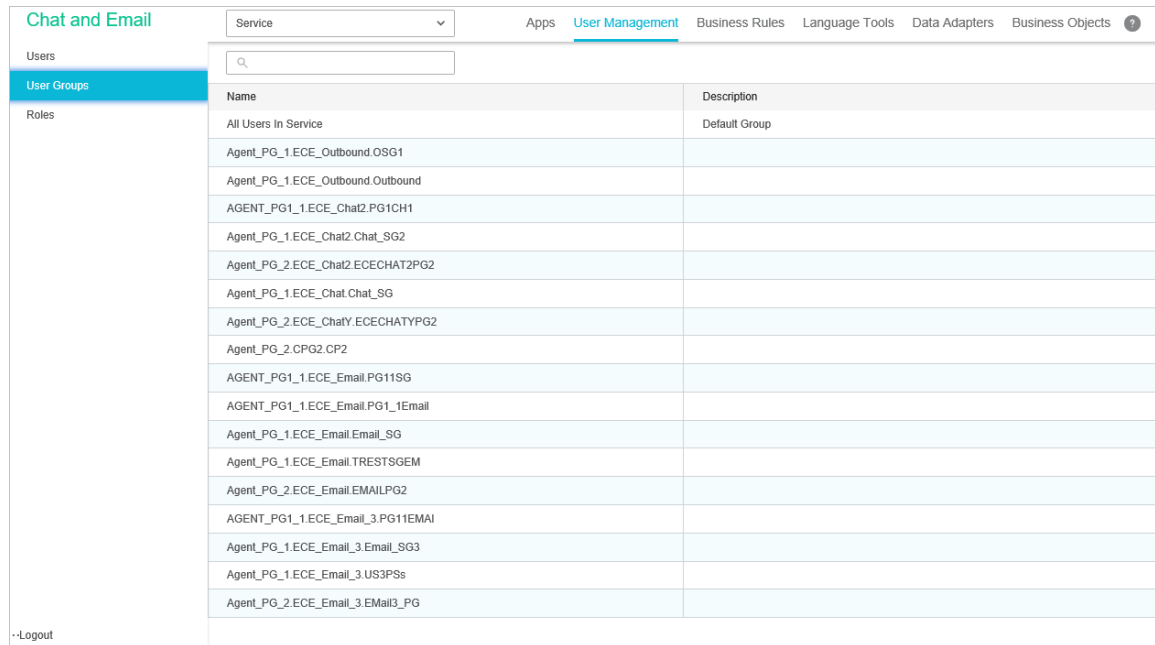
The system provided roles cannot be deleted.

To delete a user role or subrole:

1. In the department-level Top menu, click the **User Management** option.
2. In the Left menu, navigate to **Roles**.
3. Click the **Assistance** button in the Actions column next to the role you wish to delete.
4. Click the **Delete** option.
5. In the Delete Role window that appears, click the **Yes** button to confirm the deletion.

Managing User Groups

User groups are created in the system by importing users from Unified CCE to the application. New user groups cannot be manually created within the application. To learn more about importing users, see [“Importing Data” on page 26](#).






The screenshot shows the 'User Management' interface. The top navigation bar includes 'Service', 'Apps', 'User Management', 'Business Rules', 'Language Tools', 'Data Adapters', and 'Business Objects'. The left sidebar has 'Users', 'User Groups', and 'Roles'. The main area displays a table of user groups with columns for 'Name' and 'Description'. A search bar is located at the top of the table.

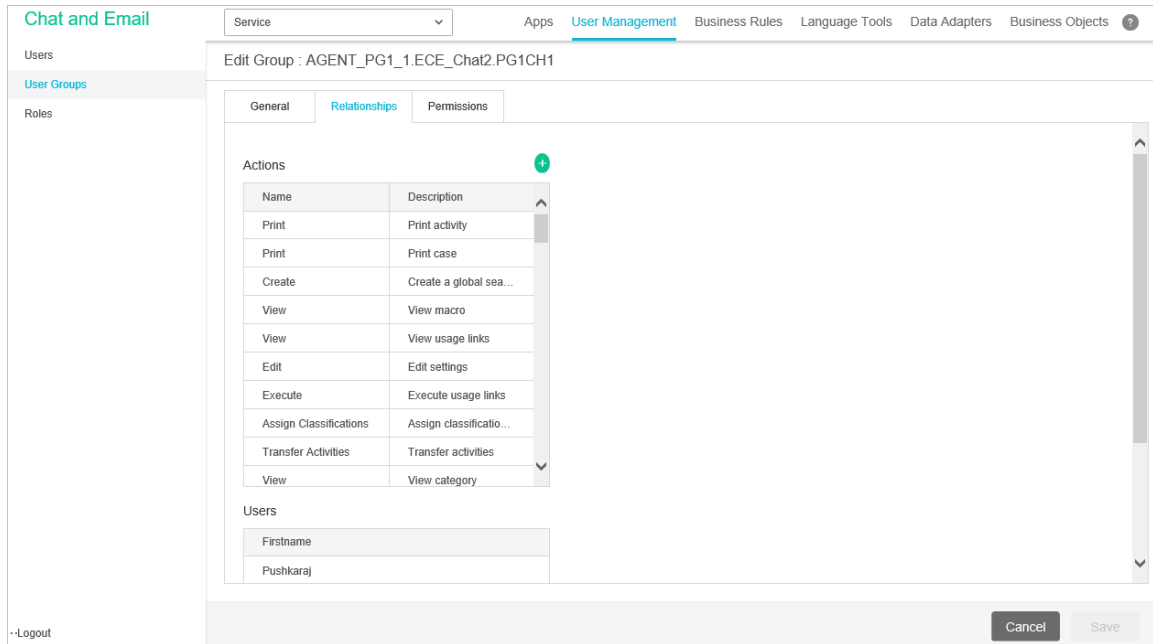
Name	Description
All Users In Service	Default Group
Agent_PG_1.ECE_Outbound.OSG1	
Agent_PG_1.ECE_Outbound.Outbound	
AGENT_PG1_1.ECE_Chat2.PG1CH1	
Agent_PG_1.ECE_Chat2.Chat_SG2	
Agent_PG_2.ECE_Chat2.ECECHAT2PG2	
Agent_PG_1.ECE_Chat.Chat_SG	
Agent_PG_2.ECE_ChatY.ECECHATYPG2	
Agent_PG_2.CPG2.CP2	
AGENT_PG1_1.ECE_Email.PG11SG	
AGENT_PG1_1.ECE_Email.PG1_1Email	
Agent_PG_1.ECE_Email.Email_SG	
Agent_PG_1.ECE_Email.TRESTSGEM	
Agent_PG_2.ECE_Email.EMAILPG2	
AGENT_PG1_1.ECE_Email_3.PG11EMAI	
Agent_PG_1.ECE_Email_3.Email_SG3	
Agent_PG_1.ECE_Email_3.US3PPS	
Agent_PG_2.ECE_Email_3.EMail3_PG	

Select a User Group

To edit user groups:

1. In the top menu, select the **User Management** option.
2. In the Left menu, navigate to **User Groups**.
3. Select a user group to edit.
4. In the Edit Group workspace, under the General tab, the following information is provided and cannot be changed:
 - Name
 - Description
 - Peripheral
 - Skill Group
 - Type
 - Media Routing Domain
5. Under the **Relationships** tab, edit the following fields:
 - **Actions:** Click the **Search and Add**  button and select an action to add it to the Actions list. To remove an action from the list, hover your mouse over it and click the **Delete** button.
 - **Users:** Users that are assigned to the user group appear here and cannot be changed.

- **Languages:** Click the **Search and Add**  button and select languages to apply to the user group. To remove a language from the list, hover your mouse over it and click the **Delete** button.
- **User roles:** Click the **Search and Add**  button and select user roles to apply to the user group. To remove a role from the list, hover your mouse over it and click the **Delete** button.



Assign the actions, users, languages, and roles to the user group

6. Under the **Permissions** tab, select the permissions that you want to assign to the user group.
7. Click **Save** button.

Managing Users

Administrators are created in the system during the installation and additional administrators can be created within the application later. All other users must be imported from Unified CCE. Users cannot be manually created within the application. To learn more about importing users, see [“Importing Users” on page 27](#).

This section talks about:

- ▶ [Editing Department Users on page 105](#)

► [Assigning Manager of Users on page 107](#)

User Name	First Name	Last Name	Status
kon	Konstantin	Goldman	Not logged in
hgupta	Himanshu	Gupta	Not logged in
pgupta	Priya	Gupta	Not logged in
ahaight	Ashley	Haight	Not logged in
anigam1	Avinash	Nigam	Not logged in
nrez	Nataliya	Rez	Not logged in
pss	Pushkaraj	Shingre	Not logged in
hstak	testag	a	Not logged in
pq	PQ	agent	Not logged in
ewm2	ewm1	ewm1	Not logged in
integ	integ	integ	Not logged in
akintali@ustraining.com	Aditya	kintali	Not logged in
test	test	test	Not logged in
pg21	pg21	pg21	Not logged in
PG11	Pushkaraj	Shingre	Not logged in

Select a user from the list of users

Editing Department Users

Department users cannot be created within ECE and can only be imported from Unified CCE or Packaged CCE. A majority of the properties for these users are edited and controlled there. For more information, see [“Importing Data” on page 26](#).

There are multiple properties and fields within ECE that apply to users within the application and can be edited once they have been properly imported to the application.



Important: If you are editing the properties of a user who is logged into the application, the user updates take effect only on the next login.

To edit user details:

1. In the department-level Top menu, select the **User Management** option.
2. From the Left menu, navigate to **Users**.
3. From the table, select the user you want to edit
4. In the Edit User space, the following options details are displayed:
 - **Username:** The username under which this user appears in the system. This is managed in Unified CCE and cannot be changed here.
 - **Screen name:** The name under which this user is visible in chats and communications. This is managed in Unified CCE and cannot be changed here.
 - **Title:** Select a title from the dropdown menu.
 - **First name:** The user's first name. This is managed in Unified CCE and cannot be changed here.
 - **Middle name:** The user's middle name.
 - **Last name:** The user's last name. This is managed in Unified CCE and cannot be changed here.

- **Suffix:** The professional suffix for this user (for example, MD).
- **Password:** The user's password. This is managed in Unified CCE and cannot be changed here.
- **Manager:** Select a user from the dropdown to assign a manager to this user.
- **Authentication Type:** The method in which the user accesses the application. This is managed in Unified CCE and cannot be changed here.
- **User Status:** The current status of the user. This is managed in Unified CCE and cannot be changed here.
- **Peripheral:** The peripheral gateway to which the user is assigned. This is managed in Unified CCE and cannot be changed here.
- **Unified CCE Agent Login Name:** The login name for the user in Unified CCE. This is managed in Unified CCE and cannot be changed here.
- **Email Address:** An external email address for the user. This is managed in Unified CCE and cannot be changed here.


The screenshot shows the 'Edit User' form for user 'hgupta'. The form is divided into three tabs: 'General', 'Relationships', and 'Permissions'. The 'General' tab is active and contains the following fields:

- Username*: hgupta
- Screen name: Himanshu Gupta
- Title: Select Title (dropdown)
- First name*: Himanshu
- Middle name: Name
- Last name*: Gupta
- Suffix: suffix
- Password: (password field)
- Manager: (dropdown)
- Authentication Type: Local Login (dropdown)

At the bottom of the form, there are 'Cancel' and 'Save' buttons. The left sidebar shows 'Users' and 'Roles' sections.

Edit the general information for a user

5. Under the Relationships tab, edit the following fields:
 - **Actions:** Click the **Search and Add** (+) button and select an action to add it to the Actions list, applying the action to the user. To remove an action from the list, hover your mouse over it and click the Delete button. Actions applied to the user by the user group to which the user is assigned cannot be removed.
 - **User Groups:** The user groups to which the user is assigned. This cannot be changed.
 - **Languages:** Click the **Search and Add** (+) button and select languages to apply to the user. To remove a language from the list, hover your mouse over it and click the Delete button.
 - **User Roles:** Click the **Search and Add** (+) button and select user roles to apply to the user. To remove a role from the list, hover your mouse over it and click the Delete button. Roles applied to the user by the user group to which the user is assigned cannot be removed.

- **Direct Reports:** Click the **Search and Add**  button and select the users who report to the user you are editing. This makes the current user a supervisor for the selected users in this list.
6. Under the Permissions tab, select the permissions that you want to assign to the user group.
 7. Click the **Save** button.


Assigning Manager of Users

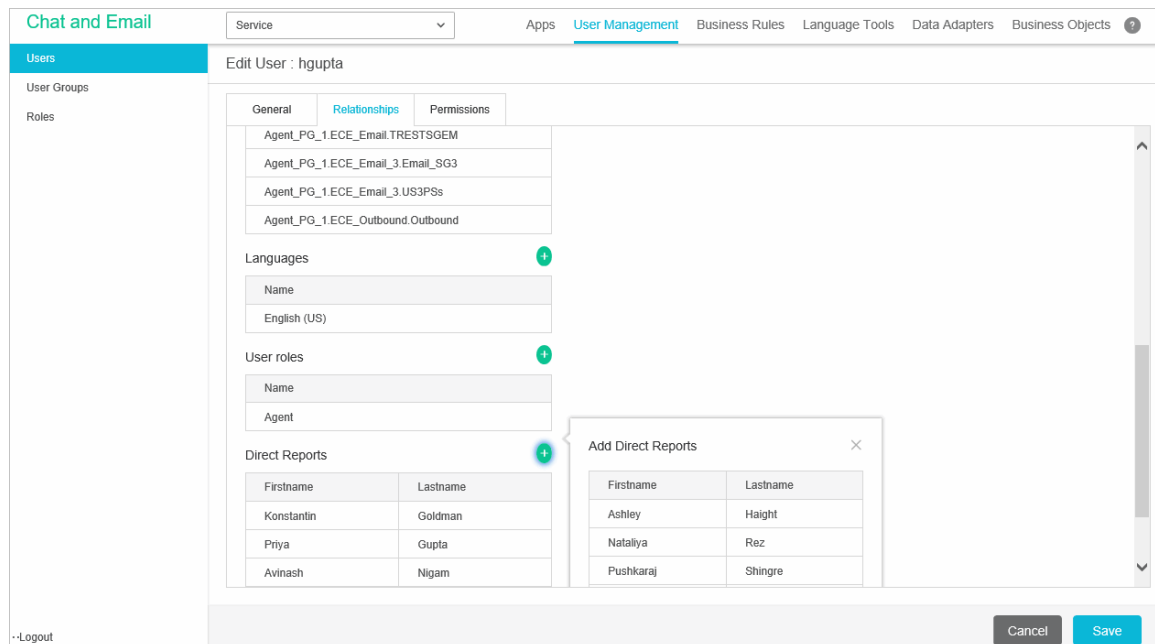
A manager can monitor the activities and cases assigned to agents from the Agent Console. The manager has a read only view of the activities and cases assigned to the users reporting to him.

You can assign a manager of the user in two ways. Either edit the properties of the manager to assign direct reports to him. Or, edit the user properties to assign the manager to the user. Use the first option if all the users are already created in the system and you want to assign managers for all the users. Use the second option to assign a manager while creating the user.

You cannot assign managers of user groups.

To assign a manager of a user:

1. In the department-level Top menu, select the **User Management** option.
2. From the Left menu, navigate to **Users**.
3. From the table, select the user you want to edit.
4. In the Edit User space, perform one of the following:
 - Under the Relationships tab, in the Direct Reports section, click the **Search and Add**  button and select the users who report to the user you are editing. This makes the current user a supervisor for the selected users in this list.



The screenshot shows the 'Edit User' interface for user 'hgupta'. The 'Direct Reports' section is active, displaying a table of users reporting to the current user. A modal window titled 'Add Direct Reports' is open, allowing selection of users from a list.

Firstname	Lastname
Konstantin	Goldman
Priya	Gupta
Avinash	Nigam

Firstname	Lastname
Ashley	Haight
Nataliya	Rez
Pushkaraj	Shingre

Select the users reporting to this user

- If you are assigning the manager of the user, navigate to the General tab. In the Manager field, select a user from the dropdown menu. The user selected in the manager field becomes the manager of the user you are editing.

The screenshot shows the 'Edit User' interface for user 'hgupta'. The 'General' tab is active, and the 'Manager' field has a dropdown menu open. The dropdown menu lists the following users: Konstantin Goldman, Priya Gupta, Ashley Haight, Avinash Nigam, Nataliya Rez, and Pushkaraj Shingre. The 'hgupta' user is currently selected in the dropdown. Other fields visible include Middle name (Name), Last name* (Gupta), Suffix (suffix), Password, Authentication Type, User status*, Peripheral, Unified CCE Agent Login Name (hgupta), and Email Address. The interface includes a 'Logout' link at the bottom left and 'Cancel' and 'Save' buttons at the bottom right.

Select a manager of the user

5. Click the **Save** button.



Configuring Security

- ▶ [Cross-Origin Resource Sharing](#)
- ▶ [Enabling Cross-Origin Resource Sharing](#)
- ▶ [About File Attachments](#)
- ▶ [Configuring Attachment Settings](#)
- ▶ [Rich Text Content Policies](#)
- ▶ [Enabling and Disabling Rich Text Content Policies](#)
- ▶ [Exporting and Importing Rich Text Content Policies](#)
- ▶ [Configuring the Rich Text Content Policy File](#)
- ▶ [Restoring Rich Text Content Policies](#)

Cross-Origin Resource Sharing

Cross-origin resource sharing (CORS) is a mechanism that allows resources (for example, fonts, JavaScript, and so on.) on a web page to be requested from another domain outside the domain from which the resource originated.



Important: CORS functionality is supported on Internet Explorer 10 and 11, as well as Firefox, Chrome, Safari, and Opera.

An administrator can do the following:

- ▶ Enable CORS
- ▶ Select the CORS origins to be used. The administrator can allow all origins or manually add selected websites.

Enabling Cross-Origin Resource Sharing

To enable cross-origin resource sharing:

1. In the partition-level Top menu, click the **Security** option.
2. In the Left menu, navigate to **CORS**.
3. In the Cross Origin Resource Sharing space, set the following:
 - **Enable Cross Origin Resource Sharing:** Click the toggle to enable CORS. By default, CORS is enabled in the application.
 - Select **Allow all origins for CORS** or select **Allow following origins for CORS** and provide the list of allowed websites for CORS. The URL must contain a protocol, `http` or `https` (in lower case), followed by the domain name or IP address. The domain name can contain only numbers, alphabets, dot (`.`), and hyphen (`-`). For example, `http://company-name.com` or `https://10.10.20.30`

Enable CORS

4. Click the **Save** button.

About File Attachments

You can specify the file types that can be attached to emails, chat messages, and articles in the knowledge base. You can choose to allow or block specific file types by creating a white list or black list, respectively. Additionally, you can enable attachments for chat and specify the maximum allowed size for chat attachments.

Attachments for chat can also be controlled at the queue level as well, allowing you to limit file sharing to chats in specific queues. For more information about queue-specific settings, see *Enterprise Chat and Email Administrator's Guide to Routing and Workflows*.

Configuring your list of blocked and allowed file types at this level affects all departments within the partition and supersedes any blocked file extensions for emails set at the department level. For more information about blocked file extensions for email, see the *Enterprise Chat and Email Administrator's Guide to Email Resources*.

Configuring Attachment Settings

To configure attachment settings for the partition:

1. In the partition-level Top menu, click the **Security** option.
2. In the Left menu, navigate to **Attachments**.
3. In the Attachments space, set the following fields
 - **Allow or Block File Type:** Set the dropdown field to one of the following options.
 - **Allow all file types**
 - **Block file types listed below**
 - **Allow file types listed below**
 - **File Types (csv):** If you selected either Block file types listed below or Allow file types listed below, enter the file extensions you wish to specifically block or allow. The extensions require a period in front of their names and a comma to separate each entry. For example:
`.txt,.exe,.xls,.pdf,.png,.log,.xml`
 - **Enable Chat Attachments for Agents and Customers:** Click the switch to enable or disable chat attachments for the partition.
 - **Maximum Size For Each Chat Attachment (MB):** Set the maximum allowed size for a chat attachment from the dropdown menu. Values include: 2 MB, 3 MB, 4 MB, 5 MB, 6 MB, 7 MB, 8 MB, 9 MB, 10 MB.
 - **Maximum Size For Each Email Template Attachment (MB):** Set the maximum total size allowed for one or multiple attachments to emails. This setting applies to attachments in header, greeting, footer, and signature articles for emails.

If the combined file size of the attachments exceed this maximum, the email is rejected. Minimum allowed value is 1 MB and maximum allowed value is 25 MB.

The screenshot shows the 'Chat and Email' settings page. The 'Attachments' section is active, displaying the following configuration:

- Allow or Block File Type: Block file types listed below
- File Types (csv): .csv
- Enable Chat Attachments For Agents and Customers:
- Maximum Size For Each Chat Attachment (MB): 4
- Maximum Size For Each Email Template Attachment (MB): 4

Buttons for 'Cancel' and 'Save' are visible at the bottom right of the settings panel.

Configure the attachment settings

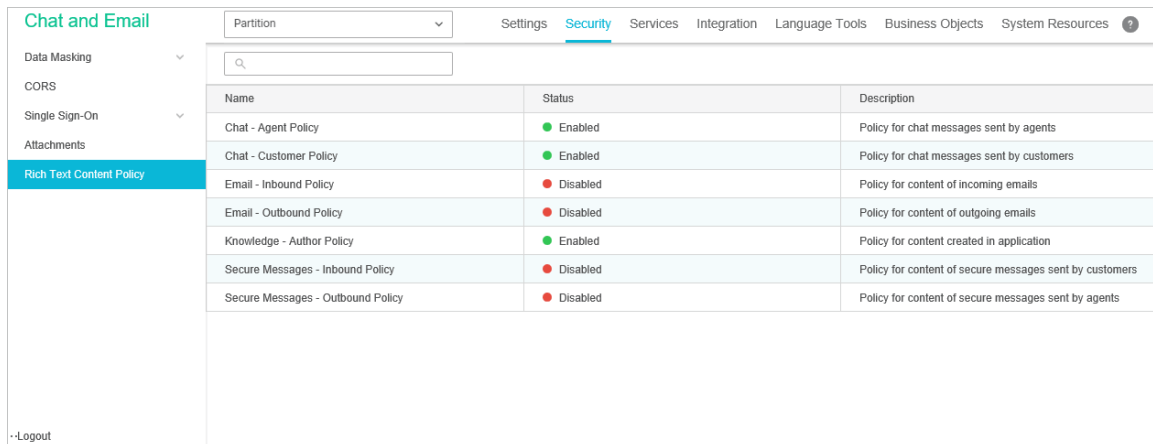
4. Click the **Save** button.

Rich Text Content Policies

In order to prevent Cross Site Scripting (XSS) issues from rich text content entered by agents, customers, and authors in chat messages and knowledge articles, the application enforces a default content policy that whitelists the allowed HTML and CSS elements and attributes. Application security administrators can modify the content policy to meet their requirements. Administrators can modify the content policy for each of the following:

- ▶ **Chat - Agent Policy:** Governs chat messages sent by agents to customers
- ▶ **Chat - Customer Policy:** Governs chat messages sent by customers to agents
- ▶ **Email - Inbound Policy:** Governs content of standard and secure incoming emails
- ▶ **Email - Outbound Policy:** Governs content of standard and secure outgoing emails
- ▶ **Knowledge - Author Policy:** Governs knowledge article content created by authors
- ▶ **Secure Messages - Inbound Policy:** Governs secure messages sent by customers

► **Secure Messages - Outbound Policy:** Governs secure messages sent by agents



Name	Status	Description
Chat - Agent Policy	● Enabled	Policy for chat messages sent by agents
Chat - Customer Policy	● Enabled	Policy for chat messages sent by customers
Email - Inbound Policy	● Disabled	Policy for content of incoming emails
Email - Outbound Policy	● Disabled	Policy for content of outgoing emails
Knowledge - Author Policy	● Enabled	Policy for content created in application
Secure Messages - Inbound Policy	● Disabled	Policy for content of secure messages sent by customers
Secure Messages - Outbound Policy	● Disabled	Policy for content of secure messages sent by agents

Select a rich text content policy

The content policy is an XML file that outlines the rules to be followed while parsing the content. It primarily addresses three things:

- What HTML tags should be allowed?
- What attributes of these HTML tags should be allowed?
- What values of these attributes should be allowed?

When the rich text content policies have been enabled, the application can begin validating and sanitizing the content of users.

- **Input validation:** If the content violates the defined policy, entire content is rejected and the user is shown an error message indicating the same. Validation is applied to:
 - Customer to Agent Chat Data (Using Chat - Customer Policy)
 - Agent to Customer Chat Data (Using Chat - Agent Policy)
- **Input sanitation:** If the content violates the defined policy, the attributes that violate the policy are stripped off and the sanitized content is saved in application. Users are not shown errors during sanitation. Sanitation is applied to:
 - Note Content (Using Default Policy)
 - Internal Messaging – Body Content (Using Default Policy)
 - Content created in application (Using Knowledge - Author Policy)

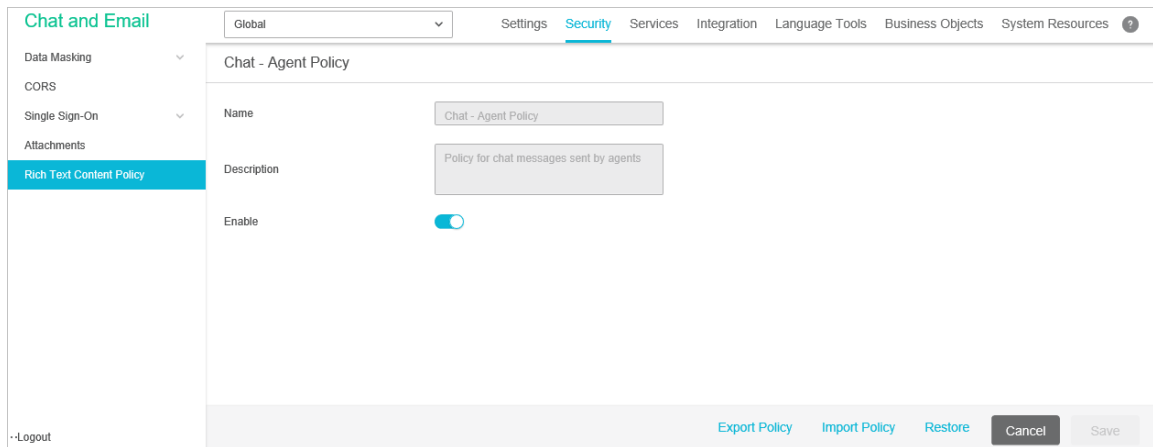
Content policies can be adjusted to only allow the use plain text as well. To learn how, see [“Using a Plain Text Policy”](#) on page 119.

Enabling and Disabling Rich Text Content Policies

To enable or disable rich text content policies:

1. In the partition-level Top menu, click the **Security** option.

2. In the Left menu, click on **Rich Text Content Policy**.
3. In the Rich Text Content Policy space, select one of the content policies.
4. In the content policy space you have selected, set the **Enable** toggle to enable or disable the policy.



Enable a rich text content policy

5. Click the **Save** button.

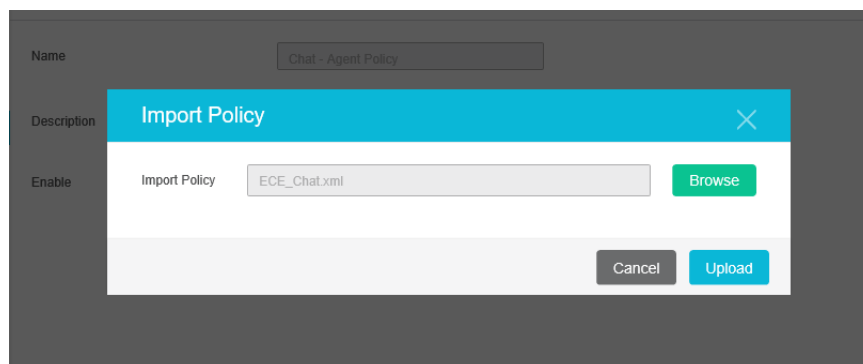
Exporting and Importing Rich Text Content Policies

If you wish to adjust the rich text policies and configure the XML files to suit your needs, you need to export the existing policies, adjust the files, and then import them back into the system.

To export and import rich text content policies:

1. In the partition-level Top menu, click the **Security** option.
2. In the Left menu, navigate to **Rich Text Content Policy**.
3. In the Rich Text Content Policy space, select one of the content policies.
4. In the toolbar for the content policy you have selected, click the **Export policy** button.
5. In the Export Policy window, select **Export Policy** and save the XML file to a local directory.
6. Make the desired changes to the policy XML file and save your changes. To learn how to configure the XML file, see [“Configuring the Rich Text Content Policy File” on page 115](#).
7. Return to the Administrator Dashboard and select the **Import Policy** button from the toolbar.

- In the Import Policy window, click the Browse button and locate the exported file, and click the **Upload** button.



Import the edited policy

- Click the **Save** button.

Configuring the Rich Text Content Policy File

The policy XML file has four notable sections:

- ▶ **Common Regular Expressions:** In this section, the regular expressions that can be used in the rest of the policy file are defined between the `<common-regexps>` tags.
- ▶ **Common Attributes:** In this section, the attributes that can be used while specifying the tag-rules are defined between the `<common-attributes>` tags.
- ▶ **Tag Rules:** In this section, the parsing rules that will be used for each tag individually are defined between the `<tag-rules>` tags.
- ▶ **CSS Rules:** In this section, the parsing rules that will be used for each CSS property individually are defined between the `<css-rules>` tags.

Once you have exported the desired policy file from the application to your local directory, you can begin making edits to the XML file.

Adding a Common Regular Expression

To create a common regular expression:

- ▶ Create an alias in the Common Regular Expressions section. For example, to add the common regular expression `(\d)+`, make the following entry:

```
<common-regexps>
<regexp name="number" value="(\d)+"/>
</common-regexps>
```

Here "number" has been used as the alias for the regular expression.

Allowing a New Tag

To allow a new tag:

- ▶ A new tag rule corresponding to this tag must be added in the Tag Rules section. For example, to allow the `` tag, make the following entry:

```
<tag-rules>
<tag name="span" action="validate"/>
</tag-rules>
```

Here, `action="validate"` ensures that the attributes of the tag follow the rules outlined for them.

Allowing a New Attribute for a Tag

To allow a new attribute for a tag:

- ▶ The attribute must be added to the corresponding tag rule in the Tag Rules section. For example, to allow attribute `dir` for the `` tag, make the following entry:

```
<tag name="span" action="validate">
<attribute name="dir"/>
</tag>
```

Adding a Rule for an Attribute Value

There are two ways for adding a rule for an attribute value:

- ▶ Adding a list of literal values
- ▶ Adding a list of regular expressions

To specify both literal values as well as regular expressions for attribute values, you can use a combination of both.

To add a list of literal values:

- ▶ If you want to allow fixed values for an attribute, you need to specify a list of literal values. For example, to allow values `ltr` and `rtl` for attribute `dir` of the `` tag, the following entry is made:

```
<tag name="span" action="validate">
<attribute name="dir" >
<literal-list>
<literal value="ltr"/>
<literal value="rtl"/>
</literal-list>
</attribute>
</tag>
```

To add a list of regular expressions:

- ▶ An example of adding a list of regular expressions is to allow values that are represented by the regular expression, such as `(\d)+(px)` and the common regular expression number, for the attribute width of the tag ``. To do so, the following entry is made:

```
<tag name="img" action="validate">
  <attribute name="width" >
    <regexp-list>
      <regexp value="(\d)+(px)"/>
      <regexp name="number"/>
    </regexp-list>
  </attribute>
</tag>
```

Adding Validation for Attributes

To add validation for attributes:

- ▶ Certain tags and attributes can be blocked by the sanitizer by default and require validation. The following entry is an example of a change that is made in the Common Attributes section to add validation.

```
<attribute name="start">
  <regexp-list>
    <regexp name="number"/>
  </regexp-list>
</attribute>
```

Allowing a New CSS Property

To allow a new CSS property:

- ▶ A new CSS rule corresponding to this property can be added in the CSS Rules section. For example, to allow the CSS property width, the following entry is made:

```
<css-rules>
  <property name="width"/>
</css-rules>
```

Adding a Rule for a CSS Property Value

There are two ways for adding a rule for a CSS property value:

- ▶ Adding a list of literal values
- ▶ Adding a list of regular expressions

To specify both literal values as well as regular expressions for CSS property values, you can use a combination of both.

To add a list of literal values:

- ▶ If you want to allow fixed values for a CSS property, you must specify a list of literal values. For example, to allow values `auto` and `inherit` for the CSS property `width`, the following entry is made:

```
<property name="width">
<literal-list>
<literal value="auto"/>
<literal value="inherit"/>
</literal-list>
</property>
```

To add a list of regular expressions:

- ▶ An example of adding a list of regular expressions is to allow values that are represented by the regular expression `(\d)+(px)` and the common regular expression number for the CSS property `width`, the following entry is made:

```
<property name="width">
<regexp-list>
<regexp value="(\d)+(px)"/>
<regexp name="number"/>
</regexp-list>
</property>
```

Allowing Links in the Source Attribute of an iframe Tag

To allow links in the source attribute of an iframe tag:

- ▶ Make the following entry in the XML file:

```
<tag name="iframe" action="validate">
<attribute name="src">
<regexp-list>
<regexp value="((http(s:|:)?)(//)?((www.)?(externaldomain/)((.)*))"/>
</regexp-list>
</attribute>
</tag>
```

If you wished to allow links from `w3schools`, for instance, simply replace `externaldomain` with `w3schools.com`.

Using a Plain Text Policy

If you wish to ensure that content of your customers, authors, and agents only use plain text, there is a simple change you can make to the policy.

To allow plain text content only:

- ▶ Import a policy file with only the following content:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>

<anti-samy-rules xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:noNamespaceSchemaLocation="antisamy.xsd">

</anti-samy-rules>
```

Restoring Rich Text Content Policies

If you're not satisfied with your changes, you can restore the default policy settings.



Important: Restoring the content policy overwrites any custom policies, so make sure to export any custom policy files before restoring.

To restore rich text content policies:

1. In the partition-level Top menu, click the **Security** option.
2. In the Left menu, navigate to **Rich Text Content Policy**.
3. In the Rich Text Content Policy space, select one of the content policies.
4. In the toolbar for the content policy you have selected, click the **Restore** button.
5. In the window that opens, click **Yes**. This restores to the content policy to the default settings. Note that any changes you have made will be removed.



ECE User Single Sign-On

- ▶ [About Single Sign-On \(SSO\)](#)
- ▶ [Preparing to Configure Single Sign-On](#)
- ▶ [Configuring Single Sign-On for Agents](#)
- ▶ [Configuring SSO for Partition Administrators](#)
- ▶ [Signing in](#)
- ▶ [Troubleshooting](#)

About Single Sign-On (SSO)

Enterprise Chat and Email (ECE) consoles can be accessed outside of Finesse, however, SSO must be enabled to allow agents and supervisors to log in to ECE through Finesse. If Single Sign On needs to be enabled, the following is required:

- ▶ Agent SSO Configuration on ECE. For more information, see [“Configuring Single Sign-On for Agents” on page 123](#).
- ▶ Configuration performed on an Identity Provider, for example, ADFS. For more information, see the *Enterprise Chat and Email Installation Guide*.

Single Sign-On can also be configured for new partition administrators. This ensures that new users who log in to Cisco Administrator’s desktop are granted access to the Enterprise Chat and Email Administration Console. For more information about how to configure single sign-on for partition-level administrators for Enterprise Chat and Email, see [“Configuring SSO for Partition Administrators” on page 125](#).

Preparing to Configure Single Sign-On

There are some important pre-configuration tasks that must be completed before configuring SSO.

Integrating with Packaged CCE

The application must already be properly integrated with Packaged CCE.

- ▶ For more information about integrating with Packaged CCE, see [“Packaged CCE Integration” on page 23](#).

Configuring an Identity Provider

SSO with Cisco IDS requires that an Identity Provider (IdP), has been configured for your ECE system, for example: ADFS. Information specific to the IdP server is required while configuring SSO for Cisco IDS. For more information about how to configure the IdP, see the *Enterprise Chat and Email Installation Guide*.

If you wish configure SSO to allow users with administrator or supervisor roles to sign in to partition 1 of ECE outside of Finesse using their SSO login credentials, the Java Keystore (JKS) certificate should be converted to public key certificate and configured in Relying party trust created on the IdP server for ECE.

To configure public key certificate in the relying party trust:

1. On the Shared or Single IdP server, select the Relying Party Trust you created during the ECE installation.
2. Open the Properties window for the trust.
3. Under the Signature tab, click the **Add...** button and add the public certificate.
4. Click **OK** to close the window.

Importing the SSL Certificate

Before configuring SSO, the Secure Sockets Layer (SSL) certificate of the Cisco IDS server must be imported to the ECE server for Packaged CCE installations. The SSL certificate can be used in “[Configuring Single Sign-On for Agents](#)” on page 123 and in “[Configuring SSO for Partition Administrators](#)” on page 125.

The certificate can be imported to an existing keystore or a new keystore can be created on the ECE server.

To obtain the SSL certificate:

1. On the ECE server, launch Internet Explorer.
2. Access `https://cisco-ids-1:8553` in the browser, where *cisco-ids-1* indicates the Fully Qualified Domain Name (FQDN) of the Primary Cisco IDS server.
3. In the page that appears, click the **Continue to this website (not recommended)** option.
4. In the address bar, click the **Certificate error** notification.
5. In the Untrusted Certificate pop-up, click the **View certificates** option.
6. In the Certificate window that appears, click the **Details** tab.
7. Click the **Copy to File...** button.
8. In the Certificate Export Wizard welcome page, click the **Next** button.
9. On the Export File Format page, select the **DER encoded binary X.509 (.CER)** option. Click **Next**.
10. Specify the path to export the certificate. For example, `C:\ciscoids1.cer`. Click **Next**.
11. Click **Finish**. If a secondary Cisco IDS server is in use, perform these steps for it as well.

To import the SSL certificate:

These steps explain how to import SSL certificate in the default Java Keystore named “cacerts”.

1. Copy the certificate file to the ECE server directory:
`ECE_server\ECE_installation_directory\env\jdk\jre\bin`
2. Open Command prompt on the ECE server and enter the directory where you copied the certificate file.
3. Run following command to import the certificate:
`ECE_server\ECE_installation_directory\env\jdk\jre\security\cacerts Java Keystore keytool -import -alias eg_custom_<alias name> ciscoids -file ciscoids.cer -keystore ..\lib\security\cacerts`



Important: If you have imported the certificate to the default JRE truststore with the “alias name” in the format of `-eg_custom_<alias name>`, the certificate does not need to be imported again.

4. When prompted for the keystore password, type “**changeit**” and press ENTER on your keyboard.
5. When prompted to trust this certificate, type “**Y**” or “**Yes**” and press ENTER on your keyboard.
6. Restart the server.

Configuring Single Sign-On for Agents

Important things to note:

- ▶ The process of configuring a system for single sign-on must be performed in the Security node at the partition level by a partition user with the following necessary actions: View Application Security and Manage Application Security.
- ▶ Single Sign-On configurations here do not apply to partition administrators.
- ▶ A Java Keystore (JKS) certificate is needed to configure SSO to allow users with administrator or supervisor roles to sign in to partition 1 of ECE outside of Finesse using their SSO login credentials. A JKS is installed during the ECE installation process. Ensure that you have imported the relevant certificate into the JKS if you enable SSL. For more information about importing the certificate, see [“Importing the SSL Certificate” on page 122](#).
- ▶ DB server collation for Unified CCE is case-sensitive. The username in the claim returned from the user info endpoint URL and the username in Unified CCE must be same. If they are not the same, single sign-on agents are not recognized as logged in and ECE cannot send agent availability to Unified CCE.
- ▶ Configuring SSO for Cisco IDS affects users who have been configured in Unified CCE for Single Sign-On. Ensure that the users you wish to enable for SSO in ECE are configured for SSO in Unified CCE. Consult your Unified CCE administrator for more information.
- ▶ For supervisors and administrators to log into the consoles other than the Agent Console, once SSO is enabled, you must provide a valid web server or load balancer URL in the partition settings. See [“Web Server URL or Load Balancer URL” on page 49](#) for more information.

To configure SSO for Agents:

1. In the partition-level Top menu, select the **Security** option.
2. In the Left menu, navigate to **Single Sign-On > Configurations**.
3. In the **Select Configuration** dropdown, select **Agent**.
4. In the General tab, set the following:
 - **Enable Single Sign-On:** Select Yes to enable SSO.
 - **Allow local login for specific users:** Select whether users should only be able to log in to the application through the SSO authentication methods, or if they can log in to the application locally as well. Select **Yes** to enable local login, **No** to disable. The type of authentication required of each user can be controlled at the user level.
 - **Single Sign-On Type:** Select the identity provider for single sign-on. By default, this is Cisco IDS.

- **Create/Update user account on login:** This toggle is used for user auto-provisioning. If you are not configuring your system for auto-provisioning, set the toggle to **off**. This is not available for ECE.

The screenshot shows the 'Chat and Email' configuration page. The left sidebar has 'Single Sign-On' selected. The main area shows the 'SSO Configuration' tab for the 'Agent' configuration. The 'Enable Single Sign-On' toggle is turned on. The 'Create or update user account on login' toggle is turned off. Other fields include 'Name' (Agent), 'Description' (Single Sign-On Configuration for agents), and 'Single Sign-On Type' (Cisco IDS).

Enable single sign-on for agents

5. Click the **SSO Configuration** tab. Contact your Unified CCE administrator to acquire the necessary details for the following sections, or refer to [“Preparing to Configure Single Sign-On” on page 121](#) for more details. Provide the following:
 - **Primary User Info Endpoint URL:** The User Info Endpoint URL of the primary Cisco IDS server. This URL validates the user token/User Info API. This value can be provided by the Cisco IDS server management team. It is in format:


```
https://cisco-ids-1:8553/ids/v1/oauth/userinfo
```

 where *cisco-ids-1* indicates the Fully Qualified Domain Name (FQDN) of the Primary Cisco IDS server.
 - **User Identity Claim Name:** The name of the claim returned by the User Info Endpoint URL, which identifies the username in Unified or Packaged CCE. The claim name and the username in Unified or Packaged CCE should match. This is one of the claims obtained in response to the Bearer token validation. This value can be provided by the Cisco IDS server management team.
 - If the username of agents in Unified or Packaged CCE matches the User Principal Name, provide “upn” as the value for User Identity Claim name field.
 - If username of agents in Unified or Packaged CCE matches with the SAM Account Name, provide “sub” as the value for User Identity Claim name field.
 - **Secondary User Info Endpoint URL:** The secondary user Info Endpoint URL of the Cisco IDS server. This value can be provided by the Cisco IDS server management team. It is in format:


```
https://cisco-ids-2:8553/ids/v1/oauth/userinfo
```

 where *cisco-ids-2* indicates the Fully Qualified Domain Name (FQDN) of the Secondary Cisco IDS server.
 - **User Info Endpoint URL Method:** The HTTP method used by ECE for making Bearer token validation calls to the User Info Endpoint URL. Select one of the options:
 - **GET:** Method used to retrieve data from the Cisco IDS server at the specified endpoint.
 - **POST:** Method used to send data to the Cisco IDS server at the specified endpoint.

The option selected here should match the IDS server's method.

- **Access Token Cache Duration (Seconds):** The duration, in seconds, for which a Bearer token should be cached in ECE. Bearer tokens for which validation calls are successful are only stored in caches. (Minimum value: 1; maximum value 30)
- **Allow SSO Login Outside Finesse:** Set this toggle to **on** if you wish to allow users with administrator or supervisor roles to sign in to partition 1 of ECE outside of Finesse using their SSO login credentials. This requires that your IdP configuration allows for a shared IdP server.

The screenshot shows the 'Chat and Email' configuration page in the ECE Admin Web interface. The 'Security' tab is selected, and the 'SSO Configuration' sub-tab is active. The configuration is for the 'Agent' partition. The 'SSO Configuration' section includes the following fields and controls:

- Primary User Info Endpoint URL*:
- User Identity Claim Name*:
- Secondary User Info Endpoint URL:
- User Info Endpoint URL Method:
- Access Token Cache Duration (Seconds):
- Allow SSO Login Outside Finesse:
- Identity Provider:

- SAML Version:
- Entity ID*:
- Identity Provider Certificate*:
- Enable Encrypted Assertion:

At the bottom right of the configuration area, there are 'Cancel' and 'Save' buttons. A 'Logout' link is visible in the bottom left corner.

Provide the necessary details for the SSO configuration

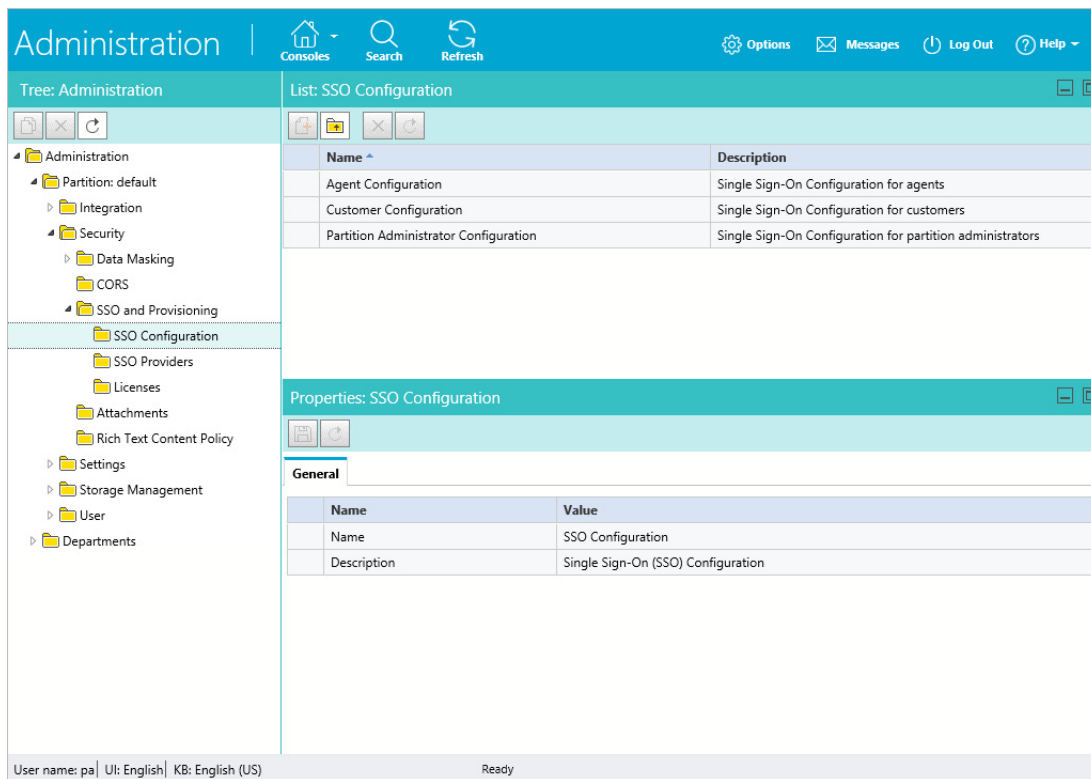
6. Click the **Save** button.
7. In the partition-level Top menu, click the **Settings** option.
8. In the Left menu, navigate to **System > Common**.
9. In the Common Settings space, select the **Web server URL** or **Load Balancer URL** setting to modify. In the field provide the web server or load balancer FQDN. For more information, see [“Web Server URL or Load Balancer URL” on page 49](#) for more information.
10. Click the **Save** button.

Configuring SSO for Partition Administrators

Important things to note:

- ▶ This process is to configure single sign-on for partition administrators that are auto-provisioned in ECE when they access the ECE gadget in the CCE Admin Web interface.

- ▶ This process must be performed in the legacy ECE Administration Console.
- ▶ This is for the ECE gadget accessed within CCE Admin WEB interface For example, `https://IP_Address/cceadmin`.
- ▶ If an LDAP SSL URL (for example, `ldaps://<ldap server>.`) is used in the SSO configuration, then an SSL certificate of the LDAP server needs to be imported to the default truststore of the JDK installation on the ECE server. For more information about importing the certificate, see [“Importing the SSL Certificate” on page 122](#).
- ▶ This should be the same LDAP server where users logging in to CCE Web Admin interface are configured. Make sure that the ECE server can access this LDAP server URL to avoid connectivity issues.



Configure SSO for Partition Administrators in the legacy ECE Administration Console.

To configure SSO for LDAP systems:

1. Sign in to the legacy ECE Administration Console as a partition administrator.
2. In the Tree pane, browse to **Administration > Partition: *partition_Name* > Security > Single Sign On > Configurations**.
3. In the List pane, select **Partition Administrator Configuration**.
4. In the Properties pane, under the SSO Configuration tab, set the following:
 - **LDAP URL:** The URL of the LDAP server. This can be Domain Controller URL (for example, `ldap://LDAP_server:389`) or Global Catalog URL (for example, `ldap://LDAP_server:3268`) of the LDAP server.
 - **DN attribute:** The attribute of the DN that contains the user login name. For example, `userPrincipalName`.

- **Base:** The value specified for Base is used by the application as the search base. Search base is the starting location for search in LDAP directory tree. For example, `DC=mycompany, DC=com`.
This field is optional. It is not required if the LDAP URL is a Global Catalog URL.
- **DN for LDAP search:** Perform one of the following:
 - If your LDAP system does not allow anonymous bind, provide the Distinguished Name (DN) of a user who has search permissions on the LDAP directory tree.
 - If the LDAP server allows anonymous bind, leave this field blank.
- **Password:** Perform one of the following:
 - If your LDAP system does not allow anonymous bind, provide the password of a user who has search permissions on the LDAP directory tree.
 - If the LDAP server allows anonymous bind, leave this field blank.



Important: LDAP enables authentication for users in multiple OUs (Organizational Units). To enable this feature, provide a username for the DN for LDAP Search field and a password.

- **SSL enabled on LDAP:** If SSL is enabled on the LDAP server, set the value to **Yes**. If not, set the value to **No**.
- **Keystore location:** The location of the Java KeyStore (JKS). This must be provided if SSL is enabled.

Properties: Partition Administrator Configuration	
SSO Configuration	
Name	Value
LDAP URL *	ldap://mlab-addc.ciscolab.com:389
DN attribute *	userPrincipalName
Base	CN=Users,DC=ciscolab,DC=com
DN for LDAP search	CN=Administrator,CN=Users,DC=ciscolab,DC=com
Password	*****
SSL enabled on LDAP	No
Keystore location *	

Provide the LDAP configuration details

5. Click the **Save**  button.

Signing in

- ▶ Once SSO has been configured for Cisco IDS, Unified CCE agents configured for SSO in Unified CCE can access the ECE gadget in Finesse without having to input their credentials. They can now simply sign in to Finesse and click the **Enterprise Chat and Email** tab in the Finesse toolbar.

Unified CCE agents who are not configured for SSO in Unified CCE can still access the ECE gadget within Finesse, but need to provide their credentials. Finesse is required for systems on which SSO is not configured for non-SSO agents.

- ▶ If the **Allow SSO login Outside of Finesse** setting is set to **Yes** and, in this example, ADFS is used as the Identity Provider:
 - Users can login with Identity Provider initiated SSO to partition using following URL:
`https://ADFS server FQDN/adfs/ls/idpinitiatedsignon.aspx?loginToRP=Relying Party Trust Identifier in URL encoded format`
 - Users can login with Service Provider initiated (SSO / Non-SSO) to the other consoles by using following URLs:
`http(s)://Load_Balancer_URL/context_root/web/view/platform/common/login/root.jsp?partitionId=1`
`http(s)://Load_Balancer_URL/context_root/web/view/platform/common/login/root.jsp?partitionId=0`

Troubleshooting

When starting the ECE service, if you receive any errors regarding being able to start the Windows service, provide the necessary password again and restart the service.



Customer Single Sign-On

- ▶ [About Customer Single Sign-On](#)
- ▶ [Customer Single Logout](#)
- ▶ [Planning Your Configuration](#)
- ▶ [Customer Single Sign-On Configuration](#)
- ▶ [Configuring Your Website for Secure Chat](#)

About Customer Single Sign-On

Customer single sign-on (SSO) is a feature that allows customers to access secure domains, which they can use to contact and interact with agents without having to enter redundant authentication information. The following types of authentication are available for customer SSO:

- ▶ **Customer 360** is a mobile response template through which website visitors can access contact channels of the application. Configuring single sign-on to use Customer 360 also applies to secure message centers configured in the system. Secure message centers are available for Enterprise Chat and Email when integrated with eGain Solve for Cisco. For more information about secure message centers, see *eGain Solve for Cisco Companion Guide*.
- ▶ **Secure Chat**, also known as **Chat Customer Single Sign-On**, allows chat entry points to transfer customer context information from the company website to the application through SAML. This allows customers who are already recognized on the company website to use a SSO-enabled entry point to chat with a customer without having to provide redundant information. This feature is available for auto-login configuration only. To learn how to enable auto-login for chat, and how to configure entry points for Secure Chat, see *Enterprise Chat and Email Administrator's Guide to Chat and Collaboration Resources*.

Since, customer single sign-on can be utilized in multiple ways on a variety of different web domains, all types of customers with different identity providers may be trying to access those resources. When configuring your system for customer single sign-on, you have the option of configuring the system for multiple identity providers to accommodate for this.

For example, a single portal can provide entry into a chat through different areas of the portal. These can be owned by different vendors, such as a virtual assistance provided by a different vendor. Thus, the application must allow customers to login to chat SSO through multiple identity providers.

Setting up customer single sign-on configurations requires the following be performed:

- ▶ Creating Identity Providers
- ▶ Configuring Customer Single Sign-On

Customer Single Logout



Important: Customer Single Logout is only supported for the Customer 360 type of SSO authentication.

It is a common scenario for customers to be logged in to multiple secure channels at a time. To help make it easier for customers to handle their secure interactions, and to coincide with the capabilities of single sign-on for customers, SAML used for customer single sign-on contains a built-in feature called SAML Single Logout (SLO). This allows customers, who logged in to multiple secure interaction channels (secure messaging center, secure chat, and so on) through single sign-on, to immediately logout of all of the various applications they are currently accessing without having to do it individually. This ensures that, when a customer terminates an online session that was initiated through single sign-on, all other related sessions are terminated at once, ensuring their information remains secure. SLO is initiated from either the Identity Provider (IdP) or any of the involved Service Providers (SP).

Setting up customer single logout configurations requires the following be performed:

- ▶ **Configure Single Logout for the Identity Provider:** This involves providing SLO endpoints exposed by the Enterprise Chat and Email application to the IdP. For more information, see [“Planning Your Configuration” on page 131](#).
- ▶ **Enable and Configure Customer SLO in the Enterprise Chat and Email Application:** This involves turning on single logout services for each provider configured in the application, as well as providing additional details required by these services. For more information, see [“Creating Identity Providers” on page 132](#).

Planning Your Configuration

Before configuring this feature, perform the following:

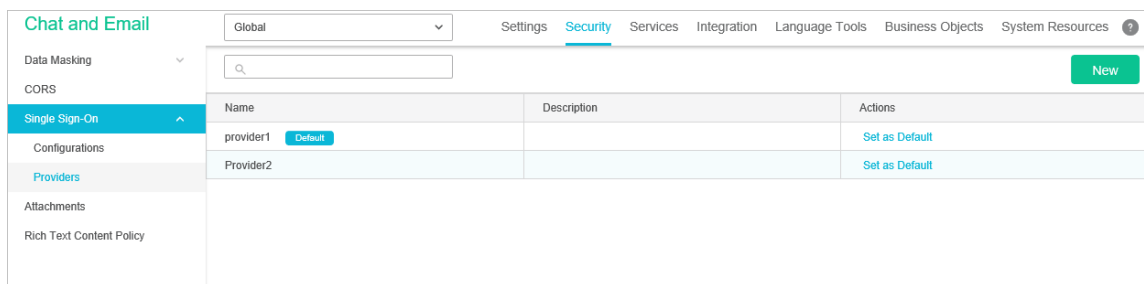
- ▶ Identify the entry points for which you want to enable Secure Chat.
- ▶ Identify the attributes you want to transfer through SAML and configure your identity provider to generate SAML assertion with these attributes.
- ▶ Obtain the SAML configuration details, such as the **Assertion Consumer Service URL** (`https://web_server/context_root/authentication/sso/saml2`), **Entity ID**, and the **Public key certificate** used to validate the SAML assertion. Have these ready when enabling the Chat Customer SSO feature. For information on obtaining these details, consult your IT department.
- ▶ If you are configuring your system for Secure Chat, you must also enable the chat templates to use customer single sign-on. For more information on configuring chat templates for Secure Chat, see *Enterprise Chat and Email Administrator’s Guide to Chat and Collaboration Tools*.
- ▶ If you are configuring SLO for Customer 360, you must provide SLO endpoints to each Identity Provider you want to enable for SLO.
 - To configure IdP initiated SLO, provide the following POST endpoint to IdP:
`https://web_server/context_root/SAML/SSO/customer/logout/request?providerId=ID`.
 - To configure SP initiated SLO, provide the following POST endpoint to IdP:
`https://web_server/context_root/SAML/SSO/customer/logout/response?providerId=ID`.

Note: the `providerId` query parameter is optional. If it is omitted, the service exposed at the specified URL assumes default provider ID configured in Enterprise Chat and Email.

Customer Single Sign-On Configuration

Since, customer single sign-on can be utilized in multiple ways on a variety of different web domains, all types of customers with different identity providers may be trying to access those resources. When configuring your

system for customer single sign-on, you have the option of configuring the system for multiple identity providers to accommodate for this.



Before configuring customer SSO, configure the identity providers

For example, a single portal can provide entry into a Enterprise Chat and Email chat through different areas of the portal. These can be owned by different vendors, such as a virtual assistance provided by a different vendor. Thus, the application must allow customers to login to chat SSO through multiple identity providers.

Setting up customer single sign-on configurations requires the follow be performed:

- ▶ [“Creating Identity Providers” on page 132](#)
- ▶ [“Configuring Customer Single Sign-On” on page 135](#)

Creating Identity Providers


Before configuring customer single sign-on, identity providers must be created and configured in the application. All the identity providers added must use SAML 2.0.


- ▶ Encrypted SAML assertion is supported. If you wish to enable encrypted SAML assertion, you will need a Java Keystore (JKS) file for the decryption certificate.
- ▶ A Java Keystore (JKS) file is necessary if the service provider is enabled to authenticate users in SAML 2.0, as well. Contact your IT to obtain the Java Keystore file.
- ▶ SAML 2.0 provides a well-defined, interoperable metadata format that can be used to expedite the trust process between the Service Provider (SP) and the Identity Provider (IdP). Metadata ensures a secure transaction between an identity provider and a service provider. To enable SAML, a Circle of Trust (COT) between the service provider and identity provider must be established. Consult your IT department about obtaining IdP and SP metadata. Note: SP metadata for customer portals, chat, agent portals, and the agent desktop should be provided separately.
- ▶ SAML is a time sensitive protocol and the IdP determines the time-based validity of a SAML assertion. If the identity provider and the service provider clocks are not synchronized, the assertion becomes invalid and stops the SAML SSO feature. For SAML SSO to operate, you must install the correct Network Time Protocol (NTP) setup and ensure the time for the IdP and SP applications is completely synchronized. Consult your IT department about synchronizing the IdP clock with the SP clock.

To create identity providers:

1. In the partition-level Top menu, select the **Security** option.
2. In the Left menu, browse to **Single Sign-On > Providers**.

3. In the pane, click the **New** button. This opens up a new workspace that is subdivided into the Create SSO Providers space and the RelayState URL Whitelisting space.
4. In the Create SSO Providers space, select the **General** tab and provide the following:
 - **Name:** The name of the identity provider. This field is required.
 - **Description:** A description of the identity provider.
 - **ID:** This field is automatically updated and cannot be changed.
 - **Default:** Select the toggle switch to make this provider the default identity provider for customer single sign-on configurations. Otherwise leave the toggle switch unselected.
 - **Start Page (Absolute URL):** Provide the URL for the page on which web-based customers should land when successfully logging in via single sign-on.
5. In the RelayState URL Whitelisting space, enter information for the following fields:
 - **RelayState URL Whitelisting:** A RelayState URL is an absolute URL of the web page where the user is redirected to after successfully logging in through SSO. RelayState URLs can serve the same purpose as the Start Page URL, however, RelayState URLs take precedence when configured.

Use this optional field to whitelist any RelayState URLs used by the service provider. Click the **Search and Add**  button, then select the desired option from the two choices below:



 - **Allow all RelayState URLs:** Whitelists all RelayState URLs of the service provider.
 - **Allow RelayState(s) that start with the following URL(s):** Click the **Search and Add**  button, provide the URLs in the field below the option, and click **Enter**. Allowed URLs will appear in the Allowed URLs field below.

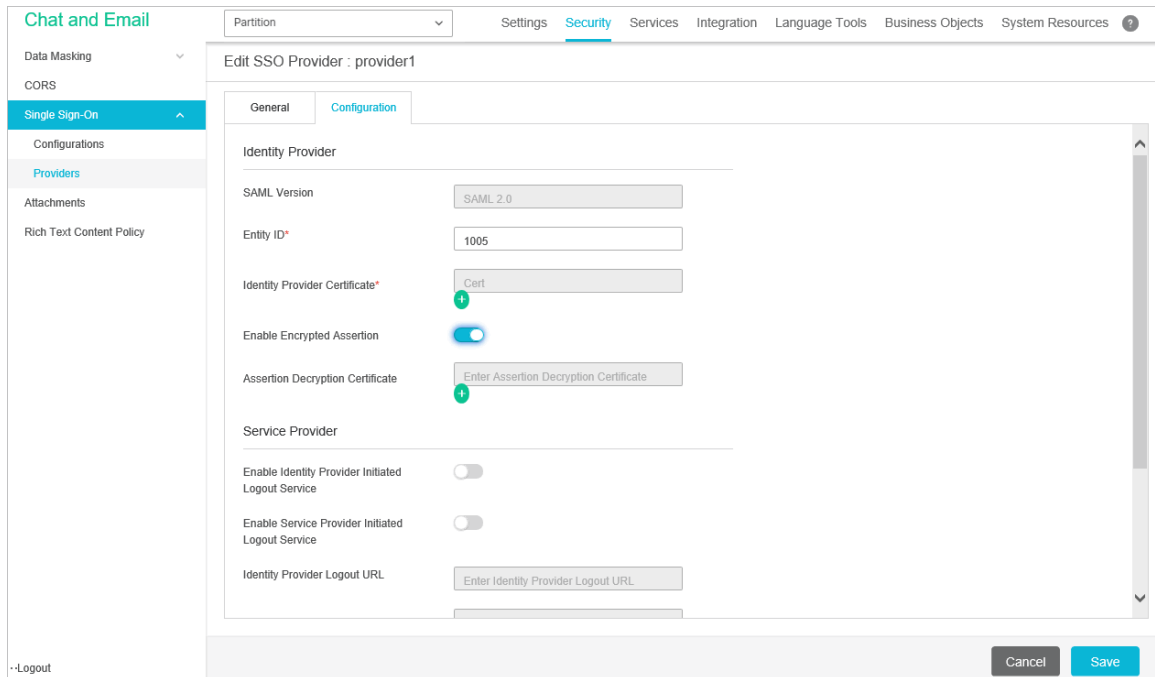
Edit the single sign-on provider general details

6. Click the **Configuration** tab to make the Identity Provider and Service Provider sections appear.

Under the SSO Configuration tab, the Service Provider can be allowed to initiate the authentication for SAML in addition to Identity Provider. For Service Provider initiated authentication, ensure that the partition level setting Web Server URL or Load Balancer URL is correctly configured. For more information, see [“Web Server URL or Load Balancer URL” on page 49](#).

7. Under the Identity Provider section, provide the following:

- **SAML Version:** This is set to SAML 2.0 and cannot be changed.
- **Entity ID:** Entity ID or the issuer. This field is required.
- **Identity provider certificate:** The public key certificate. The certificate must start with “-----BEGIN CERTIFICATE-----” and end with “-----END CERTIFICATE-----”. Click the **Search and Add**  button to open the Identity Provider Certificate popup and enter in the necessary information, then click **Done**.
- **Enable encrypted assertion:** Click the toggle button to enable assertion encryption. The default state sets it to disabled.
- **Assertion decryption certificate:** If **Enable Encrypted Assertion** is enabled, click the **Search and Add**  button and provide the following information in the Assertion Decryption Certificate window:
 - **File Name and Path:** Click the **Browse** button and provide the file name and path of your Java Keystore File. This file is in .jks format and contains the decryption key that the system needs to access files secured by SAML. The file path format looks like this:
`C:\keystore\version_number\SS0\keystore.jks.`
 - **Alias name:** The unique identifier for the decryption key.
 - **Keystore password:** The password required for accessing the Java Keystore File.
 - **Key password:** The password required for accessing the Alias' decryption key.




Configure the identity provider

- Under the Service Provider section, provide the following:
 - **Enable identity provider initiated logout service:** Click the toggle switch to allow the application to accept logout requests from the identity provider (IdP) for one or more sessions of a customer. With this setting enabled, when the customer logs out of the IdP, the IdP notifies the application, which then terminates the user's session in the application. Only requested user sessions are logged out.
 - **Enable service provider initiated logout service:** Click the toggle switch to allow the identity provider to accept logout requests from the application. With this setting enabled, when the user logs out of a channel in the application, a logout request is sent from the application to the IdP. Upon processing this logout request and also logging this user out, the IdP sends a logout response to ECE, which then redirects the user to a logout page.



Important: In default portal and secure message center templates, the logout request is sent to the default provider configured in the application. If a different provider is necessary, the templates should be reconfigured to use the new provider.

- **Identity provider logout URL:** The IdP endpoint URL where the application submits its logout requests and logout responses. This must be provided if the **Enable identity provider initiated logout service** field or **Enable service provider initiate logout service** field is set to **Yes**.
 - **Request signing certificate:** Click the **Search and Add**  button, provide the following information in the next window, and click **Done**.
 - **File Name and Path:** Click the **Browse** button and provide the file name and path of your Java Keystore File. This file is in .jks format and contains the decryption key that the system needs to access files secured by SAML. The file path format looks like this: `C:\keystore\version_number\SS0\keystore.jks`
 - **Alias name:** The unique identifier for the decryption key.
 - **Keystore password:** The password required for accessing the Java Keystore File.
 - **Key password:** The password required for accessing the Alias' decryption key.
 - **Enable service provider initiated authentication:** Click the toggle switch to enable this setting. Enabling this setting enables the **Identity provider login URL** field and the **Entity ID** field.
 - **Entity ID:** Entity ID or the service provider.
 - **Identity provider login URL:** The URL for SAML authentication.
8. Click the **Save** button.


Configuring Customer Single Sign-On

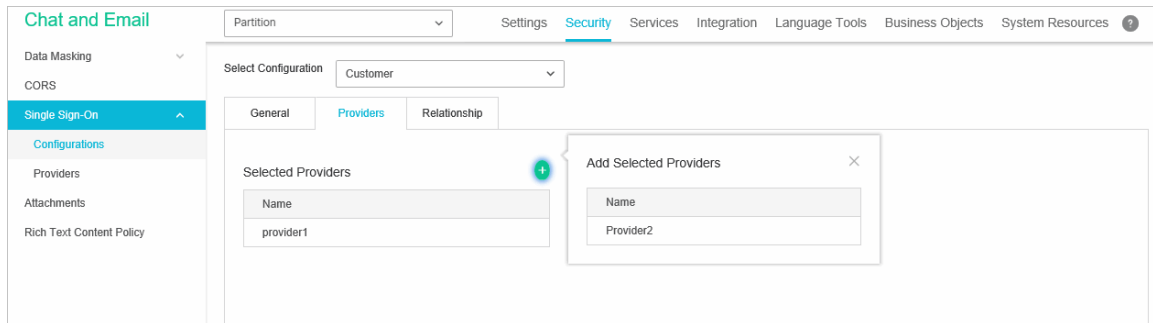
To configure customer single sign-on:

1. In the partition-level Top menu, select the **Security** option.
2. In the Left menu, navigate to **Single Sign-On > Configurations** and select the **General** tab.
3. In the workspace, navigate to the **Enable** dropdown field and set it to one of the following options:
 - **Chat:** Enables customer single sign-on for Secure Chat.

- **Customer 360:** Enables customer single sign-on for Customer 360, which can be used by customers when accessing secure messaging centers.
- **All:** Enables customer single sign-on for both Customer 360 and Secure Chat.

If the configuration is set to **Customer 360** or **All**, service provider initiated authentication can be enabled by clicking the toggle switch next to the **Enable service provider initiated authentication** field . If you want to disable it, leave the field unchecked, as the default state is disabled.

4. Select the Providers tab and click the **Search and Add**  button. Select the identity providers that have been configured for single sign-on from the Add Selected Providers field. For more information about configuring identity providers, see [“Creating Identity Providers” on page 132](#).



Select the providers for the customer single sign-on configuration

5. The Relationships tab displays all entry points in the partition that have been enabled for Secure Chat for reference. For information about configuring entry points, see *Enterprise Chat and Email Administrator’s Guide to Chat and Collaboration Resources*.
6. Click the **Save** button.

Configuring Your Website for Secure Chat

- ▶ Chat templates and entry points need to be configured for chat customer single sign-on. For more information, see *Enterprise Chat and Email Administrator’s Guide to Chat and Collaboration Resources*.



Departments

- ▶ [About Departments](#)
- ▶ [Configuring Activity Transfer Between Departments](#)

About Departments

Departments are created by the administrator. Departments function by allowing teams to focus on particular tasks, divide up organizational resources, and better manage day-to-day operations.

Each department has twelve types of resources available for use, located under the **Business Rules** option in the top menu. Each type of resource has an individual node.

The following business rules are available in departments:

- ▶ Calendars: For more information, see [“Business Calendars” on page 139](#).
- ▶ Chat: For more information, see the *Enterprise Chat and Email Administrator’s Guide to Chat and Email Resources*.
- ▶ Classifications: For more information, see [“Codes and Classifications” on page 146](#).
- ▶ Dictionaries: For more information, see [“Language Options” on page 152](#).
- ▶ Email infrastructure: For more information, see the *Enterprise Chat and Email Administrator’s Guide to Chat and Email Resources*.
- ▶ Data Masking for emails and chat: For more information, see the *Enterprise Chat and Email Administrator’s Guide to Chat and Email Resources*.
- ▶ Macros: For more information, see [“Macros” on page 159](#).
- ▶ Settings: For more information, see [“Settings” on page 44](#).
- ▶ Users: For more information, see [“Users” on page 124](#).
- ▶ Workflows: For more information, see the *Enterprise Chat and Email Administrator’s Guide to Routing and Workflows*.

Configuring Activity Transfer Between Departments

In installations, the application can be configured to allow mapped agents to transfer activities to mapped queues (that belong to the same MRD) in departments other than the department in which they are created.

To configure activity transfer between departments:

- ▶ Enable the **Allow transfer of activities to integrated queues in other departments** setting ([page 60](#)). Mapped agents now see mapped queues (that belong to the same MRD) in their home department and in all foreign departments in the Agent Console.

Business Calendars

- ▶ [About Business Calendars](#)
- ▶ [Managing Shift Labels](#)
- ▶ [Managing Day Labels](#)
- ▶ [Managing Business Calendars](#)
- ▶ [Managing Daylight Saving Changes](#)

About Business Calendars

Calendars are used to map the working hours of the contact center. In a calendar, you set up the working and non-working times of users.

It is not mandatory to set calendars. If not set, the system uses normal hours and considers the agent's work time as 24*7*365. If a calendar is set, all workflows only use business hours; normal hours are not considered for SLAs in workflows. If you set a business calendar in ECE, be sure to adjust your calendars and timezones in Finesse to align with your ECE business calendar.

To configure a calendar, you need to create the following.

- ▶ **Shift labels:** A shift label describes the type of shift, and whether agents work in that shift or not. For example, you can create shift labels like:
 - Morning shift and Evening shift, when agents work.
 - Lunch break, Holidays, and Weekends, when agents do not work.
- ▶ **Day labels:** Day labels define the work time for each shift. Shift labels are used for creating day labels. For example, you can create day labels like:
 - Weekday
 - 8 am to 12 pm: Morning shift
 - 12 pm to 1 pm: Lunch break
 - 1 pm to 5 pm: Evening shift
 - Holiday
 - 12 am to 11.59 pm: Holiday

Use day labels to create calendars.

Managing Shift Labels

Creating Shift Labels

A shift label describes the type of shift, and whether the agents work in that shift or not. For example, morning shift, afternoon shift, lunch break, Christmas holiday, and so on. Once created, shift labels are used in day labels.

To create a shift label:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Business Calendars > Shifts**.
3. In the Shifts space, click the **New** button.
4. In the Create Shift space, provide the following details.
 - **Name:** Type a name for the shift label. Do not use a comma (,) in the name.
 - **Description:** Type a brief description.

- **Agents work this shift:** Specify if agents work in this shift or not by clicking the toggle. By default **Yes** is selected. Select **No** if agents do not work in this shift.

Create and configure a shift label

5. Click the **Save** button.

Deleting Shift Labels

You cannot delete a shift label if it is used in any day label. First, remove the shift label from the day label, where it is used, and then delete the shift label.

To delete a shift label:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Business Calendars > Shifts**.
3. In the Shifts space, hover your mouse over the shift you wish to remove and click the **Delete** button.

Managing Day Labels

Creating Day Labels

In day labels, you can set the work time for each shift. For example, you can divide the 24 hours available in a day into working shifts of eight hours each. Therefore, each day would have three shifts.



Important: Before creating day labels, first create the shift labels.

To create a day label:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Business Calendars > Days**.
3. In the Days space, click the **New** button.
4. In the Create Day space, in the General tab, provide the following details.

- **Name:** Type a name for the day label. Do not use a comma (,) in the name.
 - **Description:** Type a brief description.
 - **Time zone:** It shows the time zone selected for the department. This field is disabled. If you want to change the time zone for your department, you can do it by changing the setting. For details on how to change this setting, see, “[Setting the Time Zone](#)” on page 143.
5. Next, go to the Times tab and provide the following details.
- **Start time:** Select the start time for the day label.
 - **End time:** Select the end time for the day label.
 - **Shift label:** From the dropdown list, select the shift label to be used.

Likewise, specify the start time, end time, and shift labels for the whole day.

The screenshot shows the 'Business Calendars' interface. The 'Days' tab is selected, and the 'Time' sub-tab is active. The 'Add Time' section shows a start time of 09:53:04 am and an end time of 09:53:04 am. Below this, a table lists existing time ranges:

Start Time	End Time	Shift Label
01:02:00 pm	01:10:00 pm	ShiftNameCA08

Configure the time range for the day label

6. Click the **Save** button.

Deleting Day Labels

You cannot delete a day label if it is used in any calendar. First, remove the day label from the calendar, where it is used, and then you can delete it.

To delete a day label:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Business Calendars > Days**.
3. In the Days space, hover your mouse over the day label you wish to remove and click the **Delete** button.

Managing Business Calendars

Setting the Time Zone

Before you create a calendar, determine the time zone when your agents work. Make sure that you select the appropriate time zone in the department setting. If you configure the calendar first, and then change the time zone setting, the start time and end time in the day labels get changed.

For example, you create a day label with the start time as 8 am and end time as 4 pm, and the time zone selected is (GMT -5:00) Eastern Standard Time (US and Canada). After creating a day label, you change the time zone setting to, (GMT -8:00) Pacific Standard Time (US and Canada). The day label start time changes to 5 am, and end time changes to 1 pm and the time zone changes to (GMT -8:00) Pacific Standard Time (US and Canada).



Important: Make sure that you set the time zone first and then configure the calendars.

To change the time zone setting:

1. In the department-level Top menu, select the Apps option.
2. In the Left menu, navigate to **Settings**.
3. In the Common Settings space, navigate to the Business calendar timezone dropdown menu.
4. From the dropdown list, select the desired timezone for your department. For a list of all the available timezone choices, see [“Business Calendar Timezone” on page 51](#).
5. Click the **Save** button.

Creating Business Calendars

You can create business calendars for your department. At a time, only one calendar can be active. You can set calendars for all the days of the week, and the exception days, like holidays, weekends and so on.



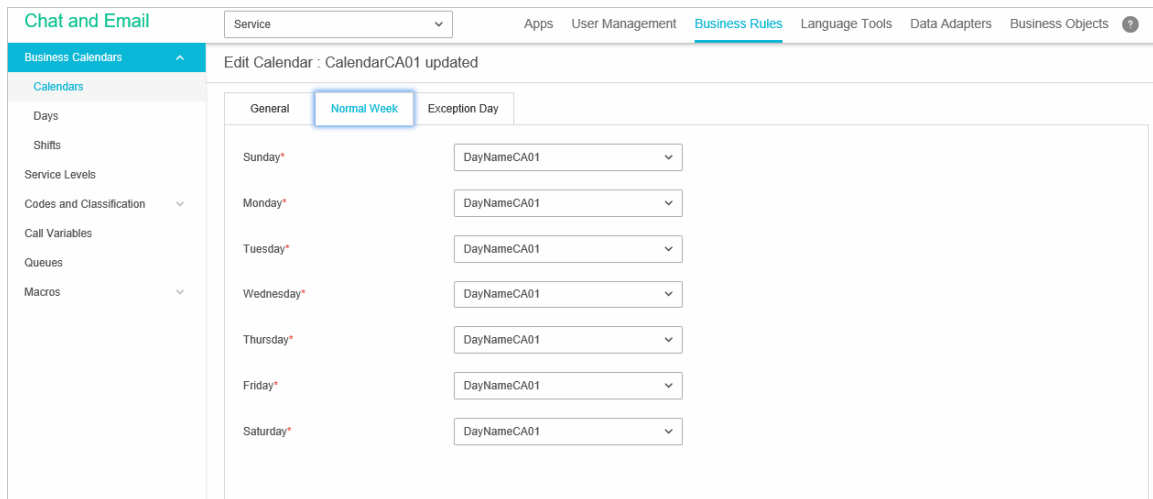
Important: You need to create day labels before creating calendars.

To create a calendar:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Business Calendars > Calendars**.
3. In the Calendars space, click the **New** button.
4. In the Create Calendar space, in the General tab, provide the following details:
 - **Name:** Type a name for the calendar.
 - **Effective start date:** Select the date on which the calendar becomes active. Two calendars in a department cannot have overlapping dates. Also, the start date should be greater than the current date.
 - **Effective end date:** Select the date on which the calendar becomes inactive. Two calendars in a department cannot have overlapping dates. Also, the end date should be greater than the start date.

On the set end date, the calendar becomes inactive. Once a calendar becomes inactive, the system considers the agents work time as 24*7*365, unless some other calendar becomes active automatically.

- **Time Zone:** It shows the time zone selected for the department. This field is disabled. If you want to change the time zone for your department, you can do it by changing the setting. For details on how to change this setting, see, “[Setting the Time Zone](#)” on page 143.
 - **Description:** Type a brief description.
5. Now, go to the Normal Week tab, and select the day label to be used for each day of the week.



The screenshot shows the 'Edit Calendar' interface for 'CalendarCA01'. The 'Normal Week' tab is selected, and the interface displays a list of days from Sunday to Saturday. Each day has a dropdown menu set to 'DayNameCA01'. The 'Normal Week' tab is highlighted in blue.

Set the day labels for each day of the normal week

6. Lastly, go to the Exception Day tab. Specify the day labels to be used for exception days, like holidays, weekends, and so on. Select the date on which there is some exception, and then select the day label to be used for that day and click the **Add Exception Day** button.



Important: The exception dates should be between the start date and end date of the calendar.

7. Click the **Save** button.

Deleting Business Calendars

To delete a calendar:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Business Calendars > Calendars**.
3. In the Calendars space, hover your mouse over the calendar you wish to remove and click the **Delete** button.

Managing Daylight Saving Changes

When changes in the day light saving occur, you need to make the following two changes in calendars.

1. Change the time zone at the department level. To review the process for changing the time zone, see [“Setting the Time Zone” on page 143](#).
2. In the department-level Top menu, click the **Business Rules** option.
3. In the Left menu, navigate to **Business Calendars > Days**.
4. Select a day label.
5. Select the **Time** tab and adjust the start times and end times for all shifts.

11 Codes and Classifications

- ▶ [About Classifications](#)
- ▶ [Managing Categories](#)
- ▶ [Managing Resolution Codes](#)
- ▶ [Managing Not Ready Reason Codes](#)

About Classifications

A classification is a systematic arrangement of resources comprising of different codes meant to track the activity of agents and activities. Classifications are of the following types:

- ▶ Categories
- ▶ Resolution codes
- ▶ Transfer Codes
- ▶ Not Ready Reason Codes

Managing Categories

Categories are keywords or phrases that help you keep track of different types of activities. This section talks about:

- ▶ [Creating Categories on page 147](#)
- ▶ [Deleting Categories on page 148](#)

Creating Categories

Categories and resolution codes can only be nested 3 levels deep.



Important: Up to 500 categories are supported per department.

To create a category:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Codes and Classification > Categories**.
3. In the Categories space, click the **New** button.
4. In the Create Category space, provide the following details.
 - **Name:** Type the name of the category.

- **Description:** Provide a brief description.

The screenshot shows the 'Create Category' form in the 'Business Rules' section of the 'Chat and Email' interface. The form has two fields: 'Name' with the value 'Returns' and 'Description' with the value 'Inquiries about making returns or exchanges of products'. The left sidebar shows a navigation menu with 'Codes and Classification' expanded to 'Categories'.

Create a category

5. Click the **Save** button.
6. If you wish to create sub categories of the category, perform the following:
 - a. Click the **Assistance** button in the Actions column next to the category
 - b. Select the **Add** option.
 - c. In the Create Category space, provide a **Name** and **Description** for the sub-category.
 - d. Once the sub-category has been saved, it appears underneath the parent category. Click the plus and minus icons to expand and contract the view of the parent categories.

Deleting Categories

To delete a category:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Codes and Classification > Categories**.
3. In the Categories space, in the Actions column of the category, click the **Assistance** button.
4. Click the **Delete** option.
5. In the Delete Category pop-up, click **Yes** to confirm the deletion. This deletes the category and any sub-categories contained within.

Managing Resolution Codes

Resolution codes are keywords or phrases that help you keep track of how different activities were fixed. This section talks about:

- ▶ [Creating Resolution Codes on page 149](#)
- ▶ [Deleting Resolution Codes on page 149](#)

Creating Resolution Codes

Resolution codes can only be nested 3 levels deep.

To create a resolution code:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Codes and Classification > Resolution Codes**.
3. In the Resolution Codes space, click the **New** button.
4. In the Create Resolution Code space, provide the following details.
 - **Name:** Type the name of the resolution code.
 - **Description:** Provide a brief description.

The screenshot shows the 'Create Resolution Code' form. The 'Name' field is filled with 'RC01' and the 'Description' field is filled with 'Completion of Activity and conversion to sale'. The left sidebar shows the navigation menu with 'Codes and Classification' expanded and 'Resolution Codes' selected. The top navigation bar includes 'Service', 'Apps', 'User Management', 'Business Rules', 'Language Tools', 'Data Adapters', and 'Business Objects'.

Create a resolution code

5. Click the **Save** button.
6. If you wish to create sub-code of the resolution code, perform the following:
 - a. Click the **Assistance** button in the Actions column next to the resolution code.
 - b. Select the **Add** option.
 - c. In the Create Resolution Code space, provide a Name and Description for the sub-code.
 - d. Once the sub-code has been saved, it appears underneath the parent category. Click the plus and minus icons to expand and contract the view of the parent codes.

Deleting Resolution Codes

To delete a resolution code:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Codes and Classification > Resolution Codes**.
3. In the Resolution Codes space, in the Actions column of the category, click the **Assistance** button.
4. Click the **Delete** option.
5. In the Delete Resolution Code pop-up, click **Yes** to confirm the deletion. This deletes the resolution code and any sub-codes contained within.

Managing Not Ready Reason Codes

To help supervisors and administrators track agent activity, Not Ready Reason codes can be created to provide reasons as to why an agent might become unavailable. These codes can be made mandatory so that agents must select a reason code each time they mark themselves unavailable. Additionally, the system comes with a list of pre-generated, basic Not Ready Reason Codes, which can be deleted if desired.

You can map the Not Ready Reason Codes in ECE with the Not Ready Reason Codes configured in Unified CCE or Packaged CCE.

- ▶ [Creating Not Ready Reason Codes on page 150](#)
- ▶ [Deleting Not Ready Reason Codes on page 151](#)

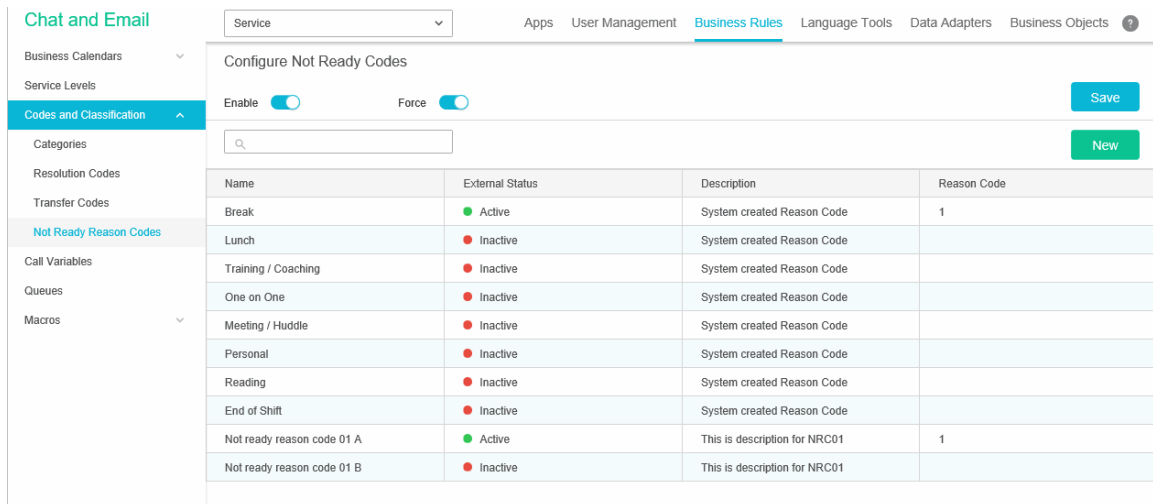
Creating Not Ready Reason Codes

To create a Not Ready Reason code:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Codes and Classification > Not Ready Reason Codes**.
3. In the Configure Not Ready Reason Codes space, click the **New** button.
4. In the Create Not Ready Reason Code space, provide the following details:
 - **Name:** Type the name of the Not Ready Reason Code.
 - **External:** Click the toggle to enable it if you are mapping the reason codes to the codes created in Unified CCE or Packaged CCE.
 - **Description:** Provide a brief description.
 - **Reason Code:** Provide the reason code ID for the code to which you are mapping in Unified CCE or Packaged CCE. For example, if the Reason Code ID for Lunch is 1001 in Unified CCE, set the same ID in the Reason Code field for Lunch.
5. Click the **Save** button.

Enabling and Enforcing Not Ready Reason Codes

Before Not Ready Reason codes can become active and incorporated into the agent’s desktop, they must be enabled. Not Ready Reason codes can also be set to be required for any time agents mark themselves as unavailable.



Enable and enforce not ready reason codes

To enable Not Ready Reason codes:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Codes and Classification > Not Ready Reason Codes**.
3. In the Configure Not Ready Codes space, click the **Enable** toggle.
4. Click the **Save** button.

To enforce Not Ready Reason codes:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Codes and Classification > Not Ready Reason Codes**.
3. In the Configure Not Read Codes space, click the **Force** toggle.
4. Click the **Save** button.

Deleting Not Ready Reason Codes

To delete a not ready reason code:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Codes and Classification > Not Ready Reason Codes**.
3. In the Configure Not Ready Codes space, hover your mouse over the code you wish to remove.
4. Click the **Delete** button.



Language Options

- ▶ [Setting the Language for the User Interface](#)
- ▶ [About Dictionaries](#)
- ▶ [Choosing a Default Dictionary](#)
- ▶ [Creating Dictionaries](#)
- ▶ [Approving and Rejecting Suggested Words](#)
- ▶ [Viewing and Adding Approved Words](#)
- ▶ [Viewing and Adding Blocked Words](#)

Setting the Language for the User Interface

The user interface (UI) is available in the following languages:

- ▶ English
- ▶ French
- ▶ Spanish
- ▶ Italian
- ▶ German
- ▶ Dutch
- ▶ Brazilian Portuguese
- ▶ Portuguese
- ▶ Danish
- ▶ Swedish
- ▶ Russian
- ▶ Canadian French
- ▶ Chinese
- ▶ Japanese
- ▶ Korean

By default the English language is selected. If users need to access the application in more than one language, you can provide a list of languages on the login page for the user to select from.

To set the language for the user interface:

1. In the partition-level Top menu, click the **Language Tools** option.
2. In the Left menu, navigate to **Language**.
3. In the Language space, each language's name is displayed in English under the Language pack header and in its native (non-English) form under the Display name header. For example, “German” is the name of the language pack, while “Deutsch” is the name under which this language option is to displayed to users for selection purposes.

4. Check the boxes next to the languages that you wish to make available to your customers and teams, including the language you want to set as your primary language.

The screenshot shows the 'Language Tools' configuration page. At the top, there are navigation tabs: 'Settings', 'Security', 'Services', 'Integration', 'Language Tools' (selected), 'Business Objects', and 'System Resources'. Below the tabs is a search bar and a table of language packs. The table has three columns: 'Language Pack', 'Display Name', and 'Actions'. The 'English' row is selected, and a blue 'Primary' badge is next to it. The 'Save' button is located at the bottom right of the page.

Language Pack	Display Name	Actions
<input type="checkbox"/> Danish	Dansk	Set Primary
<input type="checkbox"/> German	Deutsch	Set Primary
<input checked="" type="checkbox"/> English Primary	English	Set Primary
<input type="checkbox"/> Spanish	Español	Set Primary
<input type="checkbox"/> Canadian French	Français Canadien	Set Primary
<input checked="" type="checkbox"/> French	Français	Set Primary
<input type="checkbox"/> Italian	Italiano	Set Primary
<input type="checkbox"/> Japanese	Japanese	Set Primary
<input type="checkbox"/> Korean	Korean	Set Primary
<input checked="" type="checkbox"/> Dutch	Nederlands	Set Primary
<input type="checkbox"/> Brazilian Portuguese	Português do Brasil	Set Primary
<input checked="" type="checkbox"/> Portuguese	Português	Set Primary
<input type="checkbox"/> Russian	Русский	Set Primary
<input type="checkbox"/> Swedish	Svenska	Set Primary
<input type="checkbox"/> Chinese	Chinese	Set Primary

Select the languages for the application

5. Under the Actions header, navigate to the row containing your desired primary language and click **Set Primary** to make this your primary language. For example, to set English as your primary language, click **Set Primary** in the row containing the English option. A blue box marked “Primary” then pops up in the Language pack column next to the listed English option, indicating your primary language is now English.
6. Click the **Save** button.

About Dictionaries

Dictionaries refer to a list of words stored in the system for reference. Agents use dictionaries to check spellings in outgoing emails. Each department comes with predefined dictionaries and one of them is configured as the default dictionary. A department can have only one default dictionary and it can be changed according to the business requirements.

Dictionaries are available in the following languages:

1. Danish
2. Dutch
3. English (UK)
4. English (US)
5. Finnish

6. French
7. German
8. Italian
9. Norwegian (Bokmal)
10. Portuguese
11. Brazilian Portuguese
12. Spanish
13. Swedish



Important: The application does not have dictionaries for the following languages: Chinese (Traditional), Chinese (Simplified), Japanese, Korean, Czech, Greek, Norwegian (Nynorsk), and Turkish.

Choosing a Default Dictionary

To choose a default dictionary:

1. In the department-level Top menu, click the **Language Tools** option.
2. In the Left menu, navigate to **Dictionaries**.

Chat and Email Service Apps User Management Business Rules **Language Tools** Data Adapters Business Objects ?

Dictionaries New

Name	Language	Actions
Brazilian Portuguese Dictionary	Portuguese (Brazilian)	Set as Default
Danish Dictionary	Danish	Set as Default
Swedish Dictionary	Swedish	Set as Default
Finnish Dictionary	Finnish	Set as Default
Norwegian (Bokmaal) Dictionary	Norwegian (Bokmal)	Set as Default
Italian Dictionary	Italian	Set as Default
Dutch Dictionary	Dutch	Set as Default
Portuguese Dictionary	Portuguese	Set as Default
French Dictionary	French	Set as Default
Spanish Dictionary	Spanish	Set as Default
German Dictionary	German	Set as Default
English (UK) Dictionary	English (UK)	Set as Default
English (US) Dictionary	English (US)	Set as Default
Dictionary02 updated	Spanish	Set as Default Default
Dictionary03	Spanish	Set as Default
Dictionary04	Spanish	Set as Default

..Logout

Set a default dictionary

3. In the Dictionaries space, click the **Set as Default** option in the actions column corresponding to the desired dictionary to set it as the default dictionary for the department.

Creating Dictionaries

You can also create your own dictionary and store words in it and you can make this as the default dictionary for your department.

To create a new dictionary:

1. In the department-level Top menu, click the **Language Tools** option.
2. In the Left menu, navigate to **Dictionaries**.
3. In the Dictionaries space, click the **New** button.
4. In the Create Dictionary space, on the General tab, provide the following details.
 - **Name:** Provide the name of the dictionary.
 - **Language:** From the drop down list, select a language for the dictionary.
 - **Description:** Provide a brief description.
 - **Default:** Select **Yes** to make this the default dictionary of the department.
5. Click the **Save** button.

Approving and Rejecting Suggested Words

While using the spell-checker users can suggest words that can be added to the dictionary. As an administrator, you can review the list of suggested words and can add these words to the dictionary. If the same word is added in the blocked and approved list, then the word is considered as a blocked word.

To approve or reject suggested words:

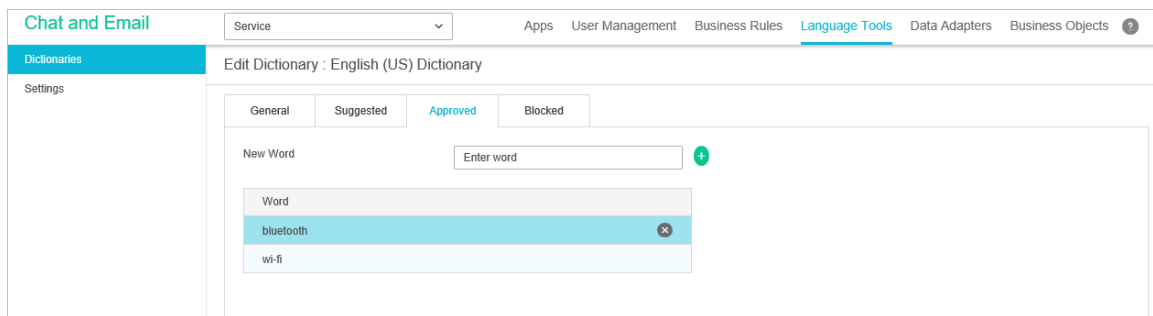
1. In the department-level Top menu, click the **Language Tools** option.
2. In the Left menu, navigate to **Dictionaries**.
3. In the Dictionaries space, select a dictionary to edit.
4. In the Edit Dictionary space, on the Suggested tab, view the list of suggested words. To approve a word, select the word, and click the **Approve** button. To delete a suggested word, select the word and click the **Reject** button.
5. Click the **Save** button.

Viewing and Adding Approved Words

You can create a list of approved words that users should be allowed to use in emails, chats, portal searches and so on without being flagged by the spell checker or any auto-corrected search tools. This can be extremely important when creating a portal to use terms that are common to a company's product to make sure a user's experience is a positive one. For example, Bluetooth and Wi-Fi are common words that should be added to the dictionary if dealing with phones, in addition to the more brand specific words like the name of a product or company.

To view and add approved words to a dictionary:

1. In the department-level Top menu, click the **Language Tools** option.
2. In the Left menu, navigate to **Dictionaries**.
3. In the Dictionaries space, select a dictionary to edit.
4. In the Edit Dictionary space, on the Approved tab, view the list of approved words. Add to the list of approved words by typing in the word to the New Word field and clicking the **Add** button. If you want to delete an approved word, select the word and click the **Delete** button.



Add or remove approved words for the dictionary

5. Click the **Save** button.

Viewing and Adding Blocked Words

You can create a list of blocked words that users should not be allowed to use in emails, chats, and so on. Any word that is included in this list is blocked, regardless of whether it is present in the list of approved words. You must remove the word from this list if you wish to allow users to use it.

To view and add blocked words to a dictionary:

1. In the department-level Top menu, click the **Language Tools** option.
2. In the Left menu, navigate to **Dictionaries**.
3. In the dictionaries space, select a dictionary to edit.

4. In the Edit Dictionary space, select the **Blocked** tab to view the list of blocked words. Add to the list of blocked words by typing in the word to the New Word field and clicking the **Add** button. If you want to delete a blocked word, select the word and click the **Delete** button.
5. Click the **Save** button.

13 Macros

- ▶ [About Macros](#)
- ▶ [Creating Business Object Macros](#)
- ▶ [Creating Combination Macros](#)
- ▶ [Deleting Macros](#)

About Macros

Macros are commands that fetch stored content. They are easy to use, and display the actual content when expanded. Macros enable you to enter a single command to perform a series of frequently performed actions. For example, you can define a macro to contain a greeting for email replies. Instead of typing the greeting each time, you can simply use the macro.

It is important to note that a macro's expansion is contextual to the object, and two macros of similar looking attribute expand differently depending upon the context object. For example, the macros "Email address of the contact point" and "Contact point data of the activity", both return the email address of the customer, but the first one returns the email address saved in the customer profile and the second one returns the email address associated with the activity in which the macro is used.

You can create two types of macros:

1. **Business Objects macros:** In Business Objects, you can create macros for several objects, such as Activity data, Customer data, User data, and so on. You must define an attribute to a macro from the list of system provided attributes. Note that you can define only a single attribute for each macro.
2. **Combination macros:** Combination macros allow the creation of macros with multiple descriptions. That is, you can combine multiple macros within a single macro. Multiple macros can be selected from both Business Objects and Combination macro types.

Creating Business Object Macros

To create a business object macro:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Macros > Business Object**.
3. In the Business Object Macro space, click the dropdown menu to select the macro type. Macro types include: **Chat Session Data, Contact Point Data, Postal Address Data, Phone Number Data, Email Address Contact Point Data, Web Site Data, Customer Data, Contact Person Data, Case Data, Activity Data, Generic Activity Data, User Data.**

Name	Description
activity_id	Unique id number of the activity
activity_type	Activity of the activity
activity_assigned_to	Unique id number of the user working on the activity
contact_point_data	Contact point data of the activity
activity_subject	Subject of the activity


Select a macro type

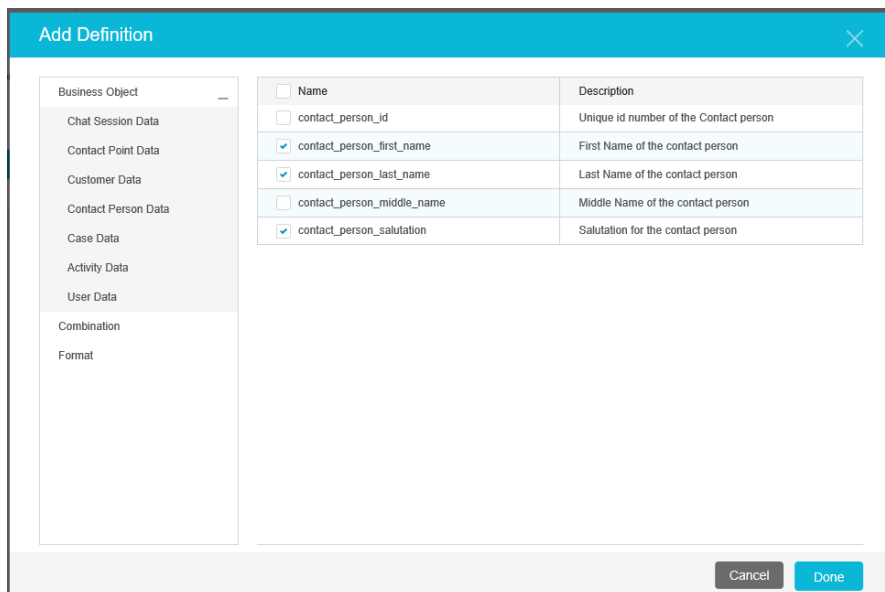
4. Click the **New** button.
5. In the Create Business Object space, provide the following details.

- **Name:** Type a name for the macro.
 - **Definition:** Click the dropdown menu and select the attribute that defines this macro. Please note that for any date attributes (for example, case creation date) are displayed in the GMT timezone.
 - **Description:** Provide a brief description.
 - **Default value:** Provide the default value for the macro.
6. Click the **Save** button.

Creating Combination Macros

To create a combination macro:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Macros > Combination**.
3. In the Combination space, click the **New** button.
4. In the Create Combination space, provide the following:
 - **Name:** Type the name of the macro.
 - **Description:** Provide a brief description.
 - **Default value:** Provide the default value for the macro.
 - **Definition:** Click the **Search and Add**  button and from the Add Definition window, select the attributes that define this macro.



Provide the definition for the macro combination

5. Click the **Save** button.

Deleting Macros



Important: Macros used in workflows cannot be deleted.

To delete a macro:

1. In the department-level Top menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Macros > Business Object** or **Macros > Combination**.
3. Mouse over any macros in the workspace you wish to delete and click the **Delete** button.

Business Objects

- ▶ [Activity Object Attributes](#)
- ▶ [Default Attributes](#)
- ▶ [Custom Attributes](#)
- ▶ [Adding Attributes to Screens](#)

Activity Object Attributes

Every activity that is created in the application when a customer contacts a support center has a substantial amount of information immediately tied to it upon creation. For example, Activity ID, Case ID, Type, status, Creation Date, Due Date, Priority, and so on. Depending on the needs of your contact center, some activity information is more valuable to agents than others. You can customize the business objects by adding custom attributes. You can add custom attributes to the following business objects.

- ▶ **Activity Object Data:** The custom attributes automatically becomes available for: Activity search data, Generic activity data.
- ▶ **Contact Person Data:** The custom attributes automatically becomes available for: Contact person search data.
- ▶ **Customer Object Data:** The custom attributes automatically becomes available for: Customer search data, Change customer data, Corporate customer data, Group customer data, Individual customer data.

Default Attributes

As an administrator, you can determine which default attributes are pertinent enough for agents to be able to view, search, or edit.

To set the permissions of default activity object attributes:

1. In the partition-level Top menu, click the **Business Objects** option.
2. In the Left menu, navigate to one of the following:
 - **Activity Object Attributes**
 - **Contact Person Attributes**
 - **Customer Object Attributes**
3. Under the Default Attributes tab, click the following check boxes next to the attribute you wish to modify:
 - **View:** Enable view permissions to make this attribute visible in the Agent Console. Disabling view permissions hides the attribute.
 - **Search:** Enable search permissions to make this attribute searchable. If enabled, an agent can use this attribute as a search term when conducting an activity search.

- **Edit:** Enable edit permissions to make this an attribute that an agent can modify in the Agent Console.

Name	<input type="checkbox"/> View	<input type="checkbox"/> Search	<input type="checkbox"/> Edit
Activity ID	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Case ID	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Department ID	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mode	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Type	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Subtype	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Status	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Substatus	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Priority	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Created on	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Created by	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Modified on	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Due on	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Last handled by	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Assigned to	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Set the permissions for the default attributes

4. Click the **Save** button.

Custom Attributes



Important: Once you create a custom attribute it cannot be deleted and its properties cannot be changed.

To add a custom attribute:

1. In the partition-level Top menu, click the **Business Objects** option.
2. In the Left menu, navigate to one of the following:
 - **Activity Object Attributes**
 - **Contact Person Attributes**
 - **Customer Object Attributes**
3. In the Attributes space, click the **Custom Attributes** tab.
4. Click the **New** button.
5. In the Create Attribute window, provide the following:
 - **Name:** Type a name for the custom attribute. The following characters are not allowed in the name: ~ ! @ # \$ % ^ & * () _ - + ? > < { } | [] = \ / , .(dot) : ; “ ” ‘ ’. Also, the name cannot start with a digit.

- **Internal Name:** Type a name for the custom attribute to identify it within the application. This name is internal only and does not appear in external-facing resources, such as chat transcripts sent to customers.
- **Data Type:** Select the type of data for the custom attribute. The options available are String and Integer.
- **Analytics:** This feature is not available for ECE at this time. Do not enable Analytics for custom attributes without first consulting your Cisco Administrator.

Provide the basic details for the attribute

6. Click the **Next** button.
7. The window refreshes to display the definition for the attribute. For integer data type, the data size nine is specified and it can't be changed. You can provide a default value for this field. Provide the following:
 - **Data size:** You can specify the maximum characters the custom attribute can have. The default value is eight. You can give a value between one and 4000. For example, if you give a value 10, then you cannot enter data exceeding 10 characters, in the custom field.
 - **String type:** This option gives you the flexibility to define how the data can be entered in the custom field. You have two options available:
 - **User specified in a text box:** You can provide an empty field where the user can type any data. You can also give a default value for the field.
 - **User-selected in the list of choice below:** Provide a list of possible values, from which the user can select one, by using the following options and clicking the **Add** button.
 - **Internal value:** Provide the internal name of the value.
 - **Display value:** Provide the common display name of the value.
 - **Selected by default:** Click this toggle to make the value select by default.

- **Allow multiple selections from the list:** Click this toggle to allow the string to use multiple selections from the list of values.

Create Attribute

Basics > Definition

Data size*

String type

User specified in a text box

Default Value

User selected in the list of choices below

Internal value Display value Selected by default

Internal value	Display value	Selected by default	Order
int3	customer level	<input type="checkbox"/>	<input type="text" value="1"/>

Allow multiple selections from the list

Provide the definition for the attribute

8. If you chose the Integer data type for the attribute, click the **Finish** button to create the attribute. If you chose to create a String type attribute, click the **Next** button.
9. The window refreshes to show translation options for the attribute. Here, you can set the display names and definitions for the attribute in the different languages that are enabled for the partition.

In the Basics section, perform the following:

- Click the **Define display name of attribute in other languages** toggle.
- Enter a name into the field under the Display value column in relation to the desired language.

If you click the **User selected in the list of choices below** option when selecting the string type for the attribute's definition, the Definition section is available. In the Definition section, perform the following:

- Click the **Define display name of choices in other languages** toggle.
- Select a value from the **Choose list item** dropdown.
- Enter a name into the field under the Display value column in relation to the desired language.

10. Click the **Finish** button.
11. The new attribute is listed under the Custom Attributes tab. In the table, you can modify the following fields:
 - **View:** Click the checkbox to make this attribute viewable in the application.
 - **Search:** Click the checkbox to make this attribute searchable in the application.
 - **Edit:** Click the checkbox to make this attribute editable in the application.
 - **Encrypt:** Click the checkbox to encrypt the attribute.
 - **Analytics:** This feature is not available for ECE at this time. Do not enable Analytics for custom attributes without consulting your Cisco Administrator.

- **Actions:** Click the Assistance button in the field and select the **Edit** option to edit the details of the attribute.
12. Click the **Save** button to save the attribute.


Adding Attributes to Screens

After creating the custom attributes make sure you add them to the screens where you want them to show in the system. You can specify which attribute you want to show in the screens and the order in which they should appear for each department. Each screen has a number of attributes that cannot be removed.

For each department, you can customize the following screens:

- ▶ Agent Console - Information - Chat - Activity Details screen
- ▶ Agent Console - Information - Email Activity Details screen
- ▶ Agent Console - Search - Activity - Advanced screen
- ▶ Agent Console - Search - Activity - Results screen

To customize a screen:

1. In the department-level Top menu, click the **Business Objects** option.
2. In the Left menu, navigate to **Screen Attributes**.
3. Select a screen to edit.
4. In the Edit Screen Attributes space, click the **Search and Add**  button and select attributes to add to the screen.
5. In the attributes section, click the toggles in the Displayable column to set which attributes are displayed on the screen.

- In the Order column, enter the number to represent its placement in order of attributes on the screen.

The screenshot shows the 'Edit Screen Attributes' interface for the 'Agent Console - Information - Chat - Activity Details screen'. The interface includes a navigation bar with 'Chat and Email' and 'Service' dropdown, and a menu with 'Apps', 'User Management', 'Business Rules', 'Language Tools', 'Data Adapters', and 'Business Objects'. The main area is titled 'Edit Screen Attributes : Agent Console - Information - Chat - Activity Details screen'. It features a table of attributes with toggle switches and order numbers. An 'Add Attributes' dialog is open, listing various attributes.

Attributes		
Department name	<input checked="" type="checkbox"/>	5
Queue name	<input checked="" type="checkbox"/>	6
Created on	<input checked="" type="checkbox"/>	7
Substatus	<input checked="" type="checkbox"/>	8
Web collaboration...	<input checked="" type="checkbox"/>	9
Customer ID	<input type="checkbox"/>	10
Subtype	<input type="checkbox"/>	11
Status	<input type="checkbox"/>	12

Add Attributes

- Displayname
- First name
- Middle name
- Last name
- Mode
- Contact point
- Customer account ID
- Call Time
- Description
- is_authenticated
- Reason for last action

Logout Cancel Save

Add attributes to the screen

- Click the **Save** button.

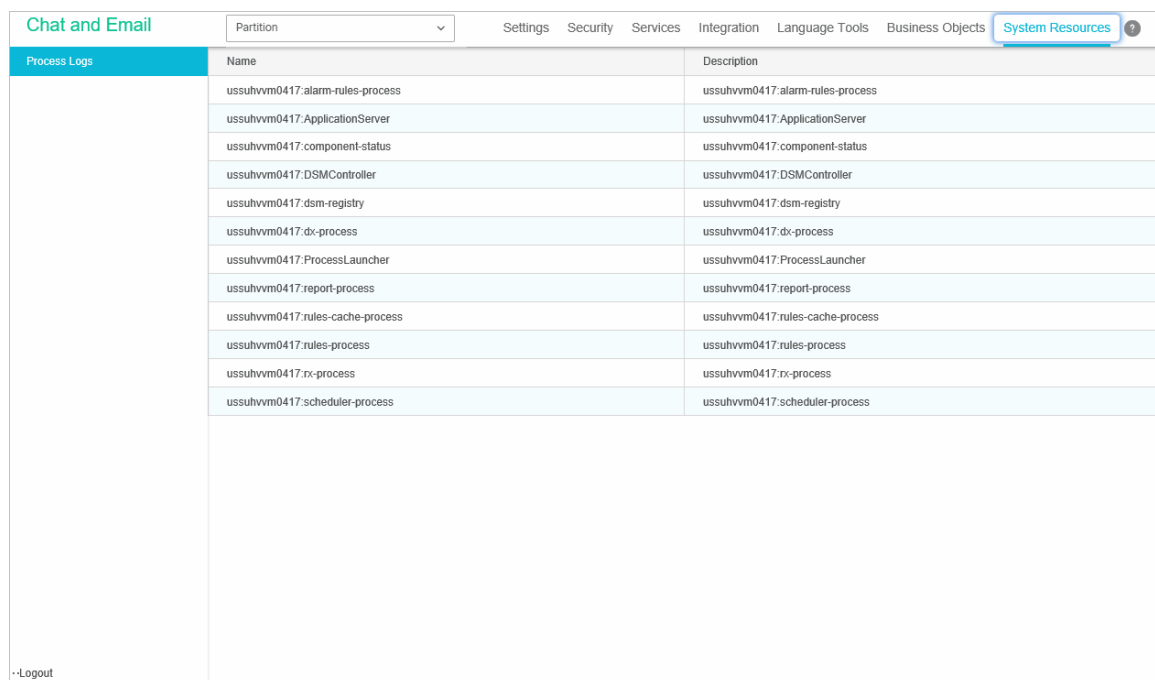
15 Loggers

- ▶ [About Loggers](#)
- ▶ [Managing Logging for Processes](#)

About Loggers

Logging is a mechanism for capturing log messages as they are encountered while the product is running. For all the java processes running in the system, separate log files are created and messages are logged in these individual files. In a single server installation, all the log files are created on the file server. In distributed server installations, log files for the application server, messaging server, and services server are created on each of these servers and not on the file server.

From the UI, you can change the level of logging, and can filter the log messages for a particular user. Also, you can create a group of processes and log all the messages in a single log file to get a comprehensive view of a single functionality, such as a single log file for email, which includes log messages for retriever, dispatcher, and workflow processes.



Chat and Email		Partition	Settings	Security	Services	Integration	Language Tools	Business Objects	System Resources
Process Logs	Name	Description							
	ussuhvmm0417:alarm-rules-process	ussuhvmm0417:alarm-rules-process							
	ussuhvmm0417:ApplicationServer	ussuhvmm0417:ApplicationServer							
	ussuhvmm0417:component-status	ussuhvmm0417:component-status							
	ussuhvmm0417:DSMController	ussuhvmm0417:DSMController							
	ussuhvmm0417:dsm-registry	ussuhvmm0417:dsm-registry							
	ussuhvmm0417:dx-process	ussuhvmm0417:dx-process							
	ussuhvmm0417:ProcessLauncher	ussuhvmm0417:ProcessLauncher							
	ussuhvmm0417:report-process	ussuhvmm0417:report-process							
	ussuhvmm0417:rules-cache-process	ussuhvmm0417:rules-cache-process							
	ussuhvmm0417:rules-process	ussuhvmm0417:rules-process							
	ussuhvmm0417:rx-process	ussuhvmm0417:rx-process							
	ussuhvmm0417:scheduler-process	ussuhvmm0417:scheduler-process							

View the process logs available in the system

Messages are logged at eight trace levels and they are:

- ▶ **1 - Fatal:** This level identifies critical messages. If messages are getting logged at this level, it generally indicates that some major component or functionality of the product is not working.
- ▶ **2 - Error:** This level identifies problems that cause certain actions in the product to fail.
- ▶ **3 - Warn:** This level identifies potential problem conditions in the product that might need attention.
- ▶ **4 - Info:** This level logs information messages that are required to check the sanity of the system.
- ▶ **5 - Perf:** This level is used by performance monitors that run in the product. Any performance related information is captured at this level.
- ▶ **6 - Dbquery:** This level logs database queries that are executed in the product.
- ▶ **7 - Debug:** This level logs messages to identify the complete flow of the code.

- ▶ **8 - Trace:** This log level identifies all the Java methods called during the complete flow of the code. This is the highest level of logging and produces maximum number of log messages.

List of Processes Available in the System

This section provides a list of the processes available in the system. For each process, we list the name of the log file in which it records information.

#	Component	Process name	Log file name
1.	Distributed Services Manager (DSM)	<i>Services_Server_Name</i> : DSMController	eg_log_ <i>Services_Server_Name</i> _DSMController.log
2.	Distributed Services Manager (DSM)	<i>Services_Server_Name</i> : dsm-registry	eg_log_ <i>Services_Server_Name</i> _dsm-registry.log
3.	Application server	<i>Application_Server_Name</i> : Application Server	eg_log_ <i>Application_Server_Name</i> _Application Server.log
4.	Alarm service process	<i>Services_Server_Name</i> : alarm-rules-process	eg_log_ <i>Services_Server_Name</i> _alarm-rules-process.log
5.	Component Status	<i>Server Name</i> : Component status	eg_log_ <i>Server_Name</i> _component-status.log
6.	Dispatcher service process	<i>Services_Server_Name</i> : dx-process	eg_log_ <i>Services_Server_Name</i> _dx-process.log
7.	Process Launcher	<i>Services_Server_Name</i> : ProcessLauncher	eg_log_ <i>Services_Server_Name</i> _ProcessLauncher.log
8.	Report service process	<i>Services_Server_Name</i> : report-process	eg_log_ <i>Services_Server_Name</i> _report-process.log
9.	Workflow Cache service process	<i>Services_Server_Name</i> : rules-cache-process	eg_log_ <i>Services_Server_Name</i> _rules-cache-process.log
10.	Workflow Engine service process	<i>Services_Server_Name</i> : rules-process	eg_log_ <i>Services_Server_Name</i> _rules-process.log
11.	Retriever service process	<i>Services_Server_Name</i> : rx-process	eg_log_ <i>Services_Server_Name</i> _rx-process.log
12.	Scheduler service process	<i>Services_Server_Name</i> : scheduler-process	eg_log_ <i>Services_Server_Name</i> _scheduler-process.log

Managing Logging for Processes

When a Java process is started in the system, an entry is automatically created that displays the logger information for that process such as the log file name, trace level, etc.

The system allows you to change the log trace levels for these process and to create filters to enable logging for specific users. You cannot create new loggers or delete existing ones.



Important: All the changes described in this section take affect immediately. You do not need to restart anything after making these changes.

Viewing Logging Details for Processes

You can view process loggers only if the “View Handler” or “Edit Handler” action is assigned to you.

To view the properties of a process logger:

1. In the partition-level Top menu, click the **System Resources** option.
2. From the list of process logs, select the process log you wish to view
3. In the Edit Process space, under the General tab, you can view the following details:
 - **Name:** The name of the logger.
 - **Description:** The description of the logger.
 - **Maximum trace level:** The maximum level of logging done by the logger. For more details, see [“Changing the Logging Trace Levels for Processes” on page 174.](#)
 - **Log file name:** The name of the log file in which the log messages are recorded.
 - **Maximum File Size:** The maximum size of the log file. The value is set to 5 MB.

The screenshot shows the 'Edit Process' interface for 'ussuhvmm0417:alarm-rules-process'. The 'General' tab is active, displaying the following fields:

- Name:** ussuhvmm0417:alarm-rules-process
- Description:** Enter Description
- Maximum trace level:** 2 - Error
- Log file name:** eg_log_ussuhvmm0417_alarm-rules-proce
- Maximum file size:** 5MB
- Extensive logging duration:** Select Extensive Logging Duration
- Extensive logging end time:** Extensive logging end time

At the bottom right, there are 'Cancel' and 'Save' buttons. A 'Logout' link is visible at the bottom left.

View the general details of a process log

4. Under the Advanced logging tab, you can create a filter to record messages for a particular user, or a session of the user. For details see, [“Enabling Logging for Specific Users” on page 174.](#)

Changing the Logging Trace Levels for Processes

You can edit process loggers only if the “Edit Handler” action is assigned to you.



Important: It is advised that you do not change the trace level until and unless Cisco TAC asks you to do so.

To change the logging trace levels for a process:

1. In the partition-level Top menu, click the **System Resources** option.
 2. From the list of process logs, select the process log you wish to view
 3. In the Edit Process space, under the General tab, change the value in the **Maximum trace level** field. The options available are:
 - **1 - Fatal:** This level identifies critical messages. If messages are getting logged at this, level it generally indicates that some major component or functionality of the product is not working.
 - **2 - Error:** This level identifies problems that cause certain actions in the product to fail.
 - **3 - Warn:** This level identifies potential problem conditions in the product that might need attention.
 - **4 - Info:** This level logs information messages that are required to check the sanity of the system.
 - **5 - Perf:** This level is used by performance monitors that run in the product. Any performance related information is captured at this level.
 - **6 - Dbquery:** This level logs database queries that are executed in the product.
 - **7 - Debug:** This level logs messages to identify the complete flow of the code.
 - **8 - Trace:** This level provides tracing information at the Java API level. This is the highest level of logging and produces maximum number of log messages.
- If Maximum trace level is set to 5-Perf, the messages with trace levels 1 - Fatal, 2 - Error, 3 - Warn, 4 - Info, and 5 - Perf are logged.
4. Click the **Save** button.

Enabling Logging for Specific Users

You can configure a process logger to log messages for a specific user or for a specific session of a user. This lets you troubleshoot issues with a specific user or a particular session of a user. This feature should be used very selectively as when logging is being done for only one user, or only a particular session of a user, the logging for the rest of the users does not happen during that time.

To get started, you need to first get the user ID and HTTP session ID of the user from the database.

- ▶ To get the user ID, run the following query on the active database:

```
Select user_ID from egpl_user where user_name = User_Name
```

Where *User_Name* is the name of the user you want to monitor.

- ▶ To get the HTTP session ID, run the following query on the active database:

```
Select session_ID from egpl_user_session_details
```

```
where user_ID in (select user_ID from egpl_user where user_name = 'User_Name')
```

```
and server_key in (select pkey from egpl_server_status where server_name =  
'Application_Server_Name')
```

Where *User_Name* is the name of the user you want to monitor, and *Application_Server_Name* is the name of the application server from where the user is logged in.

You can edit process loggers only if the “Edit Handler” action is assigned to you.

To enable logging for a specific user:

1. In the partition-level Top menu, click the **System Resources** option.
2. From the list of process logs, select the process log you wish to view
3. In the Edit Process space, click the **Advanced Logging** tab.

Chat and Email Partition Settings Security Services Integration Language Tools Business Objects System Resources

Process Logs Edit Process : ussuhvwm0417:alarm-rules-process

General Advanced logging

User

Enable advanced logging

User IDs (comma separated)* 4458,2238

Maximum trace level 2 - Error

Log file name Log file name

Maximum log file size (KB) Maximum log file size (KB)

Extensive logging duration Select Extensive Logging Duration

Extensive logging end time Extensive logging end time

User Session

Enable advanced logging

User Session IDs (comma separated)* Enter User Session IDs

Logout Cancel Save

Enable and set the trace level and logging durations

4. Enable and set the following and specify the trace level and extensive logging durations ([page 174](#)):



Important: Package and Class are advanced features and should be used only under the guidance of Cisco TAC.

- **User ID:** Provide the ID of the user for which you want to log messages. Only one user ID can be provided at a time.

Ensure that the values in these fields are correct. If the user ID and HTTP session ID do not match, no logs are created.

5. Click the **Save** button.

After troubleshooting is complete, remove the user ID and session ID from here to reset regular logging for the process.

Storage Management

- ▶ [About Storage Management](#)
- ▶ [Creating Purge Jobs](#)
- ▶ [Deleting Purge Jobs](#)

Storage Management can only be viewed or edited from the legacy Administration Console. You will need Internet Explorer to access the legacy Administration Console. For details about preparing the desktop for doing this task, see the *Enterprise Chat and Email Browser Settings Guide*.

About Storage Management

Use the Storage Management feature to free up hard disk space by purging email attachments from the active database.

About Purge Jobs

A purge job is a process that runs automatically at a scheduled time, and deletes attachments based on the specified criteria (such as, attachments for activities older than 90 days) from the active database. The purge job deletes all the attachments that meet the criteria defined for the job. This includes attachments for completed and open email activities. If you do not want attachments for open activities to be deleted, you can configure the job to abort. In this case, you will have to complete all such activities before the job can run successfully. You can create multiple purge jobs, but two jobs cannot have overlapping schedules. A job runs only when it is in active state.

After you create a job, it runs automatically on the scheduled date and time. You cannot start or stop a job manually.



Important: For purge jobs to work, the Purge service should be running.

What Can You Purge?

You can purge attachments for email activities that are more than 90 days old. Once purged, the attachments are permanently deleted from the system.

Who can Manage Purge Jobs?

Only partition users with the Manage Data Storage action can manage purge jobs. This action is part of the default partition administrator role.

Planning the Schedule of Purge Jobs

When a purge job runs, it puts additional load on the system. To ensure that the productivity of agents is not affected by the purge jobs running on the system, plan the schedule of purge jobs in a way that they do not run at peak business hours.

While scheduling jobs you can specify two things. They are:

- ▶ The days of the week when the job should run.

- ▶ The time of the day when the job should run. Set the job to run between specified start and end time. For example, if your call centre runs 24/7, and has less load from 10 pm to 6 am on Sunday, then you can schedule the archive jobs to run from 10 pm to 6 am, on Sundays.



Two jobs cannot be scheduled for the same or overlapping time. For example, you cannot have a job scheduled from 4 pm to 6pm, and another job scheduled from 5 pm to 7 pm on the same day. However, you can have one job scheduled from 4 pm to 6pm, and another from 6pm to 8pm on the same day.

Where can I View Current Storage Usage?

Partition administrators can view total data store size in use and the amount of space used by email attachments from the **Data Storage** node under **Storage Management**.

Creating Purge Jobs


To create a purge job:

1. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Storage Management > Purge Jobs**.
2. In the List pane toolbar, click the **New**  button.
3. In the Properties pane, on the General tab, set the following:
 - **Name:** Type a name for the job.
 - **Description:** Provide a description for the job.
 - **Active:** Select **Yes** to make the job active.
4. In the Properties pane, on the Options tab, set the following:
 - **Data to purge:** Set the value to **Email attachments**.
 - **Abort purge job if open activities match criteria:** Set this to **Yes** if you want the purge job to abort if any open activities with attachments match the purge criteria. In this case, you will have to complete all such activities before the job can run successfully. If you set the value to **No**, the job will delete the attachments of all completed and open activities. When agents access such activities from the Agent Console, it shows an icon informing the agent that attachments are removed from the activity.
 - **Data older than:** Either specify the number of days or select a specific date.
 - **Number of days:** Specify a number more than 90.
 - **Date:** Select a date. It must be atleast 90 days before the current date.
5. In the Properties pane, on the Schedule tab, set the following:
 - **Select when purge job should run:** Value is set to **Once a week** and cannot be changed.
 - **Day on which job should run:** Select a day of the week. Default value is **Sunday**.
 - **Start time:** Select a start time.
 - **End time:** Select an end time.
 - **Set a duration for this schedule:** Select a start date and end date for the job schedule.
6. Click the **Save**  button.

7. In the Properties pane, from the History tab you can view the history of jobs run. It shows details like when the purge job started and ended, the number of attachments purged by the job, the status of the job (can be running, completed, or failed), and number of retries for the job (in case the job is not able to run successfully in first attempt.) The **Additional Information** field provides useful information in case a job is aborted when the criteria is set to **Abort purge job if open activities match criteria**. It provides details about the departments that have open activities and the number of open activities in each department. Special attention is called to the open activities in the **Default Exception Queue** as this queue generally has activities that are not regularly processed by agents.

Deleting Purge Jobs

To delete a purge job:

1. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Storage Management > Purge Jobs**.
2. In the List pane, select a job.
3. In the List pane toolbar, click the **Delete**  button.