



# **Enterprise Chat and Email Administrator's Guide to Administration Console, Release 12.5(1) ES1**

**For Unified Contact Center Enterprise**

First Published: January, 2020

Last Updated: May, 2021

## **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 to Administration Console: For Unified Contact Center Enterprise. October 3, 2022*

© 2016-2021 Cisco Systems, Inc. All rights reserved.

# Contents

- Preface .....15**
  - About This Guide ..... 16
  - Change History ..... 16
  - Related Documents ..... 17
  - Communications, Services, and Additional Information ..... 17
    - Cisco Bug Search Tool ..... 17
  - Field Alerts and Field Notices ..... 17
  - Documentation Feedback ..... 18
  - Document Conventions ..... 18
  
- Chapter 1: Console Basics .....19**
  - Important Administration Tasks ..... 20
  - Key Terms and Concepts ..... 20
  - Sharing of Business Objects ..... 26
    - System Level ..... 26
      - Administration Console ..... 26
      - System Console ..... 26
    - Partition Level ..... 26
      - Administration Console ..... 26
      - System Console ..... 26
      - Tools Console ..... 27
    - Department Level ..... 27
      - Administration Console ..... 27
      - KB Console ..... 27
      - Reports Console ..... 27
      - Supervision Console ..... 27
      - Tools Console ..... 27
      - Agent Console ..... 28
  - Elements of the User Interface ..... 28

**Chapter 2: Unified CCE Integration.....31**

- About Unified CCE Integration ..... 32
- Configuring ECE for Unified CCE..... 32
- Importing Data ..... 34
  - Importing Media Routing Domains ..... 34
  - Importing Users..... 35
- WebEx Experience Manager Integration ..... 36
  - Converting the Cloud Connect Publisher and Subscriber Certificates ..... 36
  - Installing the Cloud Connect Publisher and Subscriber Certificates on ECE..... 38

**Chapter 3: Settings .....39**

- About Settings..... 41
  - Settings to Configure After Installation ..... 42
    - Mandatory Settings ..... 42
    - Optional Settings..... 42
- Configuring Settings ..... 43
  - Configuring System Partition Settings ..... 43
  - Configuring Business Partition Settings ..... 43
  - Configuring Department Settings ..... 43
- Unified CCE Integration Settings..... 44
  - Agent Availability Settings After Completion of Call ..... 44
    - Mark Agent Ready After Completion of Call ..... 44
    - Event Reason Code to Track Agent State ..... 44
  - Allow Transferring Chats to Agents Who Are Not Available ..... 45
  - Allow Transferring Emails to Agents Who Are Not Available ..... 45
  - Allow Transferring Emails to Agents Who Are Not Logged In..... 45
  - Allow Transfer of Activities to Integrated Queues in Other Departments ..... 45
  - Chat Watchdog Interval ..... 46
    - Web Chat (Seconds) ..... 46
    - Messaging Chat (Minutes) ..... 46
  - Enable Chat Queueing..... 46
  - Maximum Assignment Beyond Concurrent Task Limit ..... 47
  - Maximum Wait Time for Login Response From UCCE (Seconds)..... 47
  - Concurrent Task Limit Mappings by Media..... 47
  - Media Class Names..... 48
  - Proactive Monitoring Refresh Interval (Seconds)..... 48
  - Reason Code for Agent Not Ready..... 49

Starvation Time for Activities . . . . .	49
Popover Display Configuration . . . . .	49
Common Settings . . . . .	50
Installation Name . . . . .	50
Web Server URL or Load Balancer URL . . . . .	50
Date Format . . . . .	50
Date and Time Format . . . . .	51
Security Settings for Cookies . . . . .	52
Secure the Cookies Created by Application for Consoles and Knowledge Portals . . . . .	52
Secure the Cookies Created by Application for Customer Websites . . . . .	52
Proxy Server Settings . . . . .	53
Use Server . . . . .	53
Server Hostname . . . . .	53
Server Port . . . . .	53
Authentication . . . . .	54
Username . . . . .	54
Password . . . . .	54
Logger Settings . . . . .	54
Maximum Backups of Log Files . . . . .	55
Default Size in MB . . . . .	55
Default Log Level . . . . .	55
Encrypt Log Files . . . . .	55
User Account Settings . . . . .	56
Password Complexity Policy . . . . .	56
Login Name Minimum Length . . . . .	56
Login Password Case Sensitive . . . . .	57
Password Life Time . . . . .	57
Password Life Time Unit . . . . .	57
Allow Users to Change Password . . . . .	58
Unsuccessful Attempts Time Frame . . . . .	58
Unsuccessful Attempts Time Unit . . . . .	58
Maximum Number of Unsuccessful Timed Attempts . . . . .	59
Maximum Number of Unsuccessful Attempts . . . . .	59
Maximum Inactivity Time Frame . . . . .	59
Maximum Inactivity Time Unit . . . . .	60
Allow Local Login for Partition Administrators . . . . .	60
User Session Settings . . . . .	60

Inactive Time Out (Minutes).....	60
Session Time Out (Minutes).....	61
Business Calendar Settings.....	61
Business Calendar Timezone.....	61
Customer Information Settings.....	64
Customer Departmentalization.....	64
Incoming Email Settings.....	65
Number of Emails to Retrieve.....	65
Maximum Email Size for Retriever (MB).....	65
Maximum Body Size for Retriever (KB).....	66
Message Note for Large Body.....	66
Action for Large Email.....	66
Outgoing Email Settings.....	67
Maximum Body Size for Dispatcher (KB).....	67
Maximum Email Size for Dispatcher (MB).....	67
To: Address for Notifications From Services.....	68
From: Address for Notifications From Services.....	68
Notification Mails Auto BCC.....	68
Restrict To, Cc, and Bcc Email Address Fields.....	69
Default SMTP Server Settings.....	69
Server type.....	69
Use SMTP.....	69
Server name.....	70
User name (ESMTP).....	70
Password.....	70
Connection type.....	70
Port.....	71
Blocked Attachments Settings.....	71
Email - Criteria for blocking attachments.....	71
Block All Attachments.....	71
Action on Blocked Attachments.....	72
Workflow Settings.....	72
From Email Address for Alarm.....	72
Include Original Message for Auto Acknowledgement.....	73
Auto Response Number.....	73
Auto Response Time.....	73
Set “From” Email Address for Email Activities Transferred Between Departments.....	74

Activity Assignment Settings . . . . .	74
Personalized Activity Assignment Settings . . . . .	74
Personalized Activity Assignment . . . . .	74
Enable Personalized Activity Assignment for Forwarded Emails . . . . .	75
Enable Personalized Activity Assignment Only to Users with Permissions on Queue . . . . .	75
Enable Autopushback . . . . .	76
Autopushback Time (Minutes After Logout) . . . . .	76
Activity Type for Autopushback . . . . .	76
Activities to Pull First . . . . .	77
Maximum Activities to Display for Pull . . . . .	77
Maximum Activities to Pull at a Time . . . . .	77
Monitor Settings . . . . .	78
Common Settings for Monitors . . . . .	78
Refresh Interval (Seconds) . . . . .	78
Number of Activities to be Monitored for Service Level . . . . .	78
Chat - SLA for Response Time (Seconds) . . . . .	78
Chat - Daily Service Level Sample Set Definition . . . . .	79
Chat - Daily Service Level Timezone . . . . .	79
Activity Handling Settings . . . . .	82
Agent Guidance Notifications . . . . .	82
Common Settings for Activities . . . . .	83
Alert Agent When Activity Is Assigned . . . . .	83
Allow Agent to Associate a New Outbound Activity with a Queue . . . . .	83
Send Agent an Email When Activity Is Assigned . . . . .	84
Alert Subject . . . . .	84
Alert Body . . . . .	84
Force Activity Categorization . . . . .	85
Force Resolution Code . . . . .	85
Email Activity Settings . . . . .	85
Include Message Header in Reply . . . . .	85
Add Contact Point on Compose . . . . .	86
Language Detection Threshold (KB) . . . . .	86
Service Chat and Phone Activities at the Same Time . . . . .	86
Service Email and Phone Activities at the Same Time . . . . .	87
Service Email and Chat Activities at the Same Time . . . . .	87
Chat Activity Settings . . . . .	88
Chat - Force Activity Categorization . . . . .	88
Chat - Force Resolution Code . . . . .	88
Inbox Settings . . . . .	88
Common Settings for Inboxes . . . . .	88

Number of Activities Per Page .....	88
Main Inbox Settings .....	89
Inbox Sort Column .....	89
Inbox Sort Order .....	89
Email - Enable Sound Alert. ....	89
Chat Inbox Settings .....	90
Chat - Inbox Sort Column .....	90
Chat - Inbox Sort Order. ....	90
Chat - My Monitor - Activity Refresh Interval (Seconds) .....	90
Spelling and Blocked Words Settings .....	91
Preferred Dictionary of the User .....	91
Auto Spellcheck .....	91
Chat - Auto Spellcheck .....	91
Auto Blockcheck .....	92
Chat - Auto Blockcheck .....	92
Include Original Message Text During Spell Check .....	92
Ignore Words With Only Upper Case Letters .....	93
Ignore Words With a Mixture of Upper and Lower Case Letters .....	93
Ignore Words With Only Numbers or Special Characters .....	93
Ignore Words That Contain Numbers .....	94
Ignore Web Addresses and File Names .....	94
Split Contracted Words .....	94
Search Settings .....	95
Maximum Number of Records to Display for Search .....	95
Maximum Number of Records to Display for NAS Search .....	95
Knowledge Base Settings .....	95
KB Primary Language .....	95
Custom Language Label .....	96
Chat Settings .....	96
Chat Auto-Pushback Settings .....	96
Enable Auto-Pushback of Chats .....	96
Expiry Time for Auto-Pushback for Chats (Minutes) .....	97
Make Agent Unavailable on Auto-Pushback of Chats .....	97
Chat Agent Session Settings .....	97
Chat - Agent Chat Message Maximum Length .....	97
Show Smiley in Agent Chat Toolbar .....	98
Chat - Display Timestamp in Agent Chat Console .....	98
Chat - Display Timestamp in Completed Chat Transcript .....	98
Chat - Disable Typing Area and Page Push Area on Customer Exit .....	98



Chat - Enable Sound Alert . . . . .	99
Chat - Reason for Transfer . . . . .	99
Enable Conversation Stream . . . . .	99
Chat - Agent Availability Buffer Value . . . . .	100
Chat - Agent Availability Check Mechanism . . . . .	100

**Chapter 4: Users.....101**

About Users, Groups, Roles, and Actions . . . . .	102
Users . . . . .	102
User Groups. . . . .	102
User Roles . . . . .	103
Actions . . . . .	104
Permissions . . . . .	104
Important Things to Note About Picking and Pulling Activities . . . . .	105
Important Things to Note About Transferring Emails . . . . .	105
Important Things to Note About Transferring Chats . . . . .	106
What are the Actions Assigned to the Default Roles? . . . . .	108
System Administrator . . . . .	108
Partition Administrator . . . . .	109
Administrator. . . . .	110
Agent . . . . .	112
Agent (Read Only) . . . . .	118
Supervisor . . . . .	119
Supervisor (Read Only). . . . .	121
Managing User Roles . . . . .	122
Creating User Roles . . . . .	122
Creating User Subroles . . . . .	124
Copying User Roles . . . . .	125
Restoring User Roles. . . . .	125
Deleting User Roles and Subroles. . . . .	126
Managing User Groups . . . . .	126
Deleting User Groups . . . . .	127
Managing Users . . . . .	127
Creating System Administrators . . . . .	127
Creating Partition Administrators . . . . .	131
Editing Department Users . . . . .	135
Deleting Users. . . . .	140

**Chapter 5: Data Masking..... 142**

About Data Masking . . . . . 143

About Patterns. . . . . 143

Creating Patterns. . . . . 144

Creating Patterns in XML File. . . . . 146

Exporting Masking Patterns. . . . . 147

Importing Masking Patterns. . . . . 147

Copying Patterns . . . . . 148

Deleting Patterns . . . . . 149

Validating Masking Patterns . . . . . 149

    Validating Individual Patterns. . . . . 149

    Validating Masking Patterns Applied to Channels . . . . . 150

Applying Patterns to Chat Channel. . . . . 151

    At the Partition Level . . . . . 151

        What can the partition administrator do? . . . . . 151

    At the Department Level. . . . . 153

        How much control do department administrators get? . . . . . 154

Applying Patterns to Email Channel. . . . . 155

    At the Partition Level . . . . . 155

        What can the partition administrator do? . . . . . 155

    At the Department Level. . . . . 157

        How much control do department administrators get? . . . . . 158

Masking Content of Completed Activities . . . . . 159

**Chapter 6: Cross-Origin Resource Sharing..... 161**

About Cross-Origin Resource Sharing . . . . . 162

Enabling Cross-Origin Resource Sharing. . . . . 162

**Chapter 7: Agent Single Sign-On..... 164**

About Single Sign-On (SSO) . . . . . 165

Preparing to Configure Single Sign-On in ECE. . . . . 165

    Integrating with Unified CCE. . . . . 165

    Configuring an Identity Provider . . . . . 166

    Generating and Importing a Java Keystore Certificate . . . . . 166

Generating a Java Keystore File . . . . .	166
Generating a Certificate with a Java Keystore File . . . . .	167
Importing a Java Keystore Certificate . . . . .	168
Importing the SSL Certificate . . . . .	168
Configuring Agent Single Sign-On (SSO) . . . . .	169
Configuring SSO for Partition Administrators . . . . .	174
Signing in . . . . .	176
Troubleshooting . . . . .	177
<b>Chapter 8: Customer Single Sign-On . . . . .</b>	<b>178</b>
About Customer Single Sign-On . . . . .	179
Customer Single Logout . . . . .	179
Planning Your Configuration . . . . .	180
Customer Single Sign-On Configuration . . . . .	180
Creating Identity Providers . . . . .	181
Configuring Customer Single Sign-On . . . . .	185
Configuring Your Website for Secure Chat . . . . .	186
Troubleshooting . . . . .	186
<b>Chapter 9: Attachments . . . . .</b>	<b>188</b>
About File Attachments . . . . .	189
Blocking Attachment File Types . . . . .	189
Allowing Attachment File Types . . . . .	190
Enabling Chat Attachments . . . . .	191
<b>Chapter 10: Rich Text Content Policies . . . . .</b>	<b>192</b>
About Rich Text Content Policies . . . . .	193
Enabling and Disabling Rich Text Content Policies . . . . .	194
Exporting and Importing Rich Text Content Policies . . . . .	195
Configuring the Rich Text Content Policy File . . . . .	195
Adding a Common Regular Expression . . . . .	195
Allowing a New Tag . . . . .	196
Allowing a New Attribute for a Tag . . . . .	196

Adding a Rule for an Attribute Value . . . . .	196
Adding Validation for Attributes . . . . .	197
Allowing a New CSS Property . . . . .	197
Adding a Rule for a CSS Property Value . . . . .	198
Allowing Links in the Source Attribute of an iframe Tag . . . . .	198
Using a Plain Text Policy . . . . .	199
Restoring Rich Text Content Policies . . . . .	199
<b>Chapter 11: Blocked Visitors</b> . . . . .	<b>201</b>
About Blocked Visitors . . . . .	202
Configuring Blocked Visitor Settings . . . . .	202
<b>Chapter 12: Departments</b> . . . . .	<b>203</b>
About Departments . . . . .	204
Creating Departments . . . . .	205
Configuring Activity Transfer Between Departments . . . . .	206
Copying Departments . . . . .	206
<b>Chapter 13: Business Calendars</b> . . . . .	<b>209</b>
About Business Calendars . . . . .	210
Managing Shift Labels . . . . .	211
Creating Shift Labels . . . . .	211
Deleting Shift Labels . . . . .	211
Managing Day Labels . . . . .	212
Creating Day Labels . . . . .	212
Deleting Day Labels . . . . .	213
Managing Business Calendars . . . . .	213
Setting the Time Zone . . . . .	213
Creating Business Calendars . . . . .	214
Deleting Business Calendars . . . . .	215
Managing Daylight Saving Changes . . . . .	216
<b>Chapter 14: Classifications</b> . . . . .	<b>217</b>
About Classifications . . . . .	218

Managing Transfer Codes . . . . .	218
Creating Transfer Codes . . . . .	218
Deleting Transfer Codes . . . . .	219
Managing Not Ready Codes . . . . .	219
Creating Not Ready Codes . . . . .	219
Deleting Not Ready Codes . . . . .	221
Managing Categories . . . . .	221
Creating Categories . . . . .	221
Deleting Categories . . . . .	222
Managing Resolution Codes . . . . .	222
Creating Resolution Codes . . . . .	222
Deleting Resolution Codes . . . . .	223
<b>Chapter 15: Dictionaries</b> .....	<b>224</b>
About Dictionaries . . . . .	225
Choosing a Default Dictionary . . . . .	225
Creating Dictionaries . . . . .	226
Adding Blocked Words . . . . .	227
Approving Suggested Words . . . . .	227
Viewing Approved Words . . . . .	227
<b>Chapter 16: Macros</b> .....	<b>228</b>
About Macros . . . . .	229
Creating Business Object Macros . . . . .	229
Creating Combination Macros . . . . .	230
Deleting Macros . . . . .	231
<b>Chapter 17: Storage Management</b> .....	<b>232</b>
About Storage Management . . . . .	233
About Purge Jobs . . . . .	233
What Can You Purge? . . . . .	233
Who can Manage Purge Jobs? . . . . .	233
Planning the Schedule of Purge Jobs . . . . .	233
Where can I View Current Storage Usage? . . . . .	234

Creating Purge Jobs .....	234
Deleting Purge Jobs .....	235

# 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 to Administration Console* introduces you to the Administration Console 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
<b>Update of Document</b>		December 2021
Removed invalid Direct Reports references regarding user management chapter	<a href="#">“Users” on page 101</a>	
<b>Update of Document</b>		May 2021
Note added about single sign-on configuration allowing for more SAML identity providers	<a href="#">“About Single Sign-On (SSO)” on page 165</a>	
Update important message about picking, pulling, transferring activities.	<a href="#">“Important Things to Note About Transferring Emails” on page 105</a>	
<b>Update of Document for Release 12.5(1) ES1</b>		July 2020
Updated Screen Name field to include allowed characters	<a href="#">Editing Department Users on page 135</a>	
Updated SSO chapter to remove references to outdated releases	<a href="#">“Agent Single Sign-On” on page 164</a>	
Updated information about configuring partition administrators for SSO	<a href="#">“Configuring SSO for Partition Administrators” on page 174</a>	
Chat Watchdog Interval setting updated to include new product extension settings	<a href="#">“Chat Watchdog Interval” on page 46</a>	
WebEx Experience Manager Integration details added to Unified CCE Integration chapter.	<a href="#">“WebEx Experience Manager Integration” on page 36</a>	



## 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)	<a href="https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/tsd-products-support-series-home.html">https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/tsd-products-support-series-home.html</a>

## 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](http://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](mailto: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.
<b>Bold</b>	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](#)
- ▶ [Elements of the User Interface](#)

The Administration Console is the main management console in the system. It helps managers set up users and resources such as calendars, workflows, and email aliases.

## Important Administration Tasks

---

All business resources are set up and managed in the Administration Console. Some important tasks performed in this console include:

- ▶ Settings for system partition, business partition, and various departments
- ▶ User accounts
- ▶ Business calendars
- ▶ Queues, service levels, and workflows
- ▶ Data masking rules for email and chat
- ▶ Chat infrastructure
- ▶ Email infrastructure
- ▶ Data masking for email and chat
- ▶ Attachments
- ▶ Single Sign-On configuration
- ▶ Data adapters
- ▶ Classifications
- ▶ Dictionaries
- ▶ Macros
- ▶ Secure Messaging

The next section describes each of these concepts in detail.

## Key Terms and Concepts

---

### System and Business Areas

The application has two areas:

- ▶ **System area:** Used by system administrators to set up and manage system resources such as host machines and services. It has two consoles:
  - Administration Console
  - System ConsoleVery few users need access to this area as it is used only for system administration tasks.
- ▶ **Business area:** The main part of the installation, used by business users to perform their tasks. It has all seven consoles:

- Administration Console
- Agent Console
- Knowledge Base Console
- Reports Console
- Supervision Console
- System Console
- Tools Console

## 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 `S e r v i c e` and can be renamed.

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 configure the way 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. Settings are administered in groups. The available groups are:

- ▶ System settings group
- ▶ Partition settings group
- ▶ Department settings group

For more information, see [“Settings” on page 39](#).

## Users

A user is an individual—an administrator, manager, or agent—who has a distinct identification with which they log in to ECE 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 can be created at three levels:

- ▶ System level user: This user is typically the system administrator of the system who manages the system partition resources such as: services, loggers, and so on.
- ▶ Partition level user: This user is typically the system 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.

Two users are created during the installation:

1. **System Administrator:** The first system user, created during installation, is a user called **System Administrator**. Assigned the System Administrator role, this user sets up system resources and creates one or more system-level users.
2. **Partition Administrator:** The first business user, created during installation, is a user called **Partition Administrator**. Assigned the Partition Administrator role, this user manages partition users and settings and creates more partition users as well as one or more department-level users to manage department resources.

For more information, see [“Users” on page 125](#).

## 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 user roles as per the needs of your organization, and assign these roles to your employees. To ease your task, the system comes with some default user roles. You can assign one or more roles to a group of users or an individual user.

For more information, see [“Users” on page 125](#).

## 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 the system partition, business partition, and departments. 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.

For more information, see [“Users” on page 125](#).

## Email Infrastructure

The email infrastructure enables you to configure email addresses to which customers send messages to your company. It also helps you restrict the types of emails or attachments a user is allowed to receive or send.

The following objects can be configured for emails:

- ▶ **Aliases:** Aliases are email addresses that customers use to contact your company—typically something like support@yourcompany.com or sales@yourcompany.com. They function as entry and exit points for emails processed by the system. The Retriever Service monitors the specified aliases and retrieves emails from these aliases when they arrive in the email server. They are used by the inbound workflows to identify which emails to process through the workflows.
- ▶ **Blocked File Extensions:** This is a security feature, which allows you to selectively block certain types of attachments that may contain viruses. You can block attachments of such types from entering the system. (For example, .exe, .vbs, .js, and so on.) Using settings for email attachments, the system can be configured to block all attachments, block incoming and outgoing attachments, and delete or quarantine blocked attachments.
- ▶ **Delivery Exceptions:** This feature allows you to handle bounced back emails. The system includes 144 common delivery exception scenarios. Other exceptions can be created as needed. You can set up different words and phrases for email subjects and email addresses of incoming email. Emails are treated as bounce backs, permanent or temporary, if any of these words or phrases are found in the subject or email address. A permanent bounceback indicates that an irreparable reason (such as invalid email address) caused the email to bounce back. A temporary bounceback indicates that a temporary reason (such as out of office reply, destination server down, and so on.) caused the email to bounce back.

For more information, see *Enterprise Chat and Email Administrator's Guide to Email Resources*

## Chat and Collaboration Infrastructure

Chat and collaboration activities are created when customers click chat help links on your web site. The appearance of these links is configured with the help of templates. Each link is associated with an entry point and each entry point is in turn associated with a queue. A default entry point is provided in each department.

The following objects should be configured for chat and collaboration activities:

- ▶ **Template sets:** The template sets consists of CSS (cascading style sheets) and JSP (JavaServer pages) files that control the look and feel of the chat pane that customers use to type in their messages. The templates are also used to determine what information is requested to identify the customer (for example, name, email address, phone number). You can also compose messages that the customer will see under certain circumstances (for example, if they request a chat session out of hours).
- ▶ **Entry points:** An entry point is the starting point for a customer to initiate a chat interaction. Every chat help link on a web site is mapped to an entry point. Each entry point in turn has a queue associated with it, so that any chat activity created, when the user asks for chat is routed to the queue.

For more information, see *Enterprise Chat and Email Administrator's Guide to Chat and Collaboration Resources*

## Data Masking for Email and Chat

Data masking allows businesses to ensure that sensitive information, like credit card numbers, Social Security Numbers, bank account numbers, and so on, is not transmitted from the system to the customers and vice versa. If the customer and agent do add any sensitive data in the email content and chat messages, all such data is masked before it is displayed to customers and agents and before it is stored in the System.

Data masking is the process of scanning the content for sensitive information and applying regular expressions to mask the sensitive information and hide the original data with characters, like, \* ^ #. Data is masked using patterns, which are defined using Javascript and Java regular expressions.

Data masking is available for emails and chats. For more information, see [“Data Masking” on page 142](#).

## Data Adapters

You may need to access data from external sources, and data links enable you to perform this function. They act like bridges between the application and external data sources. Data can be accessed through various mediums: phone, links, and data adapters.

The following objects should be configured for data adapters:

- ▶ **Data Access Links:** Enables you to create links to fetch data from external or internal sources.
- ▶ **Data Usage Links:** Allows you to define the format in which you want to display the data fetched by the data access links.

For more information, see *Enterprise Chat and Email Administrator's Guide to Data Adapters*.

## Workflows

Workflows allow you to implement business processes by defining and automating the progression of activities based on certain rules. A workflow lists the sequence of rules that are applied on an activity as it moves through the system. There are four types of workflows:

- ▶ Alarm workflows
- ▶ Inbound workflows
- ▶ Outbound workflows

For more information, see *Enterprise Chat and Email Administrator's Guide to Routing and Workflows*

## Queues

Queues hold incoming customer service activities such as emails and chat sessions that are waiting to be assigned to agents. A department can have any number of queues to map their business process. A single queue can hold multiple activity types like email, task, chat and so on. Agent access to queues is controlled by permissions.

For more information, see *Enterprise Chat and Email Administrator's Guide to Routing and Workflows*

## Service Levels

Some customers may be more valuable to your company than others. In order to provide good service, agents in your department need to know about the importance of every customer. For this, you can assign service levels to your customers and use them in your workflows. Service levels enable you to define the importance of a particular customer, thereby directing agents to respond immediately to customers with high importance.

For more information, see *Enterprise Chat and Email Administrator's Guide to Routing and Workflows*

## Calendars

You can create a business calendar for your organization. It allows you to set up working and non-working hours and days for employees in your department. To create your business calendar, it is essential that you 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 209](#).

## 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 [“Classifications” on page 217](#).



## 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 13 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 [“Dictionaries” on page 224](#).

## 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 228](#).

## Solve

Solve is a knowledge app that can easily be embedded into the agent desktop to quickly enable Voice, Email and Chat agents with the powerful Knowledge resources. These resources can greatly assist agents in quickly

resolving customer issues and answering questions. Solve is currently available only for systems integrated with eGain Solve for Cisco. For more information, see the *eGain for Solve for Cisco Companion Guide*.

## Sharing of Business Objects

---

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

### System Level

The following objects are common for the entire system and are managed by the system administrators.

#### Administration Console

- ▶ Roles, users, and user groups
- ▶ Settings

#### System Console

- ▶ Service Processes
- ▶ Loggers
- ▶ Hosts

### Partition Level

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

#### Administration Console

- ▶ Roles, users, and user groups
- ▶ Settings: partition and department settings
- ▶ Integration options: integrate with Unified CCE, configure Solve
- ▶ Security settings: data masking rules, CORS, SSO, attachments, rich text content policies
- ▶ Departments: create new or copies of existing departments

#### System Console

- ▶ Service Instances: All departments in an installation use common services that are managed by partition administrators.

## **Tools Console**

- ▶ Login page language setting: Set at partition level and is available to users in all departments.
- ▶ Sections available in the Agent Console: Set at partition level and are available to agents in all departments.
- ▶ New Activity Shortcuts: Set at partition level and are available to agents in all departments.
- ▶ Activity types: Set at partition level and are available to agents in all departments.

## **Department Level**

### **Administration Console**

- ▶ Settings
- ▶ Roles, users, and user groups
- ▶ Business calendars
- ▶ Queues, service levels, and workflows
- ▶ Chat infrastructure
- ▶ Email infrastructure
- ▶ Data masking
- ▶ Classifications
- ▶ Dictionaries
- ▶ Macros

### **KB Console**

- ▶ KB Articles
  - Not shared

### **Reports Console**

- ▶ Not shared

### **Supervision Console**

- ▶ Not shared

### **Tools Console**

- ▶ Not shared

## Agent Console

- ▶ Not shared
- ▶ Exceptions:
  - Customers: If customer departmentalization is not enabled (see [“Customer Departmentalization” on page 64](#)), agents can search and view customers across departments. And, when an agent creates an activity for a customer that already exists in another department, they will see the complete history of the customer (all cases and activities).

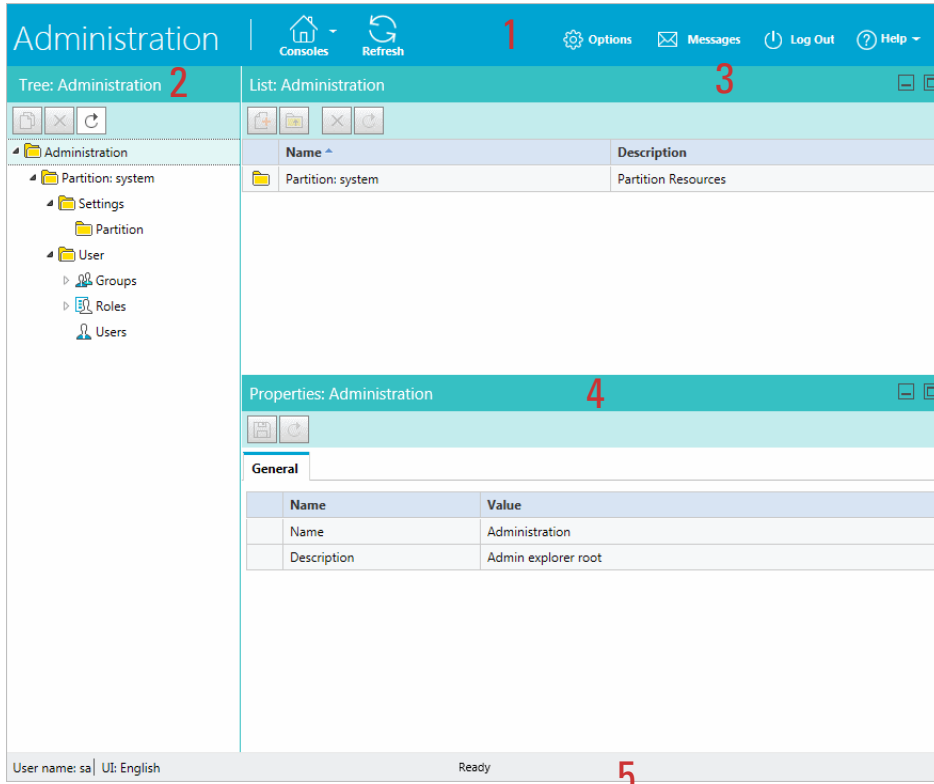
## Elements of the User Interface

---

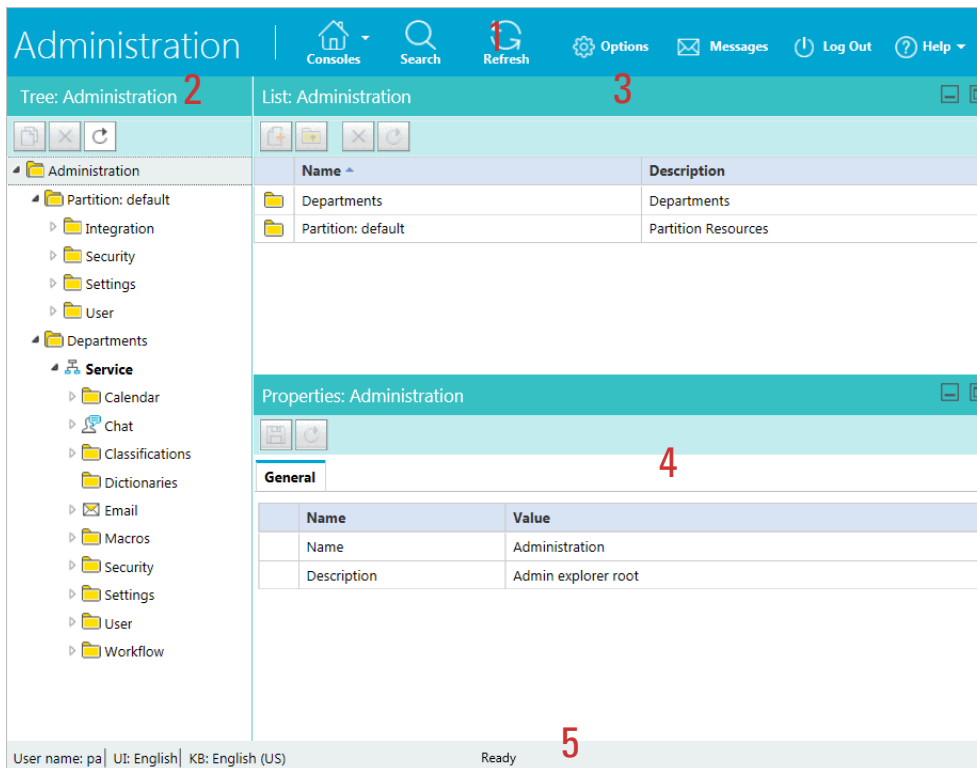
The console user interface has five functional areas:

1. **Console toolbar:** The main toolbar of the console appears at the top of the screen. It allows you to access some frequent commands with a single click.
2. **Tree pane:** The Tree pane lists all the business objects in the application, allowing you to select the node (folder) that you wish to work in. When you select a folder, its first-level contents are displayed in the List pane. In the Tree pane, you can cut paste or copy paste folders, delete folders which you have created, manage bookmarks and print folder contents.

To expand all first and second level nodes with a single click, shift + click the plus [+] button next to the topmost node. The contents of all first and second level nodes are displayed in the Tree pane.
3. **List pane:** The List pane displays first-level contents of the folder selected in the Tree pane. You can view the name, description, date of creation, and so on, of the displayed items. In this pane, you can create items or select existing ones to modify or delete them.
4. **Properties pane:** The Properties pane displays the contents of the business object selected in the List pane. In this pane, you can edit the properties of the selected item.
5. **Status bar:** The status bar is present at the bottom of every screen. It displays the following information:
  - The user name with which the user has logged in the system.
  - The language currently in use.
  - The status of the system (**Loading**, **Ready**, and so on).



*Elements of the Administration Console available in the system partition*



*Elements of the Administration Console available in the business partition*

The screenshot shows the Administration Console interface. At the top, there is a navigation bar with icons for Consoles, Search, Refresh, Options, Messages, Log Out, and Help. The main area is divided into three panes:

- Tree: Administration (2):** A left-hand navigation pane showing a hierarchical tree structure. The 'Service' folder is expanded, showing sub-items like Calendar, Chat, Classifications, Dictionaries, Email, Macros, Security, Settings, User, and Workflow.
- List: Administration (3):** A central pane displaying a list of items. The table below shows the data for the 'Departments' folder.
- Properties: Administration (4):** A right-hand pane showing the properties of the selected item. It includes a 'General' tab with a table of key-value pairs.

At the bottom, a status bar (5) displays the user name 'manju', UI language 'English', KB language 'English', and the system status 'Ready'.

Name	Description
Departments	Departments

Name	Value
Name	Administration
Description	Admin explorer root

*Elements of the Administration Console available in a department*



# Unified CCE Integration

- ▶ [About Unified CCE Integration](#)
- ▶ [Configuring ECE for Unified CCE](#)
- ▶ [Importing Data](#)
- ▶ [WebEx Experience Manager Integration](#)

This chapter describes the process of integrating ECE with Cisco Unified Contact Center Enterprise (Unified CCE).

## About Unified CCE Integration

The process of integrating ECE with Cisco Unified 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 ECE for Unified CCE

### To configure ECE for Unified CCE:

1. In the Tree pane, browse to **Administration > Partition:** *Partition Name* > **Integration > Unified CCE > Unified CCE.**
2. In the List pane toolbar, select **Unified CCE.**
3. In the Properties pane, on the General tab, you can view the following properties:
  - **Name:** This is provided by the system and cannot be changed.
  - **Description:** This is provided by the system and cannot be changed.
  - **Enable integration:** This field is set to **Yes** and cannot be edited.
  - **Deployment type:** This field is set to **On-Premises** and cannot be edited.



Name	Value
Name *	Unified CCE
Description *	Unified CCE
Enable integration *	Yes
Deployment type *	On-Premises

*View the general properties*


4. In the Properties pane, on the On-Premises tab, provide the following details for the Primary AWDB section:
  - **Unified CCE administration host name:** The server name or IP address of the host on which Packaged CCE or Unified CCE is installed.
  - **Active:** Set to **Yes**.
  - **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.

Name	Value
Unified CCE administration host name *	10.1.61.1
Active *	Yes
SQL server database name *	awdb
Port number *	1433
Database administrator login name *	sa
Database administrator login password *	*****
Maximum capacity *	360

*Provide the primary AWDB server details*

5. If you have a secondary AWDB and wish to apply it to your integration, click the Secondary AWDB section and provide the necessary details.
6. Click the **Save**  button.
7. In the Properties pane, on the Configuration tab, set the following:
  - Select the application instance.
  - Select the Agent Peripheral Gateways that apply.




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

Name	Value
Application instance *	Appinstance

Peripherals

Available Agent Peripheral Gateways	Selected Agent Peripheral Gateways
Agent_PG_Test2	Agent_PG
Agent_PG_Test	

*Provide configuration details*

8. 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 34](#).

# 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:

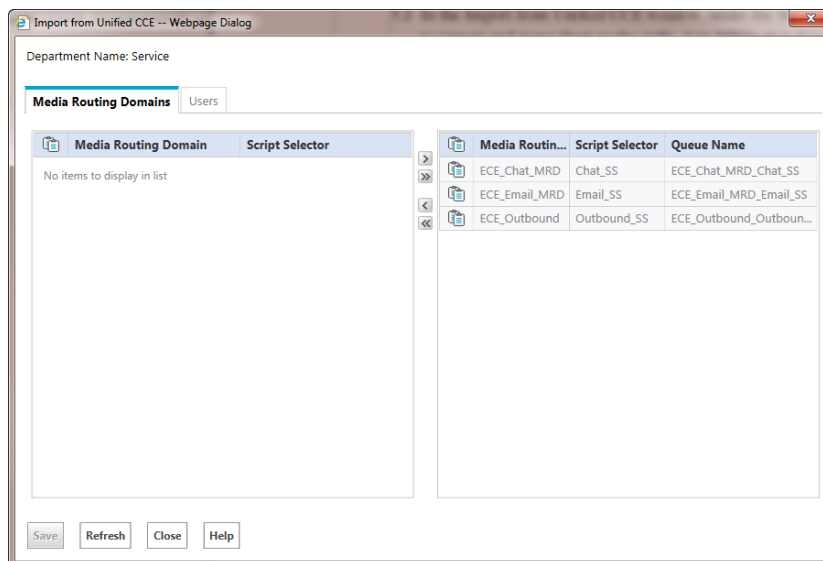
- ▶ **Media Routing Domains (MRDs):** These are shown as queues upon importing to a selected department.
- ▶ **Users:** These are shown as users upon importing to a selected department.

## Importing Media Routing Domains

The MRDs available for importing are decided based on the media classes configured in the partition level setting: Media Class Names ([page 48](#)). 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. MRDs for email cannot be non-interruptible.

### To import MRDs:

1. In the Tree pane, browse to **Administration > Partition:** *Partition Name* > **Integration > Unified CCE > Unified CCE.**
2. In the List pane toolbar, select the **Unified CCE.**
3. In the Properties pane, click the **Import** button.
4. From the Select Department window, select the department to which you are importing the MRDs. If you only have one department in your system, this step is skipped.
5. In the Import from Unified CCE window, under the Media Routing Domains tab, select the MRDs you wish to import and move them to the right. Any MRDs that do not have script selectors, or that have already been imported, are not shown.



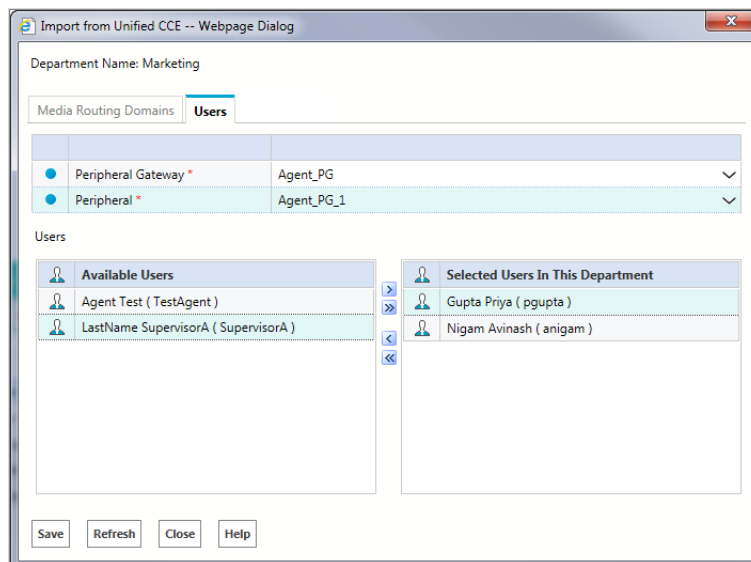
*Import MRDs*

- 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. If a queue created during the MRD import requires a name change later, it must be done through the Queue node in the department.
- Click the **Save** button.

## Importing Users

### To import Unified CCE users:

- In the Tree pane, browse to **Administration > Partition: *Partition Name* > Integration > Unified CCE > Unified CCE**.
- In the List pane toolbar, select **Unified CCE**.
- In the Properties pane, click the **Import** button.
- From the Select Department window, select the department to which you are importing the users. If you only have one department in your system, this step is skipped.
- In the Import from Unified CCE window, click the Users tab and set the following:
  - Select the peripheral gateway from the dropdown.
  - Select the appropriate peripheral.
  - Select the users from the Available Users list if you wish to import and move them to the Select Users in this Department list.



*Import users*

- Click the **Save** 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 135](#).

## WebEx Experience Manager Integration

WebEx Experience Manager (WXM) is a CCE product that provides Cisco customers a method of communicating their overall experience. Refer to your Unified CCE documentation for information about setting up WXM in Unified CCE.

ECE being a part of Unified CCE allows it to integrate with WXM and provide email and chat contact points to WXM. WXM integration in ECE brings insights from the overall customer journey to Agents and Supervisors via survey links in chat and email interactions. WXM survey links are then automatically appended to outbound emails and to customer chat windows when a chat is completed.

## Converting the Cloud Connect Publisher and Subscriber Certificates

In order to integrate WXM with ECE, a Cloud Connect Publisher and a Cloud Connect Subscriber certificate in PEM format must be installed on ECE. If the certificate is in DER/Binary format, it must be converted to PEM format.



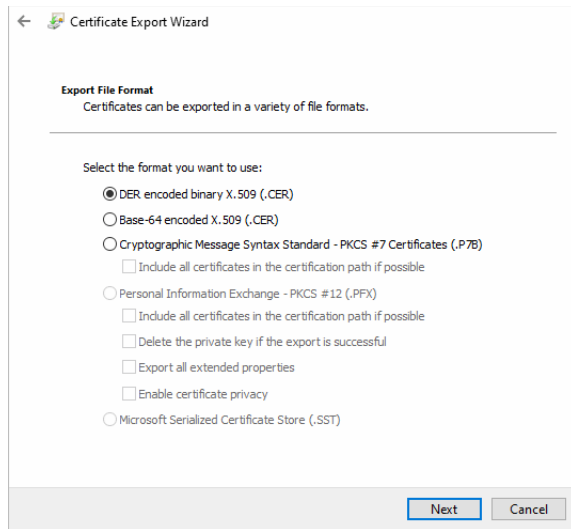
**Important:** This can be performed from any user desktop on which OpenJDK 11.0 is installed.

---

### To obtain the Cloud Connect Publisher Certificate:

1. In a browser, navigate to `https://cloudconnectpublisher.fqdn:8445/`.
2. Click the security icon in the address bar to bring up the option to view certificates.
3. Click the Certificate option.
4. In the certificate window, navigate to the Details tab and click on the Copy To File button.
5. Continue the Certificate Export wizard and select DER encoded binary X.509 (CER)

- Browse to the location on your local machine and provide a name for the certificate and complete the wizard to store the certificate.



Select the DER option in the certificate export wizard

### To obtain the Cloud Connect Subscriber Certificate:

- In a browser, navigate to `https://Cloud Connect Subscriber FQDN:8445/`.
- Click the security icon in the address bar to bring up the option to view certificates.
- Click the Certificate option.
- In the certificate window, navigate to the Details tab and click on the Copy To File button.
- Continue the Certificate Export wizard and select DER encoded binary X.509 (CER)
- Browse to the location on your local machine and provide a name for the certificate and complete the wizard to store the certificate.

### To convert a certificate from DER or Binary to PEM format:

- Copy the DER/Binary certificate file (for example, `example.cer`) to the `JAVA_HOME\bin` folder.
- Open command prompt at `JAVA_HOME\bin` folder.
- Import the DER/Binary certificate to the default java truststore using the following command:

```
JAVA_HOME\bin\keytool.exe -import -trustcacerts -file test.cer -alias test_alias -keystore ..\lib\security\cacerts
```

- Provide the keystore password and press ENTER on your keyboard.
- Export the certificate in PEM format using following command:

```
JAVA_HOME\bin\keytool.exe -exportcert -alias test_alias -file test.pem -rfc -keystore ..\lib\security\cacerts
```

- Provide the keystore password and press ENTER on your keyboard.
- This creates the PEM certificate with the `.pem` extension in the `JAVA_HOME\bin` folder.
- Delete the DER/Binary certificate by executing the following command:

```
JAVA_HOME\bin\keytool.exe -delete -alias test_alias -keystore
..\lib\security\cacerts
```

9. Provide the keystore password and press ENTER on your keyboard.



## Installing the Cloud Connect Publisher and Subscriber Certificates on ECE



**Important:** WXM communicates with ECE via the Application server, which uses TCP 8445 port for HTTPS connections with Cloud Connect services. This port must be open on the ECE Application server to operate.

---

### To install the Cloud Connect Publisher and Subscriber certificates on ECE:

1. Sign in as a partition administrator and in the Tree pane, browse to **Administration > Partition:** *Partition Name* > **Security > Certificates**
2. In the List pane, click the **New**  button.
3. In the Properties pane, provide the following:
  - **Name:** Name of the certificate.
  - **Description:** Description of the certificate.
  - **Certificate:** Click the **Assistance** button, Paste the contents of the Cloud Connect Publisher certificate into the area and click **OK**. The certificate must be in PEM format before copying and pasting here. The certificate should start with -----BEGIN CERTIFICATE----- and end with -----END CERTIFICATE----- .For more details, see [“Converting the Cloud Connect Publisher and Subscriber Certificates” on page 36](#).
4. Click the **Save**  button.



**Important:** These steps must also be performed for the Cloud Connect Subscriber server if the self-signed certificate is used or only the root certificate is uploaded in PEM format.

---

# 3 Settings

- ▶ [About Settings](#)
- ▶ [Configuring Settings](#)
- ▶ [Unified CCE Integration Settings](#)
- ▶ [Common Settings](#)
- ▶ [Security Settings for Cookies](#)
- ▶ [Proxy Server Settings](#)
- ▶ [Logger Settings](#)
- ▶ [User Account Settings](#)
- ▶ [User Session Settings](#)
- ▶ [Business Calendar Settings](#)
- ▶ [Customer Information Settings](#)
- ▶ [Incoming Email Settings](#)
- ▶ [Outgoing Email Settings](#)
- ▶ [Blocked Attachments Settings](#)
- ▶ [Workflow Settings](#)

- ▶ [Activity Assignment Settings](#)
- ▶ [Monitor Settings](#)
- ▶ [Activity Handling Settings](#)
- ▶ [Inbox Settings](#)
- ▶ [Spelling and Blocked Words Settings](#)
- ▶ [Search Settings](#)
- ▶ [Knowledge Base Settings](#)
- ▶ [Chat Settings](#)



This chapter helps you configure various aspects of the system with the help of 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.

Settings are administered in groups. The available groups are:

1. **System settings group:** This group is available to system administrators to control the system level resources. These settings cannot be reset at lower levels. This group includes dispatcher settings.
2. **Partition settings group:** This group is available to partition administrators to control the partition level resources. These settings cannot be reset at lower levels. This group includes:
  - a. Activity settings
  - b. Activity pushback settings
  - c. Chat settings
  - d. Common settings
  - e. Dispatcher settings
  - f. Retriever settings
  - g. General settings
  - h. Knowledge base settings
  - i. Monitoring settings
  - j. Workflow Engine settings
  - k. Security settings
3. **Department settings group:** This group is available to administrators to control the department level resources. Department settings can be configured by partition administrators for all departments in the partition, by department administrators for individual departments, and by individual users as user preferences. This group includes:
  - a. Activity settings
  - b. Activity pushback settings
  - c. Chat settings
  - d. Common settings
  - e. Email blocked file extension settings
  - f. General settings
  - g. Knowledge base settings
  - h. Monitoring settings
  - i. Queue settings

- j. Security settings
- k. Spell checker settings
- l. User settings

## Settings to Configure After Installation

In this section, we describe certain settings that should be configured soon after installation. These settings are of two types:

1. **Mandatory settings:** These settings must be configured before using the application.
2. **Optional settings:** Although it is not mandatory to change these settings, you are likely to feel the need to configure them for your business.

### Mandatory Settings

#### At the Partition Level

Make sure you configure the following settings:

- ▶ To: address for notifications from services ([page 68](#))
- ▶ From: address for notifications from services ([page 68](#))
- ▶ Default SMTP server settings ([page 69](#))

#### At the Department Level

Configure the following setting for each department.

- ▶ From email address for alarm ([page 72](#))

### Optional Settings

Although it is not mandatory to change these settings, you are likely to feel the need to configure them for your business.

#### At the Partition Level

- ▶ Customer departmentalization ([page 64](#))
- ▶ Inactive time out ([page 60](#))
- ▶ Session time out ([page 61](#))

#### At the Department Level

- ▶ Business calendar timezone ([page 61](#))


# Configuring Settings

---

## Configuring System Partition Settings

Login to the System partition (zero partition) of the application to access the system partition setting.


### To configure a system partition setting:

1. Log in to the system partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Context\_Root\_Name* > **Settings > Partition**.
3. In the List pane, select the Partition settings group.  
The Properties pane refreshes to show the attributes of the group.
4. Next, in the Properties pane, go to the Attributes tab to configure values for settings. From the list, select a setting to modify. In the **Value** field provide a value for the setting.
5. Click the **Save**  button.

## Configuring Business Partition Settings

Login to the Business partition of the application to access the business partition setting.

### To configure a business partition setting:

1. Log in to the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition\_Name** > **Settings > Partition**.
3. In the List pane, select the partition settings group.  
The Properties pane refreshes to show the attributes of the group.
4. Next, in the Properties pane, go to the Attributes tab to configure values for settings. From the list, select a setting to modify. In the **Value** field provide a value for the setting.
5. Click the **Save**  button.

## Configuring Department Settings

### To configure a department setting:

1. Log in to the business partition and go to the Administration Console.
2. In the Tree pane, browse to the Settings node.
  - If you want to configure the settings for all departments, then browse to **Administration > Partition\_Name** > **Settings > Department**.
  - If you want to configure the setting for an individual department, then browse to **Administration > Departments > Department\_Name** > **Settings > Department**.
3. In the List pane, select the department settings group.

The Properties pane refreshes to show the attributes of the group.

4. Next, in the Properties pane, go to the Attributes tab to configure values for settings. From the list select a setting to modify and do the following:

- a. In the **Value** field provide a value for the setting.
- b. If you are configuring the setting for all departments in the partition or for all users in the department (for settings that can be configured at the user setting group level), then in the **Can be reset at lower level** field select **No**. Once it is set to **No**, the value of the setting cannot be changed at lower level. By default it is set to **Yes**.

If a setting is made unavailable for lower levels, the value set at the higher level is applicable. When the setting is reset to be available at lower levels, the setting is made available only at the next level and the administrator has to decide if the setting should be made available to levels lower than that. The value of the setting configured at the higher level is carried over to lower levels.

5. Click the **Save**  button.

## Unified CCE Integration Settings

---

### Agent Availability Settings After Completion of Call

To view or configure the settings, click the **Assistance** button in the **Value** field of the setting.

#### Mark Agent Ready After Completion of Call

Use this setting to adjust the default agent availability status upon completion of a call activity. 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: -

## Allow Transferring Chats to Agents Who Are Not Available

Use this setting to allow chats 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 Available

Use this setting to allow emails 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 emails to be transferred to agents who are not logged in. When you enable this setting, you may want to disable the autopushback settings ([page 76](#)), otherwise the activities assigned to agents when they are not logged in will be automatically pushed back from their inbox.

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

## 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

## Chat Watchdog Interval

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

To view or configure the settings, click the **Assistance** button in the **Value** field of the setting.

## Web Chat (Seconds)

This setting applies to standard incoming web chat activities that are created via chat entry points.

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

## Messaging Chat (Minutes)

This setting applies to incoming chat activities that are created via the eGain Messaging Hub SolutionPlus product extension, for example: Facebook Messenger, Twitter DMs, or WhatsApp messages. This setting is not in use if the product extension is not installed. For more information about the eGain Messaging Hub SolutionPlus product extension, see the *eGain Solve for Cisco User Guide*.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE Integration
- ▶ Data type: Integer
- ▶ Default value: 210
- ▶ Minimum value: 5
- ▶ Maximum value: 210 (3.5 hours)

## Enable Chat Queueing

This allows customers to initiate new chats even when all agents are working at their maximum capacity. The chat requests 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** ([page 46](#)) setting.

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

## Maximum Assignment Beyond Concurrent Task Limit

This setting determines the maximum number of activities to that can be assigned to an agent beyond concurrent task limit (CTL) of the Media Routing Domain. Changes made to this setting can affect how activities are transferred to agents.

For more information, see [“Important Things to Note About Picking and Pulling Activities” on page 105.](#)

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

## Maximum Wait Time for Login Response From UCCE (Seconds)

This setting refers to the maximum time allowed while waiting for a login response from Unified CCE before a timeout occurs. If the integrated agent is not logged in the defined time, a message is displayed to the agent. 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

## Concurrent Task Limit Mappings by Media

This setting controls the default concurrent task limit (CTL)for activities by media class. This allows administrators to specifically control the default concurrent task limit for each type of activity type: email, chat, and outbound. Be aware that this is only the default setting for CTL and to change the CTL for queues is done at

the queue level. For more information, see the *Enterprise Chat and Email Administrator's Guide to Routing and Workflows for Unified Contact Center Enterprise*.

Note that changes made to this setting can affect how activities are transferred to agents. To view or configure the settings, click the **Assistance** button in the **Value** field of the setting.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE Integration
- ▶ Data type: String
- ▶ Default value: 1:1:1
- ▶ Minimum value: 1:1:1
- ▶ Maximum value: 10:10:10

## 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.

To view or configure the settings, click the **Assistance** button in the **Value** field of the setting.

- ▶ 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
- ▶ Value options: The secondary window allows for custom Media Classes to be designated.

## 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



## Reason Code for Agent Not Ready

The reason code sent to Unified CCE when agents mark themselves unavailable. You need to change this setting only if the default reason code 2 is currently used to track some other agent status.

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

## Starvation Time for Activities

The maximum time the system will wait to send a routing request for an activity. After the time limit set in these settings is met, the request for the waiting activity is sent first. 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 after the starvation time of chat activity, it will process the chat activity first before processing the next call activity.

- ▶ 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

## Popover Display Configuration

Use this setting to configure counter type and display time for popover notifications. Use the **Assistance** button to change the values of this setting.

- ▶ Type: Partition settings group
- ▶ Subtype: Unified CCE integration
- ▶ Data type: String
- ▶ Default values:
  - Counter Type: Count down

- Counter Value (in seconds): 10
- ▶ Value options:
  - Counter Type: Count up; Count down
  - Counter Value (in seconds): minimum of 10; maximum of 60

## Common Settings

---

### Installation Name

Define a unique name for your installation. Provide a 1 to 4-letter code. For example: PRD, EG, TEST, PROD, TST2, DEMO. The name must not contain spaces or special characters. If you have more than one ECE deployments, make sure that you use a unique installation name for all your ECE installations. This installation name is appended to the article IDs.

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

### Web Server URL or Load Balancer URL

This URL is used for the following:

- ▶ Single Sign-On configurations ([page 165](#))

In this setting, define the Web Server URL. If your installation has multiple web servers, provide the Load Balancer URL.

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

### 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
- ▶ Can be reset 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 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
- ▶ Can be reset at lower level: Yes

## Security Settings for Cookies

---

Use these settings to secure the cookies created by the application for user consoles. When the cookies are secure, the browser prevents the transmission of cookies over an unencrypted channel. To view or configure the settings, click the **Assistance** button in the **Value** field of the setting.

### Secure the Cookies Created by Application for Consoles and Knowledge Portals

Enable this setting to secure all the cookies created by the application for user consoles (For example, Agent Console, Administration Console, and so on.). When this setting is enabled, you must configure 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. You can enable this setting only 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

Enable this setting to secure 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

# Proxy Server Settings

---

Deployments using a proxy server for connections from the application and services servers to the Internet must configure the proxy settings.

To view or configure the proxy server settings, click the **Assistance** button in the **Value** field of the setting. Deployments can utilize a HTTP(S) proxy server as well as a Socks proxy server. You can choose to have the Socks proxy server use the same configuration as the HTTP(S) proxy, with a different server port if necessary.

Socks proxy server support POP3, IMAP, SMTP, and ESMTP mail protocols as well. Select all that apply.

## Use Server

Enable this setting if your deployment uses a proxy server for connections from the application server to the Internet.

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

## Server Hostname

Provide the fully qualified domain name of the proxy server.

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

## Server Port

Provide the port number of the proxy server.

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: Integer
- ▶ Default value: —
- ▶ Minimum value: —

- ▶ Maximum value: —

## Authentication

Enable this setting if the proxy server requires authentication. Also make sure that you configure the Proxy Username and Proxy Password settings.

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

## Username

Provide the username of the user used to connect to the proxy server. You need to configure this setting if you have enabled the Enable Proxy Authentication setting.

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

## Password

Provide the password of the user used to connect to the proxy server. You need to configure this setting if you have enabled the Enable Proxy Authentication setting.

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: Encrypted
- ▶ Default value: —

## 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

## User Account Settings

---

This set of settings allow administrators to configure and enforce login and password policies for agents and other users.

### Password Complexity Policy

Use this setting to define the password policy you want to enforce for all user passwords in the system. The value of this setting is defined as a regular expression. Click the **Assistance** button to change the various properties for the setting. You can test a password after defining the regular expression. You can also change the message that you want to show to users when their passwords do not comply with the password policy. If you do not wish to enforce a policy, you can delete the value of this setting.

- ▶ 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

### 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

## Allow Local Login for Partition Administrators

While this setting applies to partition administrators that utilize Single Sign-On for SAML 2.0, it is not required for Cisco IDS to function. See [“Preparing to Configure Single Sign-On in ECE” on page 165](#) for more information.

Use this setting to define whether or not a partition administrator should be able to log into the application locally once SSO has been enabled.

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

## User Session Settings

---

### Inactive Time Out (Minutes)

Use this setting to define the time after which a user session is made inactive if the user does not do any activity in the application. Users can activate the session by providing their password. The session is resumed 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)

Use this setting to define the time for which a user session is kept in the memory of the server after the user session has become inactive. Once this time is elapsed, the system deletes the session from the memory. Users have to login in to the application by providing their user name and password and a new user session is created.

- ▶ Type: Partition settings group
- ▶ Subtype: Security
- ▶ Data type: Integer
- ▶ Default value: 60
- ▶ Minimum: 5
- ▶ Maximum: 1440

## Business Calendar Settings

---

### 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

- ▶ Can be reset at lower level: No

## Customer Information Settings

---

### Customer Departmentalization

Use this setting to decide if customers should be shared across departments. Enable this setting if you do not want to share customer history and customer information across departments.





**Important:** This setting can only be changed while there is one department in the partition. As soon as the second department is created in the partition, the setting becomes disabled and cannot be changed.

---

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

## Incoming Email Settings

---

### Number of Emails to Retrieve

Use this setting to define the maximum number of emails to be picked by the Retriever Service for processing.

- ▶ Type: Partition settings group
- ▶ Subtype: Email retriever
- ▶ Data type: Integer
- ▶ Default value: 10
- ▶ Minimum value: 10
- ▶ Maximum value: 250

### Maximum Email Size for Retriever (MB)

Use this setting to define the maximum size of emails that the Retriever Service can retrieve from the Mail Server. This size includes the email subject, body (text and HTML content), header, and attachments. For example, if the value of the setting is 1 MB, and an email with 1 MB content comes in, this email will not be retrieved, as the size of the email is greater than 1 MB because of headers and both text and HTML parts of email. If the email size exceeds the number specified in this setting, the email is either skipped or deleted, and a notification is sent. This action is defined in the “Action for Large Email” setting.

- ▶ Type: Partition settings group
- ▶ Subtype: Email retriever
- ▶ Data type: Integer
- ▶ Default value: 16
- ▶ Minimum value: 2
- ▶ Maximum value: 35

## Maximum Body Size for Retriever (KB)

Use this setting to define the maximum size of the email body that the Retriever Service can retrieve from the Mail Server. This size does not include the header and attachments. If the body size exceeds the size specified in this setting, the body is saved as a text file and is attached to the email. A note is added to the email body that the original email content is available as an attachment. This note can be changed from the “Message note for large body” setting.

- ▶ Type: Partition settings group
- ▶ Subtype: Email retriever
- ▶ Data type: Integer
- ▶ Default value: 1000 KB
- ▶ Minimum value: 100
- ▶ Maximum value: 1000 KB

## Message Note for Large Body

Use this setting to change the message added to emails, which exceed the allowed maximum body size for incoming emails.

- ▶ Type: Partition settings group
- ▶ Subtype: Email retriever
- ▶ Data type: String
- ▶ Default value: Email body was too large. It is saved as an attachment
- ▶ Minimum value: —
- ▶ Maximum value: 255

## Action for Large Email

Use this setting to decide what should be done with large emails coming in the system. An email is considered as large if it exceeds the size specified in the “Maximum email size for retrieval” setting.

- ▶ Type: Partition settings group
- ▶ Subtype: Email retriever
- ▶ Data type: Enumeration
- ▶ Default value: Skip and notify
- ▶ Value options:
  - Skip and Notify: Retriever skips the email and notifies the administrator about the same.
  - Delete and Notify: The email is deleted from the mail server and a notification is sent to the administrator.

# Outgoing Email Settings

---

## Maximum Body Size for Dispatcher (KB)

Use this setting to define the maximum body size of an outgoing email. This size considers only the email body size and excludes the email attachments. The system will not allow agents or workflows to create outgoing emails whose body size is larger than this setting value. Users are notified while composing email from the Agent Console, and while configuring workflows from Administration Console. If a system generated email (auto-acknowledgements and so on.) exceeds this size, the email will not be sent and a notification is sent to the email address configured in the “To: address for notification from Services” setting.

- ▶ Type: Partition settings group
- ▶ Subtype: Email dispatcher - Common
- ▶ Data type: Integer
- ▶ Default value: 100
- ▶ Minimum value: 100
- ▶ Maximum value: 1000

## Maximum Email Size for Dispatcher (MB)

Use this setting to define the maximum size of an outgoing email. This size includes the body of the email and the attachments. The system will not allow agents or workflows to create outgoing emails whose size is larger than this setting value. Users are notified while composing email from the Agent Console, and while configuring workflows from Administration Console. If a system generated email (auto-acknowledgements and so on.) exceeds this size, the email will not be sent and a notification is sent to the email address configured in the “To: address for notification from Services” setting.

**Note:** The value of this setting should be 40% less than the email size configured on the SMTP server. This buffer is needed because email data (content and attachments) is encoded before an email is sent out by the SMTP server. For example, if the size configured on SMTP is 10 MB, the value of this setting should be 6 MB.

- ▶ Type: Partition settings group
- ▶ Subtype: Email dispatcher - Common
- ▶ Data type: Integer
- ▶ Default value: 25
- ▶ Minimum value: 1
- ▶ Maximum value: 150

## To: Address for Notifications From Services

DSM sends out notifications when any error occurs in the functioning of services (example, retriever, dispatcher, etc). Use this setting to specify the email address to which notifications are sent by the DSM.

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: String
- ▶ Default value: —
- ▶ Minimum value: 0
- ▶ Maximum value: 255

## From: Address for Notifications From Services

DSM sends out notifications when any error occurs in the functioning of services (example, retriever, dispatcher, etc). Use this setting to specify the email address displayed in the “from” field of the notifications sent by the DSM.

- ▶ Type: Partition settings group
- ▶ Subtype: Common
- ▶ Data type: String
- ▶ Default value: —
- ▶ Minimum value: 0
- ▶ Maximum value: 255

## Notification Mails Auto BCC

DSM sends out notifications when any error occurs in the functioning of services (example, retriever, dispatcher, etc). Use this setting to specify the email address that will be sent notification emails, but remain hidden to other recipients.

- ▶ Type: Partition settings group
- ▶ Subtype: Email dispatcher-Mail
- ▶ Data type: String
- ▶ Default value: —
- ▶ Minimum value: 0
- ▶ Maximum value: 255

## Restrict To, Cc, and Bcc Email Address Fields

Use this setting to determine if the To, Cc, and Bcc fields in the Agent Console require the dropdown menu to select an email address, or if agents can manually enter email addresses. Restricting agents from manually entering email addresses prevents auto-complete from affecting the fields.

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Enumeration
- ▶ Default value: Allow user to type a new address and select from dropdown
- ▶ Value options: Allow user to type a new address and select from dropdown, Prevent user from selecting from dropdown, Prevent user from typing new email address
- ▶ Can be reset at lower level: Yes

## Default SMTP Server Settings

For various objects in the system, you can configure notifications to be sent to administrators. Some of the objects for which you can configure notifications are, Monitors (in the Supervision Console), Reports (in the Reports Console), Alarm workflows (in the Administration Console), Abandoned chats (in the Administration Console). The address to which these notifications are sent, is specified in the properties of the object and the from email address is specified in the “From: address for notifications from services” setting.

Configure the settings described in this section for the server to send notifications to administrators. To view or configure the default SMTP server settings, click the **Assistance** button in the **Value** field of the setting.

### Server type

In this setting select the protocol (SMTP or ESMTP) to be used for the server.

- ▶ Type: Partition settings group
- ▶ Subtype: Default SMTP Server
- ▶ Data type: Enumeration
- ▶ Default value: Never
- ▶ Value options: Never, If authentication fails

### Use SMTP

If the “Server type” setting is set to ESMTP, to be used for the server.

- ▶ Type: Partition settings group
- ▶ Subtype: Default SMTP Server
- ▶ Data type: Enumeration
- ▶ Default value: SMTP
- ▶ Value options: SMTP, ESMTP

## Server name

In this setting provide the name of the server.

- ▶ Type: Partition settings group
- ▶ Subtype: Default SMTP Server
- ▶ Data type: String
- ▶ Default value: —
- ▶ Minimum value: 0
- ▶ Maximum value: 256

## User name (ESMTP)

If the “Server type” setting is set as “ESMTP”, provide the user name to be used to connect to the mail server.

- ▶ Type: Partition settings group
- ▶ Subtype: Default SMTP Server
- ▶ Data type: String
- ▶ Default value: —
- ▶ Minimum value: 0
- ▶ Maximum value: 255

## Password

If the “Server type” setting is set to “ESMTP”, provide the password to be used to connect to the mail server. Verify the password in the field immediately below.

- ▶ Type: Partition settings group
- ▶ Subtype: Default SMTP Server
- ▶ Data type: Encrypted
- ▶ Default value: —
- ▶ Minimum value: 0
- ▶ Maximum value: 255

## Connection type

Select the authentication connection type for the server to use.

- ▶ Type: Partition settings group
- ▶ Subtype: Default SMTP Server
- ▶ Data type: Enumeration
- ▶ Default value: Plain text

- ▶ Value options: Plain text, SSL, TLS

## Port

In this setting provide the default port of the SMTP server. The value of the setting cannot be changed from the UI. **Note:** The port value changes based on the connection type.

- ▶ Type: Partition settings group
- ▶ Subtype: Default SMTP Server
- ▶ Data type: String
- ▶ Default value: 25
- ▶ Value options: —

# Blocked Attachments Settings

---

## Email - Criteria for blocking attachments

Use this setting to configure the criteria for blocking attachments. You can choose to block attachments for incoming emails, or for both incoming and outgoing emails.



**Important:** After changing the value of the setting, you need to restart all retriever instances in the system.

---

- ▶ Type: Department settings group
- ▶ Subtype: Email blocked file ext
- ▶ Data type: Enumeration
- ▶ Default value: Inbound emails only
- ▶ Value options: Inbound email only, Both inbound and outbound emails
- ▶ Can be reset at lower level: No



**Important:** If the “Both inbound and outbound emails” option is selected, agents do not see the “Attachment” option in the More Options menu when replying to emails.

---

## Block All Attachments

Use this setting to block all attachments coming in the system.



**Important:** After changing the value of the setting, you need to restart all retriever instances in the system.

---

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

## Action on Blocked Attachments

Use this setting to decide what should be done with all the block attachments. You can either save the attachments in the `Cisco_Home\eService\storage\1\mail\attachments` folder or you can delete them.




---

**Important:** After changing the value of the setting, you need to restart all retriever instances in the system.

---

- ▶ Type: Department settings group
- ▶ Subtype: Email blocked file ext
- ▶ Data type: Enumeration
- ▶ Default value: Quarantine
- ▶ Value options:
  - Quarantine: The attachment is saved in the `Cisco_Home\eService\storage\1\mail\attachments` folder and a notification email is sent to the administrator.
  - Delete: The attachment is deleted.
- ▶ Can be reset at lower level: No

## Workflow Settings

---

### From Email Address for Alarm

Use this setting to configure the email address to be displayed in the “From” field of alarm notifications.

- ▶ Type: Department settings group
- ▶ Subtype: Common
- ▶ Data type: String
- ▶ Default value: —
- ▶ Minimum value: 0
- ▶ Maximum value: 255



- ▶ Can be reset at lower level: No

## Include Original Message for Auto Acknowledgement

Use this setting to include the content of incoming emails in the auto-acknowledgement emails sent to customers in response to the incoming emails.

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

## Auto Response Number

Use this setting to define the number of auto-acknowledgements and auto-responses to be sent to a customer in a specified time duration. The time duration is configured through the “Auto response time” setting. For example, if the value in this setting is three and a customer sends four emails in one hour (time duration configured through the “Auto response time” setting), the customer will get auto responses to three emails only.

- ▶ Type: Partition settings group
- ▶ Subtype: Workflow engine
- ▶ Data type: Integer
- ▶ Default value: 3
- ▶ Minimum value: 3
- ▶ Maximum value: 100
- ▶ Can be reset at lower level: No

## Auto Response Time

In this setting define the time duration (in minutes) to be considered to decide the number of auto responses to be sent to a customer.

- ▶ Type: Partition settings group
- ▶ Subtype: Workflow engine
- ▶ Data type: Integer
- ▶ Default value: 1440
- ▶ Minimum value: 360
- ▶ Maximum value: 1440

## Set “From” Email Address for Email Activities Transferred Between Departments

This setting determines how the from email address is set for the email activities that are transferred to the department from other departments. Administrators can choose from the following options:

- **Do not change:** The original email address set in the From field is retained.
  - **Use default alias of destination department:** The From email address is set to the default alias configured for the department. Make sure that a default alias is configured for the department.
  - **Force agents to select “From” email address:** The value of the “From” field is reset to “Please select an email address” and agents are required to pick the From address while sending out the email.
- ▶ Type: Department setting group
  - ▶ Subtype: Activity
  - ▶ Data type: Enumeration
  - ▶ Default value: Do not change
  - ▶ Value options: Do not change, Use default alias of destination department, Force agents to select “From” email address
  - ▶ Can be reset at lower level: No

## Activity Assignment Settings

### Personalized Activity Assignment Settings



**Important:** This setting does not apply to installations integrated with Packaged CCE.

The personalized activity assignment feature allows you to assign activities pertaining to a case to the agent who last sent a response for that case. This feature applies to email activities. For example, say an email (activity ID 1001) comes in for case 2001, and agent Mary responds to the activity. The next email reply (activity ID 1003) from the customer will be assigned to agent Mary. Say, agent Mary transfers the activity to agent John, and agent John responds to this email, the next email (activity ID 1005) for the case 2001 will be assigned to agent John.

To view or configure the personalized activity assignment settings, click the **Assistance** button in the **Value** field of the setting.

### Personalized Activity Assignment

Use this setting to enable the personalized activity assignment feature and to define if personalized activity assignment should happen always, or only when the agent is logged in and available for emails.

- ▶ Type: Department settings group
- ▶ Subtype: Queue

- ▶ Data type: Enumeration
- ▶ Default value: Logged in
- ▶ Value options:
  - **Logged in:** Activities are assigned to the agent if they are logged into any ECE Media Routing Domains, irrespective of their state in the domain. They do not need to be in the ready status; they can be in not-ready status and personalized activity assignment setting will still assign emails.
  - **Always:** Activities are always assigned to the agent whether the agent is logged in or not.



**Important:** Note that Unified CCE does not assign activities to agents who are not signed in. Unified CCE routes the activity to an agent based on availability. The preferred agent ID must be handled by Unified CCE to ensure an email is assigned to the same agent.

---

- **Disable:** Personalized activity assignment is disabled.
- ▶ Can be reset at lower level: No

## Enable Personalized Activity Assignment for Forwarded Emails

Use this setting to enable personalized activity assignment for forwarded emails. For example, if an agent forwards an email from a case, and another email comes in for the same case, it will get assigned to the agent who had forwarded the last email.

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

## Enable Personalized Activity Assignment Only to Users with Permissions on Queue

Use this setting to enable personalized activity assignment feature only for users in a department who have queue permissions. This setting ensures that agents who may have had a correspondence with a customer are not assigned activities from that customer if the agent does not meet the criteria of the queue to which the incoming activity belongs.

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

## Enable Autopushback

Use this setting to enable the auto-pushback feature for your department. Auto-pushback helps you to automatically pull back activities from logged out agents and assign these activities to other available agents. Pinned activities are not candidates for auto-pushback. Along with this setting, make sure you configure the time duration after which an activity should be considered for pushback and the criteria for activities to be pushed back from the agent's inbox. Note that these auto-pushback settings apply to the following activities - inbound emails associated with queues, supervisory activities associated with queues, tasks associated with queues, and custom activities associated with queues. The following activities are not considered for auto-pushback - rejected supervisory activities, drafts, pinned activities, locked activities, and outbound emails.

- ▶ Type: Department settings group
- ▶ Subtype: Activity pushback
- ▶ Data type: Enumeration
- ▶ Default value: Enabled
- ▶ Value options: Disabled, Enabled
- ▶ Can be reset at lower level: No

## Autopushback Time (Minutes After Logout)

In this setting, define the time duration after which an activity is pulled back from an agent and is sent back to the original queue to be reassigned to another agent.

- ▶ Type: Department settings group
- ▶ Subtype: Activity pushback
- ▶ Data type: Integer
- ▶ Default value: 30
- ▶ Minimum value: 0
- ▶ Maximum value: 21600 (15 Days)
- ▶ Can be reset at lower level: Yes

## Activity Type for Autopushback

In this setting, determines the criteria for automatically pulling back activities from the agent's inbox.

- ▶ Type: Department settings group
- ▶ Subtype: Activity pushback
- ▶ Data type: Enumeration
- ▶ Default value: New activities only
- ▶ Value options:
  - None: No activities will be pushed back to the queues.
  - New activities only: Only activities with substatus "New" will be pushed back to the queues.

- Both new and incomplete activities: All the activities will be pushed back to the queues.
- ▶ Can be reset at lower level: Yes

## Activities to Pull First

This setting determines the criteria for pulling activities in the Agent Console. When the agent clicks the **Pull** button in the Agent Console, the activities based on this criteria are assigned to the agent.

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Enumeration
- ▶ Default value: Most overdue
- ▶ Value options: Most overdue, Due Soonest, Highest Priority, Newest, Oldest
- ▶ Can be reset at lower level: Yes

## Maximum Activities to Display for Pull

Use this setting to specify the maximum number of activities that are displayed in the Pull activities window in the Agent Console.

- ▶ Type: Partition settings group
- ▶ Subtype: Activity
- ▶ Data type: Integer
- ▶ Default value: 50
- ▶ Minimum value: 1
- ▶ Maximum value: 100

## Maximum Activities to Pull at a Time

This setting determines the maximum number of activities that are assigned to an agent when he clicks the **Pull** button in the Agent Console.

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Integer
- ▶ Default value: 10
- ▶ Minimum value: 1
- ▶ Maximum value: 25
- ▶ Can be reset at lower level: Yes

# Monitor Settings

---

## Common Settings for Monitors

### 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
- ▶ Can be reset 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
- ▶ Can be reset at lower level: No

### Chat - SLA for Response Time (Seconds)

This setting is required for the, Chat - Current service level (%) and Chat - Daily service level (%), queue-monitoring attributes, viewed from the Supervision Console. With this setting you can decide the threshold interval (in seconds) that all in-progress sessions are checked against, to measure what percentage had a wait time lesser than the threshold. Any session picked up after a wait time lesser than this threshold is counted as having met the service level. The service level is shown as an aggregate percentage based on how many sessions have met the service level and gives an indication of the timely pick-up of sessions by agents. If this value is set to blank, then the “Chat - Current service level (%)” and “Chat - Daily service level (%)” attributes will show a value of 100% for all queues. The default value is 600.

- ▶ Type: Department settings group

- ▶ Subtype: Monitoring
- ▶ Data type: Integer
- ▶ Default value: 600
- ▶ Minimum value: —
- ▶ Maximum value: 3600
- ▶ Can be reset at lower level: No

## **Chat - Daily Service Level Sample Set Definition**

This setting defines if the abandoned chat activities should be considered while calculating the daily service level for chats.

- ▶ Type: Department settings group
- ▶ Subtype: Monitoring
- ▶ Data type: Enumeration
- ▶ Default value: All chats handled including abandoned
- ▶ Value options: All chats handled including abandoned, All chats handled excluding abandoned
- ▶ Can be reset 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

## Activity Handling Settings

---

### Agent Guidance Notifications

When the agent selects an activity in the inbox and there is a note attached to the activity from the last agent who transferred it to the current agent, the latest note appears in the bottom right corner. Here you can adjust the duration of the notifications that appears in the Agent Console. Click the **Assistance** button to view and configure the setting.

- ▶ Type: Department settings group
- ▶ Subtype: Common
- ▶ Data type: String
- ▶ Default value: —
- ▶ Value options:
  - **Name:** Name of the notification type.
  - **Duration:** Select **Short**, **Long**, or **Sticky**.
  - **Style:** This is set to **Default** and cannot be changed.
  - **Color:** This is set to **White** and cannot be changed.
  - **Active:** Click the checkbox to make the setting active.

## Common Settings for Activities

### Alert Agent When Activity Is Assigned

Use this setting to decide if an alert should be displayed to agents when new activities are assigned to them. If the Agent Console is minimized, or not in focus, an alert is displayed in the bottom right hand side section of the screen. This setting does not apply to chat activities.

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Enumeration
- ▶ Default value: Always
- ▶ Value options:
  - **Never:** Activity is displayed in the Inbox, but no alert is displayed to agents.
  - **Always:** An alert is displayed every time an activity is assigned to the agent.
  - **When the agent has no open activity:** The alert is displayed only when the agent has no activities in the inbox.
- ▶ Can be reset at lower level: Yes

### Allow Agent to Associate a New Outbound Activity with a Queue

Use this setting to allow agents to associate an outbound activity with a queue upon creation.

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

- ▶ Can be reset at lower level: Yes

## Send Agent an Email When Activity Is Assigned

Use this setting to decide if an email notification should be sent to agents when new activities are assigned to them. This setting does not apply to chat activities.

- ▶ Type: Department settings group
- ▶ Subtype: Common
- ▶ Data type: Enumeration
- ▶ Default value: Never
- ▶ Value options:
  - Never: Email notifications will not be sent.
  - When Logged In: Email notifications will be sent only if the agent is logged in.
  - When not Logged in: Email notifications will be sent only if the agent is not logged in.
  - Always: Email notifications will always be sent whether the agent is logged in or not.
- ▶ Can be reset at lower level: Yes

## Alert Subject

Notifications can be sent to users when new activities are assigned to them. Use this setting to configure the subject of these notifications.

- ▶ Type: Department settings group
- ▶ Subtype: Common
- ▶ Data type: String
- ▶ Default value: You have received a new activity
- ▶ Value options: —
- ▶ Can be reset at lower level: No

## Alert Body

Notification can be sent to users when new activities are assigned to them. Use this setting to configure the message displayed in these notifications.

- ▶ Type: Department settings group
- ▶ Subtype: Common
- ▶ Data type: String
- ▶ Default value: You have received a new activity (id = ``activity\_id) from customer identified by ``contact\_point\_data
- ▶ Value options: —

- ▶ Can be reset at lower level: No

## Force Activity Categorization

Use this setting to ensure that agents assign categories to each activity before completing it. This setting does not apply to chat activities. For chat, use the [Chat - Force Activity Categorization](#) setting.

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

## Force Resolution Code

Use this setting to ensure that agents assign resolution codes to each activity before completing it. This setting does not apply to chat activities. For chat, use the [Chat - Force Resolution Code](#) setting.

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

## Email Activity Settings

### Include Message Header in Reply

With this setting you can decide the amount of header information that is displayed to agents in the Agent Console. This information is available in the Activity pane.

- ▶ Type: Department settings group
- ▶ Subtype: User
- ▶ Data type: Enumeration
- ▶ Default value: Basic
- ▶ Value options: None, Basic, Complete
- ▶ Can be reset at lower level: Yes

## Add Contact Point on Compose

In this setting you can decide if the email address specified in the **To** field of a composed email activity should be added to the customer profile associated with the case to which the activity belongs.

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

## Language Detection Threshold (KB)

Use this setting to define the amount of data that is required to be present in activity before the application is able identify the language of the activity.

- ▶ Type: Partition settings group
- ▶ Subtype: Activity
- ▶ Data type: Integer
- ▶ Default value: 10
- ▶ Minimum value: 1 KB
- ▶ Maximum value: 1024 KB

## 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.
- ▶ Can be reset at lower level: No

## Service Email and Phone Activities at the Same Time

Use this setting to determine if agents can be assigned new email activities, as well continue to work on email activities that 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. 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. 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 pick or pull emails from queues or other agents. Agents cannot create outbound emails while they are on a phone call.
- ▶ 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.
- ▶ Can be reset at lower level: No

## Chat Activity Settings

### Chat - Force Activity Categorization

Use this setting to ensure that agents assign categories to each chat activity before completing it.

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

### Chat - Force Resolution Code

Use this setting to ensure that agents assign resolution codes to each chat activity before completing it.

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

## Inbox Settings

---

### Common Settings for Inboxes

#### 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: —
- ▶ Can be reset at lower level: Yes

## Main Inbox Settings

### Inbox Sort Column

In this setting, define the column that is used to sort items in the Activity and Cases folders in the Agent Console. Use the “Inbox sort order” setting to define whether the items are sorted in the ascending or descending order. This setting does not apply to the Chat Inbox. For chat, use the [Chat - Inbox Sort Column](#) setting.

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Enumeration
- ▶ Default value: Activity ID
- ▶ Value options: Activity ID, Activity Priority, Case ID, Contact point, Department name, Subject, When created, Activity type, Activity sub status
- ▶ Can be reset at lower level: Yes

### Inbox Sort Order

Use this setting to define the order - ascending or descending, in which items appear in the Activity and Cases folders in the Agent Console. Use the “Inbox sort column” setting to determine the column by which items are sorted. This setting does not apply to the Chat Inbox. For chat, use the [Chat - Inbox Sort Order](#) setting.

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Enumeration
- ▶ Default value: Ascending
- ▶ Value options: Ascending, Descending
- ▶ Can be reset at lower level: Yes

### Email - Enable Sound Alert

Use this setting to define if you want the system to play a sound when an email is assigned to the agent. To minimize distraction, the alert sounds only when the focus is not in the main inbox.

- ▶ Type: Department settings group
- ▶ Subtype: General
- ▶ Data type: Enumeration
- ▶ Default value: Yes

- ▶ Value options: No, Yes
- ▶ Can be reset at lower level: No

## Chat Inbox Settings

### Chat - Inbox Sort Column

In this setting, define the column that is used to sort items in the Chat Inbox in the Agent Console. Use the “Chat - Inbox sort order” setting to define whether the items are sorted in the ascending or descending order.



**Important:** If you specify a column that is not part of the agent's inbox list or if there is a tie between two activities with the same value for the sorting column, the inbox will then be sorted by the shortcut key.

---

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Enumeration
- ▶ Default value: Key
- ▶ Value options: Key, Activity ID, Case ID, When Created, Customer name, Subject, Activity sub status, Queue name
- ▶ Can be reset at lower level: Yes

### Chat - Inbox Sort Order

Use this setting to define the order - ascending or descending, in which items appear in the Chat Inbox in the Agent Console. Use the “Chat - Inbox sort column” setting to determine the column by which items are sorted.

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Enumeration
- ▶ Default value: Descending
- ▶ Value options: Ascending, Descending
- ▶ Can be reset at lower level: Yes

### Chat - My Monitor - Activity Refresh Interval (Seconds)

In this setting configure the time interval (in seconds) at which the chat activities are refreshed in the My Monitor's folder of the supervisor's Advisor Desktop. The following details of chat activities are refreshed - the list of activities for the queue or agent being monitored; the transcript of chats that the supervisor has not joined and is monitoring passively.

- ▶ Type: Department settings group

- ▶ Subtype: Activity
- ▶ Data type: Integer
- ▶ Default value: 30
- ▶ Minimum value: 30
- ▶ Maximum value: 600
- ▶ Can be reset at lower level: No

## Spelling and Blocked Words Settings

### 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

### 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

### 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

## 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 Administration Console. For details, see [“Adding Blocked Words” on page 227](#).

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

## 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 Administration Console. For details, see [“Adding Blocked Words” on page 227](#).

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

## 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

## 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

## 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

## Search Settings

---

### 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 launched from 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 decide the maximum number of search results to be displayed when an agent uses new activity shortcuts to create activities.

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

## Knowledge Base Settings

---

### KB Primary Language

Use this setting to specify the language in which content is added in the knowledge base.

- ▶ 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

## Chat Settings

---

### Chat Auto-Pushback Settings

The chat auto-pushback feature allows you to pushback chat activities to the queue, if the agents do not click on the new chats assigned to them in the configured time (default value is 2 minutes). You can also automatically mark the agents unavailable when chats are pushed-back from their inbox.

To view or configure the chat auto-pushback settings, click the **Assistance** button in the **Value** field of the setting.

### Enable Auto-Pushback of Chats

Use this setting to decide if new chats assigned to agents should be automatically pushed back from the agent's inbox if they do not click on the activity in the time defined in the **Expiry time for auto-pushback for chats** setting.

Type: Partition settings group

Subtype: Chat

Data type: Enumeration

Default value: Yes

Value options: Yes, No



## **Expiry Time for Auto-Pushback for Chats (Minutes)**

In this setting, define the time, in minutes, after which the new chat assigned to the agent will be automatically pushed back from the agent's inbox, if the agent does not click on the chat in the defined time.

- ▶ Type: Partition settings group
- ▶ Subtype: Chat
- ▶ Data type: Integer
- ▶ Default value: 2
- ▶ Minimum value: 1
- ▶ Maximum value: 210

## **Make Agent Unavailable on Auto-Pushback of Chats**

Use this setting to define if agents should be made unavailable after a chat is pushed back automatically from the agent's inbox. By default this setting is disabled.

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

## **Chat Agent Session Settings**

### **Chat - Agent Chat Message Maximum Length**

Use this setting to determine the maximum length of messages sent by agents to customers.

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Integer
- ▶ Default value: 800
- ▶ Minimum value: 60
- ▶ Maximum value: 2000
- ▶ Can be reset at lower level: No

## Show Smiley in Agent Chat Toolbar

The toolbar in the Chat pane has a **Smiley** button that can be used to add emoticons in the chat messages. Use this setting to determine if this **Smiley** button should be available to the agents.

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

## Chat - Display Timestamp in Agent Chat Console

Use this setting to decide if the timestamp should be displayed with the chat messages in the Agent Console. This setting applies to open chat activities only.

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

## Chat - Display Timestamp in Completed Chat Transcript

Use this setting to decide if the timestamp should be displayed with the chat messages in the Agent Console. This setting applies to completed chat activities only.

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

## Chat - Disable Typing Area and Page Push Area on Customer Exit

Use this setting to disable Page Push and the typing area of the Chat pane for agents and supervisors, when a customer leaves the chat session.

- ▶ Type: Department settings group
- ▶ Subtype: Common

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

## Chat - Enable Sound Alert

Use this setting to decide if you want play a sound alert to draw the agent's attention to the chat inbox when a new chat is assigned to the agent, or a new message is sent by the customer. The sound alert is played only when the Agent Console is minimized or not in focus. If the agent is already working in the Agent Console, the sound alert is not played.

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

## Chat - Reason for Transfer

Use this setting to decide if you want agents to always assign a transfer code to chat activities while transferring chats to other users, queues, or departments.

- ▶ Type: Department settings group
- ▶ Subtype: Activity
- ▶ Data type: Enumeration
- ▶ Default value: Optional
- ▶ Value options:
  - Optional
  - Required
- ▶ Can be reset at lower level: No

## Enable Conversation Stream

Use this setting to enable the Conversation View in the Chat pane for agents. When the Conversation View is active, agents are able to scroll up in the Chat pane and view chat conversations the customer has previously had with any agents. When disabled, the Chat pane only shows the messages sent and received for the current chat activity. This setting is enabled by default for new installations of the application, however, it must be manually enabled on systems that have upgraded from a previous version of the application.

- ▶ Type: Department settings group
- ▶ Subtype: Chat

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

## Chat - Agent Availability Buffer Value

This setting determines the minimum number or percentage of agents that have to be available for a chat queue mapped to an MRD, before a chat offer is presented to a website visitor. When a website visitor becomes eligible for a chat offer, the system checks the number or percentage of available agents, whose assigned skill groups match those of the queue, against the value configured in this setting. If this condition is met, the chat offer is presented to the website visitor.

- ▶ Type: Department settings group
- ▶ Subtype: Chat
- ▶ Data type: Integer
- ▶ Default value: 5
- ▶ Minimum value: —
- ▶ Maximum value: —
- ▶ Can be reset at lower level: No

## Chat - Agent Availability Check Mechanism

This setting determines whether the value set in the “Chat - Agent Availability Buffer Value” setting is an absolute value or a percentage of the total number of agents that belong to the chat queue mapped to an MRD and have the required skill groups.

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

# 4 Users

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

This chapter will assist you in understanding users, groups, roles, and actions and how to set them up according to your business requirements.

## 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.

Users operate at three levels:

- ▶ System level user: This user is typically the system administrator of the system who manages the system partition resources, such as services, loggers, handlers, and so on.
- ▶ Partition level user: This user is typically the system 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, and the agents handle customer interactions, such as chat, emails, phone calls, and so on. Department level users are ECE users that are mapped to an Unified CCE user. Activities to this user are assigned from Unified CCE queues only. For more details on queues, see *Enterprise Chat and Email Administrator's Guide to Routing and Workflows*

If an ECE user's attributes are modified in Unified CCE, when the ECE user is selected in the Administration Console, the modifications are automatically retrieved and synchronized in ECE.

Two users are created during the installation:

1. System Administrator: The first system user, created during installation, is a user called `System Administrator`. Assigned the System Administrator role, this user sets up system resources and creates one or more system-level users.
2. Partition Administrator: The first business user, created during installation, is a user called `Partition Administrator`. Assigned the Partition Administrator role, this user manages partition users and settings and creates more partition users as well as one or more department-level users to manage department resources.

### 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 nothing but 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 the department, and has access to the Administration console. You will find that there are two types of administrators that the system allows you to create; Partition Administrator and Department Administrator. Let us see the difference between these two roles. A partition administrator has to be created while installing the application, but additional partition administrators can be created later. The partition administrator is responsible for both her partition and for the departments contained within her partition. To know more about the role of a partition administrator, see ["Partition Administrator" on page 109](#).

A department administrator is imported into the system by the partition administrator from Unified CCE, and has the authority to create all the resources for the department he administers. For example, setting rules for incoming and outgoing activities through workflows, creating classifications, dictionaries, users, and assigning permissions to the users to perform various tasks.

- ▶ **Agent:** An agent is a person who handles customer queries, who is directly in contact with the customer. He has access to the Agent console. Agents are imported into the system by the partition administrator from Unified CCE.
- ▶ **Agent (Read Only):** An agent (read only) will have access to the Agent console, but he will not be able to compose replies for the customer queries. He 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 Administration console interface. On the left is a navigation tree with categories like Administration, Departments, and Service. The main area is split into two panes. The top pane, 'List: Users', contains a table of users. The bottom pane, 'Properties: kon', shows the 'Relationships' tab with 'Available roles' and 'Selected roles' lists.

User Nam...	Firs...	Last...	Email Address	Departme...	Unified C...	Manager	User Status
gagan	Gag...	Kaur		Home	Yes		Not logge...
hgupta	Him...	Gupta		Home	Yes		Not logge...
kon	Kons...	Gol...		Home	Yes		Not logge...
manju	Manju	Ram...		Home	Yes		Logged in

Available roles		Selected roles	
Name ^		Name ^	
Administrator		Agent	
Agent (Read Only)			
Supervisor			
Supervisor (Read Only)			
Wrap-up			

*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.

## 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 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 Unified 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 Unified CCE 12.0(1), agents cannot pick activities while working on non-interruptible chats or voice calls.

---

- ▶ Agents with the Administrator Role and Supervisor 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) and are integrated with Unified CCE 12.0(1) or a later version:

**As a part of blended routing enhancements, the Pick/Pull node must be added to existing Unified CCE scripts for inbound emails and chats, as well as outbound emails.**

**Also, appropriate registry edits needs to be made on the Unified CCE system for agents to pick, pull, or transfer activities. For details on the specific blended routing changes that are required, refer to the appropriate Unified CCE scripting and configuration guide.**

---

- ▶ 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 104](#).

### 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 45](#)) setting is enabled, agents can transfer activities to queues of other departments.
- ▶ If the **Allow email transfer to agents who are not available** ([page 45](#)) 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 45](#)) 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 45) 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** (page 47) setting.
- ▶ Based on the **Maximum assignment beyond concurrent task limit** (page 47) 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 45) 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?

Now that you already know that every default role has a set of permissible actions assigned to them, you must be curious to find out what these actions are. To learn more about them look at the following tables.

## System Administrator

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

Resource Name	Actions Permitted
System Resource	View Administrator, View System
User	Create, Own, View, Edit, Delete
User Group	Create, Own, View, Edit, Delete
User Role	Create, View, Edit, Delete
Partition	Administer, Own, View, Edit
Monitor	Create, Run, Edit, Delete
Messaging	Create message, Delete message
Instance	Create, View, Edit, Delete, Start, Stop
Process	Create, View, Edit, Delete, Start, Stop
Host	View, Edit, Delete, Start, Stop
Handler	View, Edit
Logger	Edit, View
Preference group	View, Delete, Edit, Create

*Actions assigned to the System Administrator role*

## 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.

Resource Name	Actions Permitted
Administration Console	View
Supervision Console	View
Agent Console	View
Reports Console	View
System Console	View
Knowledge Base Console	View
Tools Console	View
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
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

<b>Resource Name</b>	<b>Actions Permitted</b>
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
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
Agent Console	View
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 <b>New Activity</b> button in the Main Inbox toolbar.
	Complete	Enables the <b>Complete</b> button in the Reply pane toolbar when working on email activities, custom activities, or tasks. Also enables the <b>Send &amp; Complete</b> button in the Reply pane toolbar if the <b>Send Email</b> action is also assigned to the agent.
	Pin	Enables the <b>Pin/Unpin</b> 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 <b>Pull</b> button in the Main Inbox toolbar. To be able to pull activities using this button, the agent needs: <ul style="list-style-type: none"> <li>▶ <b>Pull Activities</b> action for routing queues.</li> <li>▶ <b>Pull Activities</b> permission on queues.</li> </ul> For chats, the following action is also required: <ul style="list-style-type: none"> <li>▶ <b>Pull Next Chat Activity</b> action for chats.</li> </ul>
	Pull Selected Activities	Enables the <b>Pick</b> 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"> <li>▶ <b>Pull Activities</b> action for routing queues.</li> <li>▶ <b>Pull Activities</b> action for users.</li> <li>▶ <b>Pull Activities</b> permission on queues.</li> <li>▶ <b>Pull Activities</b> permission on users.</li> </ul>
	Transfer Activities	Enables the <b>Transfer</b> 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"> <li>▶ <b>Transfer Activities</b> action for routing queues.</li> <li>▶ <b>Transfer Activities</b> action for users.</li> <li>▶ <b>Transfer Activities</b> permission on queues.</li> <li>▶ <b>Transfer Activities</b> permission on users.</li> </ul>
	Assign Classification	Enables the <b>Save</b> 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 <b>Save</b> button in the Information pane, Case section. The <b>Case status</b> field is enabled only if the agent has the <b>Close Case</b> action.
	Close Case	Allows an agent to close an open case. It enables the <b>Close Case</b> button in the Inbox pane toolbar (Inbox Tree pane > My Work > Cases > My Cases > Open). If the agent has the <b>Edit case</b> action, it also enables the <b>Case status</b> 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 <b>Change Case</b> 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 <b>Create Case</b> button in the Information pane, Case section.

Resource Name	Actions Permitted	Description
Chat	Complete Chat Activity	Enables the <b>Complete</b> button in the Chat pane toolbar.
	Leave Chat Activity	Enables the <b>Leave</b> 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 <b>Pull</b> 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"> <li>▶ <b>Pull Next Activities</b> action for activities</li> <li>▶ <b>Pull Activities</b> action for routing queues</li> <li>▶ <b>Pull Activities</b> permission on queues</li> </ul>
	Transfer Chat Activity	Enables the <b>Transfer</b> 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"> <li>▶ <b>Transfer Activities</b> action for routing queues</li> <li>▶ <b>Transfer Activities</b> action for users</li> <li>▶ <b>Transfer Activities</b> permission on queues</li> <li>▶ <b>Transfer Activities</b> permission on users</li> </ul>

Resource Name	Actions Permitted	Description
Customer	Create	Allows agents to create new customers. It enables the <b>Save</b> button when an agent creates a new customer (by clicking the <b>New</b> 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 <b>New Activity</b> button in the Inbox pane toolbar), it displays the <b>New</b> option in the <b>Customer</b> field.
	Edit	Allows an agent to edit the details of a customer. It enables the <b>Save</b> button in the Information pane > Customer section toolbar.
	Delete	Allows an agent to delete a customer associated with an activity. It enables the <b>Delete</b> button in the Information pane, Customer section toolbar.
	Change Customer	Allows an agent to change the customer associated with an activity. Displays the <b>Change customer</b> 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 <b>New</b> 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 <b>Save</b> 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 <b>Delete</b> 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 <b>New</b> 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 <b>Save</b> 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 <b>Delete</b> 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 <b>New</b> 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 <b>Save</b> 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 <b>Delete</b> 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 <b>Restore</b> button in the View Attachments window, which opens when an agent double-clicks the <b>Attachment</b> icon in the Inbox List pane.
	Delete	It allows agents to delete blocked attachments. Unblocked attachments cannot be deleted. It enables the <b>Delete</b> button in the View Attachments window, which opens when an agent double-clicks the <b>Attachment</b> icon in the Inbox List pane.

Resource Name	Actions Permitted	Description
Filter Folder	Create	Enables the <b>New</b> and <b>Properties</b> 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 <b>Delete</b> 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 <b>View Folder</b> 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 <b>View Folder</b> permission on those folders.
	Add Notes	Allows agents to view, delete, and add notes. It enables the <b>Notes</b> button.
Macro	View	Allows agents to view and use macros in emails, chats, tasks, and custom activities. It enables the <b>Add macro</b> button in the reply pane.
Notes	View	Allows an agent to view notes associated with cases, activities, customers, and customer associations. It displays the <b>View notes</b> option in the Notes window, which can be accessed using the <b>Notes</b> button from the following panes: <ul style="list-style-type: none"> <li>▶ Main Inbox toolbar</li> <li>▶ Chat Inbox toolbar</li> <li>▶ Reply pane</li> <li>▶ Chat pane</li> <li>▶ Information pane, in the following sections: Activity, Case, History, and Customer.</li> </ul>
	Add	Allows an agent to add notes to cases, activities, customers, and customer associations. It displays the <b>Add notes</b> option in the Notes window, which can be accessed using the <b>Notes</b> button from the following panes: <ul style="list-style-type: none"> <li>▶ Main Inbox</li> <li>▶ Chat Inbox</li> <li>▶ Reply pane</li> <li>▶ Chat pane</li> <li>▶ Information pane, in the following sections: Activity, Case, History, and Customer.</li> </ul> <p>If an agent has the <b>View Notes</b> action, it also enables the <b>Add</b> button in the Notes window. It displays the <b>Add notes</b> option in the Notes window, which can be accessed using the <b>Notes</b> button from the following panes:</p> <ul style="list-style-type: none"> <li>▶ Main Inbox</li> <li>▶ Chat Inbox</li> <li>▶ Reply pane</li> <li>▶ Chat pane</li> <li>▶ Information pane, in the following sections: Activity, Case, History, and Customer.</li> </ul>
	Delete	Allows an agent to delete the notes associated with cases, activities, customers, and customer associations. It enables the <b>Delete button</b> in the Notes window. The Notes window can be accessed using the <b>Notes</b> button from the following panes: <ul style="list-style-type: none"> <li>▶ Main Inbox</li> <li>▶ Chat Inbox</li> <li>▶ Reply pane</li> <li>▶ Chat pane</li> <li>▶ Information pane, in the following sections: Activity, Case, History, and Customer.</li> </ul> <p>The Notes window can only be accessed by agents with the <b>View Notes</b> 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"> <li>▶ <b>Pull Next Activities</b> or <b>Pull Selected Activities</b> action for activities</li> <li>▶ <b>Pull Activities</b> permission on routing queues</li> </ul> <p>For chats, the following action is also required:</p> <ul style="list-style-type: none"> <li>▶ <b>Pull Next Chat Activity</b> action for chats</li> </ul>
	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"> <li>▶ <b>Transfer Activities</b> action for activities</li> <li>▶ <b>Transfer Activities</b> permission on queues</li> </ul>
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"> <li>▶ <b>Pull Selected Activities</b> action for activities</li> <li>▶ <b>Pull Activities</b> permission on users</li> </ul>
	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"> <li>▶ <b>Transfer Activities</b> action for activities</li> <li>▶ <b>Transfer Activities</b> permission on users</li> </ul>

*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
Agent Console	View
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 <b>Note:</b> These actions provide access to the Agent Console, Reports Console, and Supervision Console
Report	Create, Delete, View, Run, Edit, Schedule <b>Note:</b> With these actions, users can manage reports from the Reports Console.
Monitor	Create Edit, Delete, Run <b>Note:</b> 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 <b>Note:</b> 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
<b>Note:</b> 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
Supervision Console	View
Agent Console	View
Reporting Console	View
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

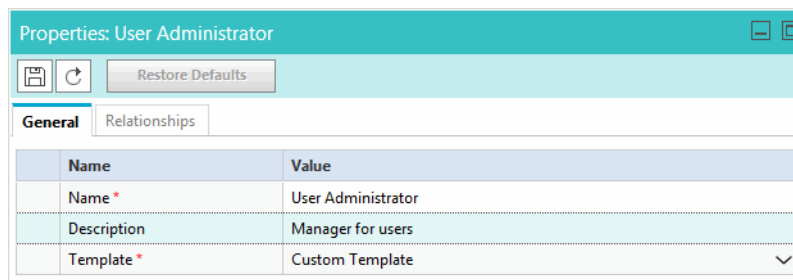
This section talks about:

- ▶ [Creating User Roles on page 122](#)
- ▶ [Creating User Subroles on page 124](#)
- ▶ [Copying User Roles on page 125](#)
- ▶ [Restoring User Roles on page 125](#)
- ▶ [Deleting User Roles and Subroles on page 126](#)


## Creating User Roles

### To create a user role:

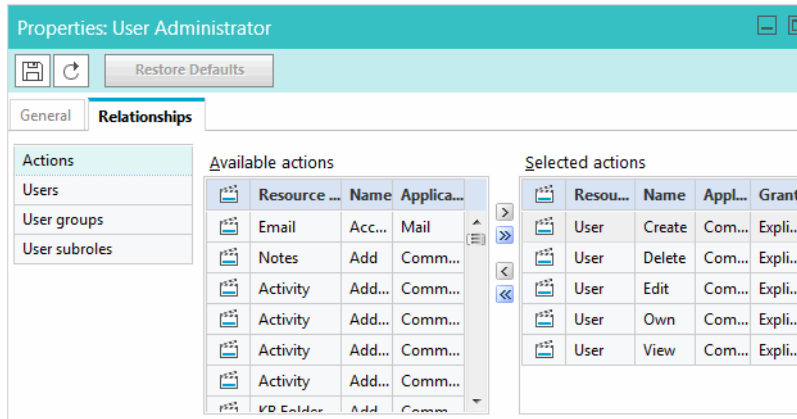
1. In the Tree pane, browse to the **Users** node. Based on where you want to create a user role, do one of the following:
  - If you are a system administrator, go to the system partition and browse to **Administrator > Partition: *Context\_Root\_Name* > User > Roles**.
  - If you are a partition administrator, go to the business partition and browse to **Administrator > Partition: *Partition\_Name* > User > Roles**.
  - If you are a department administrator, browse to **Administration > Departments > *Department\_Name* > User > Roles**.
2. In the List pane toolbar, click the **New**  button.
3. In the Properties pane, 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 or select **Custom Template** to start with a blank role. The template cannot be changed once you save the role.



*Set general properties*

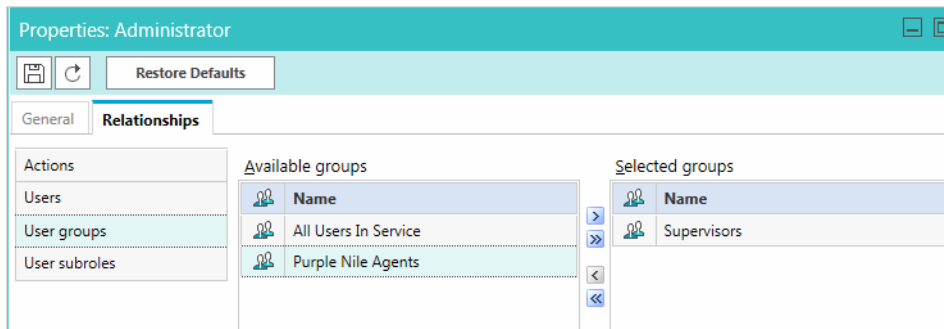
4. Click the **Save**  button. This enables the Relationships tab.
5. Next, go to the Relationships tab and do the following.

- 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.



*Select actions*

- 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.

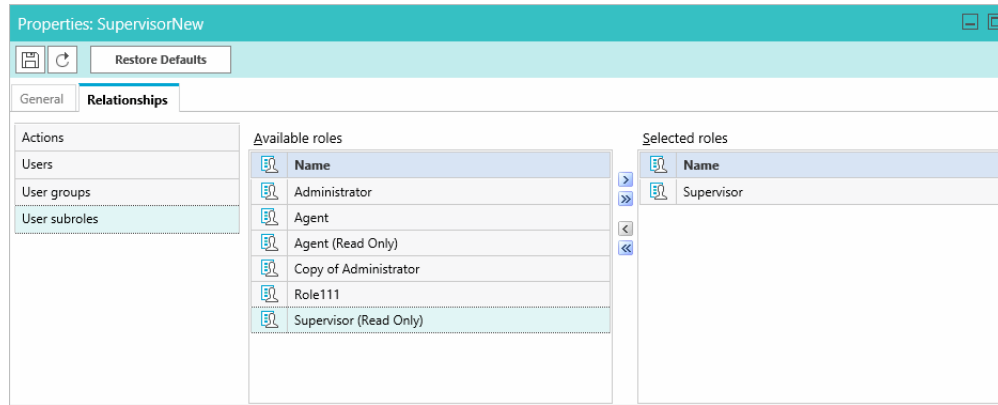



*Assign the role to user groups*

- 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 [“Creating User Subroles” on page 124](#).

Select subroles



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

The role that you create is displayed in the List pane.

## Creating 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.

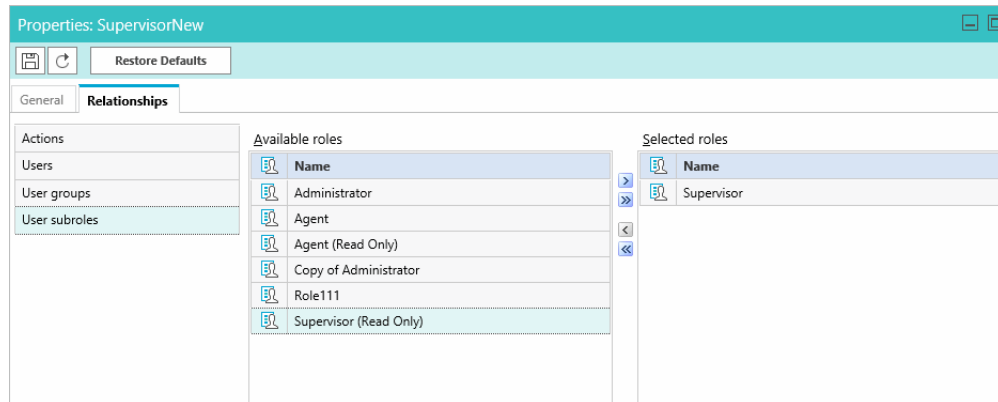
A role can be a subrole of more than one roles.

### To create a subrole:

1. In the Tree pane, browse to the **Users** node. Based on where you want to create a user subrole, do one of the following:
  - If you are a system administrator, go to the system partition and browse to **Administrator > Partition: *Context\_Root\_Name* > User > Roles**.
  - If you are a partition administrator, go to the business partition and browse to **Administrator > Partition: *Partition\_Name* > User > Roles**.
  - If you are a department administrator, browse to **Administration > Departments > *Department\_Name* > User > Roles**.
2. Select the role for which you want to create a subrole.

- If you want to use an existing role as a subrole, go to Relationships tab and in the User subroles section, select from the available roles.

Select subroles



- If you want to create a new subrole, follow steps 2 to 5 in “[Creating User Roles](#)” on page 122. When you create a role under an existing role, it automatically becomes the subrole of the role.

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 Tree pane, browse to the Users node. Based on where you want to copy a user role, do one of the following:
  - If you are a system administrator, go to the system partition and browse to **Administrator > Partition: *Context\_Root\_Name* > User > Roles**.
  - If you are a partition administrator, go to the business partition and browse to **Administrator > Partition: *Partition\_Name* > User > Roles**.
  - If you are a department administrator, browse to **Administration > Departments > *Department\_Name* > User > Roles**.
2. In the List pane, select the role you want to copy.
3. In the List pane toolbar, click the **Copy** button.
4. A copy of the role is created. The copied role retains the template of the original role.

## Restoring User Roles

When you restore a role, the list of actions associated with the role is reset to its default state. All subroles associated with the role are also removed from the role. You can create a copy of the role before restoring it to its default state. Note that the copied role is not assigned to any users or user groups.

### To restore a role:


1. In the Tree pane, browse to the Users node. Based on where you want to restore a user role, do one of the following:
  - If you are a system administrator, go to the system partition and browse to **Administrator > Partition:** *Context\_Root\_Name* > **User > Roles.**
  - If you are a partition administrator, go to the business partition and browse to **Administrator > Partition:** *Partition\_Name* > **User > Roles.**
  - If you are a department administrator, browse to **Administration > Departments > Department\_Name** > **User > Roles.**
2. In the List pane, select the role you want to restore to its default state.
3. In the Properties pane toolbar, click the **Restore Defaults** button.
4. A prompt is displayed to confirm the restore action. In this prompt, you get an option to create a copy of the role before restoring it.

## 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 Tree pane, browse to the **Users** node. Based on where you want to delete the user role from, do one of the following:
  - If you are a system administrator, go to the system partition and browse to **Administrator > Partition:** *Context\_Root\_Name* > **User > Roles.**
  - If you are a partition administrator, go to the business partition and browse to **Administrator > Partition:** *Partition\_Name* > **User > Roles.**
  - If you are a department administrator, browse to **Administration > Departments > Department\_Name** > **User > Roles.**
2. In the List pane, select the role or subrole you want to delete.
3. In the List pane toolbar, click the **Delete**  button.

You will be prompted to confirm the deletion. Click **OK** to delete the role.


## 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 34.](#)

## Deleting User Groups

### To delete a user group:

1. In the Tree pane, browse to the **Users** node. Based on from where you want to delete the user group, do one of the following.
  - If you are a system administrator, go to the system partition and browse to **Administrator > Partition: *Context\_Root\_Name* > User > Roles**.
  - If you are a partition administrator, go to the business partition and browse to **Administrator > Partition: *Partition\_Name* > User > Roles**.
  - If you are a department administrator, browse to **Administration > Departments > *Department\_Name* > User > Roles**.
2. In the List pane, select the user group you want to delete.
3. In the List pane toolbar, click the **Delete**  button.

## Managing Users

System and partition administrators are created in the system during the installation and additional system or partition 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 35.

This section talks about:

- ▶ [Creating System Administrators on page 127](#)
- ▶ [Creating Partition Administrators on page 131](#)
- ▶ [Editing Department Users on page 135](#)
- ▶ [Deleting Users on page 140](#)

## Creating System Administrators




---

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

---

### To create a system administrator:

1. Log in to the system partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition: *Context\_Root\_Name* > User > Users**.
3. In the List pane toolbar, click the **New**  button
4. In the Properties pane, on the General tab, set the following:
  - a. In the General section, provide the following details.

- **User name:** Type a name for the user. This name is used by the user to log in to the application.
- **Password:** Type the password.

The following fields are optional.

- **Title**
- **First name**
- **Middle name**
- **Last name**
- **Suffix**
- **User status:** The status of users cannot be adjusted here. The following statuses can be displayed: Enabled, Disabled, Logged in, and Not logged in.
- **Screen name:** This field is not in use.
- **Peripheral:** This field is disabled.
- **Unified CCE Agent Login Name:** This field is disabled.

Name	Value
Title	
First name	
Middle name	
Last name	
Suffix	
User name *	
Password	
User status	Enabled
Screen name	
Peripheral	
Unified CCE Agent Login Name	

*Set general properties*

- b. Next, go to the Business section, and provide the following information. All the fields are optional.
- **Employment status:** The options available are - Customer, Employee, Partner, and Reseller.
  - **Company**
  - **Division**
  - **Department**
  - **Job title**
  - **Work address line 1**
  - **Work address line 2**
  - **Work city**
  - **Work state**
  - **Work zip code**
  - **Work country**



- **Work phone**
- **Extension**
- **Work pager**
- **Work fax**
- **Email address**
- **Mobile number 2**
- **ACD name**
- **Hire date**

The screenshot shows a window titled 'Properties: Thomas' with a teal header. Below the header are icons for save and refresh. There are three tabs: 'General' (selected), 'Relationships', and 'Permissions'. The 'General' tab contains a table with the following data:

General	Name	Value
Business	Employment status	Employee
Personal	Company	
Miscellaneous	Division	
	Department	Support
	Job title	System Manager
	Work address line 1	
	Work address line 2	
	Work city	Sunnyvale
	Work state	California
	Work zip code	94056
	Work country	

*Set business properties*

- c. Next, go to the Personal section, and provide the following information. All the fields are optional.
- **Home address line 2**
  - **Home city**
  - **Home state**
  - **Home zip code**
  - **Home country**
  - **Home phone**
  - **Home pager**
  - **Home fax**
  - **Mobile number 3**
  - **Secondary email address**

General	Name	Value
Business	Home address line 2	
Personal	Home city	San Jose
Miscellaneous	Home state	California
	Home zip code	95634
	Home country	
	Home phone	
	Home pager	
	Home fax	
	Mobile number 3	
	Secondary email address	

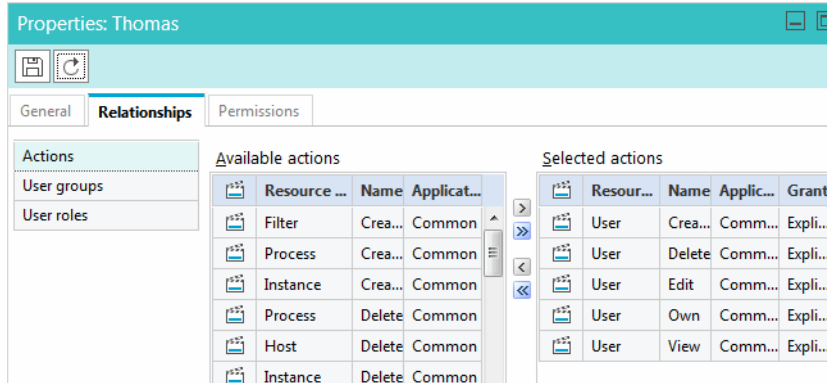
*Set personal properties*

- d. Finally, go to the Miscellaneous section, and provide the following information. All the fields are optional.
- **Primary language**
  - **Gender**
  - **Creation date:** This field displays the name of the user who created the user. The value is populated automatically when the user is saved and it cannot be changed.
  - **Created by:** This field displays the date and time when the user is created. The value is populated automatically when the user is saved and it cannot be changed.
  - **Social Security Number**


General	Name	Value
Business	Primary language	English
Personal	Gender	M
Miscellaneous	Creation date	12/27/2014 05:12 PM
	Created by	sa
	Social Security Num...	

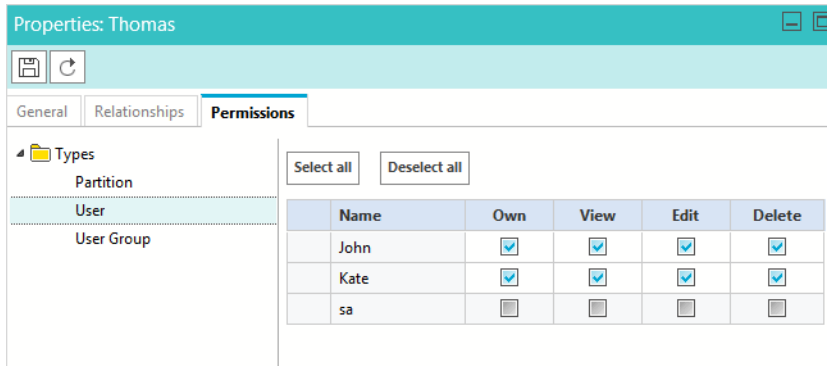
*Set miscellaneous properties*

5. Next, go to the Relationships tab, and select the Actions section. View the list of actions assigned to the user. Here you can assign the necessary actions to the user. You can identify how actions are assigned from the Grant field in the Selected actions section. The actions assigned explicitly show the value “Explicit”.



Select actions

6. Click the **Save**  button to enable the various options in the Permissions tab.
7. On the Permissions tab, assign permissions for the following objects.
  - **Partition:** Own, View, Edit, Administer
  - **User:** Own, View, Edit, Delete
  - **User group:** Own, View, Edit, Delete, Own, View Edit, Delete



Set permissions


8. Click the **Save**  button.

## Creating Partition Administrators



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

### To create a partition administration:

1. Log in to the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition: *Partition\_Name* > User > Users**.
3. In the List pane toolbar, click the **New**  button.
4. In the Properties pane, on the General tab, set the following:

- a. In the General section, provide the following details:
- **User name:** Type a name for the user. This name is used by the user to log in to the application.
  - **Password:** Type the password.

The following fields are optional.

- **Title**
- **First name**
- **Middle name**
- **Last name**
- **Suffix**
- **User status:** The status of users cannot be adjusted here. The following statuses can be displayed: Enabled, Disabled, Logged in, and Not logged in.
- **Screen name:** This field is not in use.
- **Peripheral:** This field is disabled.
- **Unified CCE Agent Login Name:** This field is disabled.

The screenshot shows a window titled 'Properties: pa' with three tabs: 'General', 'Relationships', and 'Permissions'. The 'General' tab is active and displays a table with two columns: 'Name' and 'Value'. The table contains the following rows:

Name	Value
Title	▼
First name	Partition
Middle name	
Last name	Administrator
Suffix	
User name *	pa
Password	☰
User status	Logged in ▼
Screen name	
Peripheral	<Select> ▼
Unified CCE Agent Login Name	▼

*Set general properties*

- b. Next go to the Business section, and provide the following information. All the fields are optional.
- **Company**
  - **Division**
  - **Department**
  - **Job title**
  - **Email address**
  - **Work phone**
  - **Extension**
  - **Mobile number 1**
  - **Employment status:** The options available are - Customer, Employee, Partner, and Reseller.

Properties: Tony

General Relationships Permissions

General	Name	Value
Business	Company	TCS
Personal	Division	
Miscellaneous	Department	Support
	Job title	Department Manager
	Email address	tony@tcs.com
	Work phone	6504086523
	Extension	
	Mobile number 1	
	Employment status	Employee

*Set business properties*

- c. Next, go to the Personal section, and provide the following information. All the fields are optional.
- **Home address line 1**
  - **Home address line 2**
  - **Home city**
  - **Home state**
  - **Home zip code**
  - **Home phone**
  - **Mobile number 2**
  - **Secondary email address**

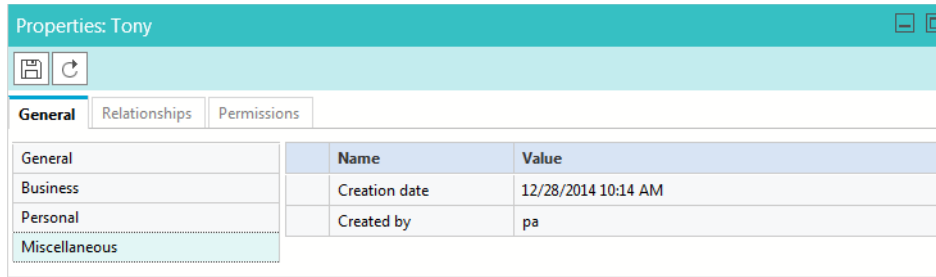
Properties: Tony

General Relationships Permissions

General	Name	Value
Business	Home address line 1	1839 Jackson Street
Personal	Home address line 2	
Miscellaneous	Home city	Mountain View
	Home state	CA
	Home zip code	95632
	Home phone	
	Mobile number 2	
	Secondary email address	

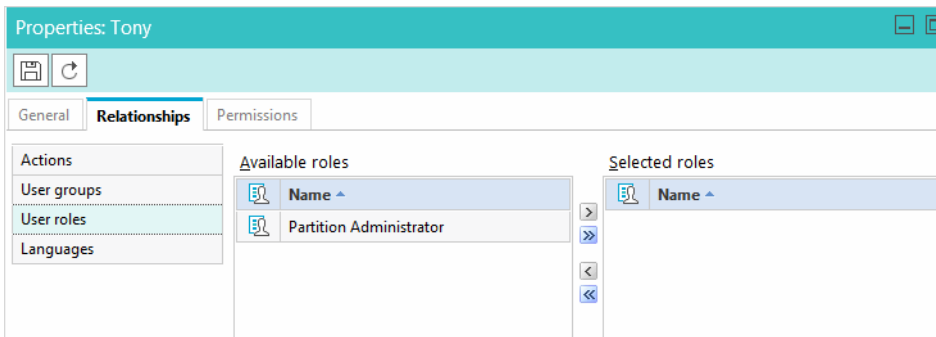
*Set personal properties*

- d. Finally, go to the Miscellaneous section. The following information is displayed.
- **Creation date:** This field displays the name of the user who created the user. The value is populated automatically when the user is saved and it cannot be changed.
  - **Created by:** This field displays the date and time when the user is created. The value is populated automatically when the user is saved and it cannot be changed.



View miscellaneous properties

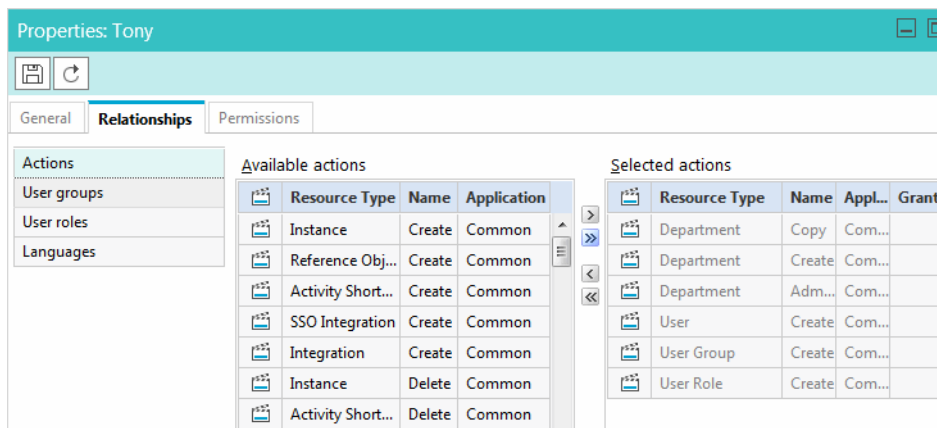
5. Next, go to the Relationships tab, and set the following.
  - e. Go to the User roles section and select the roles to be assigned to the user. If you want to view the actions that come as part of the selected role, save the user and go to the Actions tab to see the list of actions.



Select user roles


- f. Next, go to the Actions section, and view the list of actions assigned to the user. Here you can also assign additional actions to the user. You can identify how actions are assigned from the Grant field in the Selected actions section. The actions assigned explicitly show the value “Explicit”.

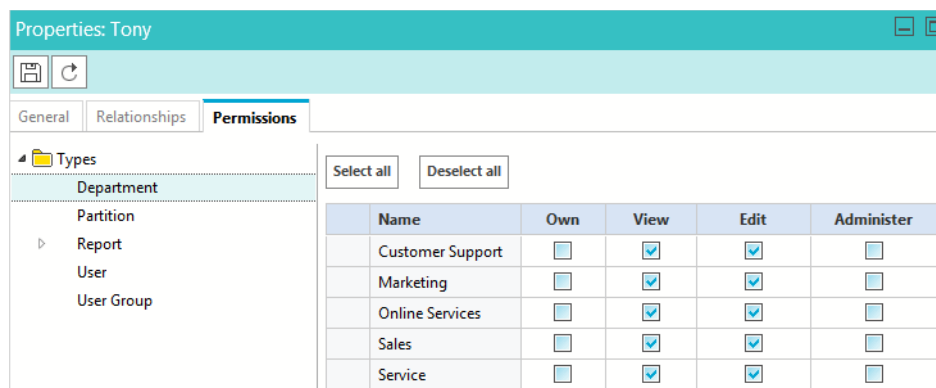
You should not assign actions directly to user. You should always use roles with the actions and assign the roles to the user. This makes user management easier.



Select actions

- g. Lastly, in the Languages section, select the primary KB language for the user.

6. Click the **Save**  button to enable the various options in the Permissions tab.
7. On the Permissions tab, assign permissions for the following objects.
  - **Department:** Own, View, Edit, Administer
  - **Partition:** Own, View, Edit, Administer
  - **Report:** View, Run, Edit, Delete, Schedule
  - **User:** Own, View, Edit, Delete
  - **User group:** Own, View, Edit, Delete, Own, View Edit, Delete



*Set permissions*

8. Click the **Save**  button.

## 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 34](#).

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 a department user:

1. In the Tree pane, browse to **Administration > Departments > *Department\_Name* > User > Users**.
2. In the List pane toolbar, select a user.
3. In the Properties pane, on the General tab, set the following.
  - a. In the General section, provide the following details.
    - **User name:** This name is used by the user to log in to the application. This is managed in Unified CCE and cannot be changed here.
    - **First name:** First name of the user. This is managed in Unified CCE and cannot be changed here.
    - **Last name:** Last name of the user. This is managed in Unified CCE and cannot be changed here.

- **Password:** Password of the user. This is managed in Unified CCE and cannot be changed here.
- **User status:** The status of users cannot be adjusted here. The following statuses can be displayed: Enabled, Disabled, Logged in, and Not logged in.
- **Screen name:** The screen name of the chat agent. This is the name displayed to chat customers in the Customer Console. You can change the value in this field. This is a required field for users who have the ECE Chat license. You can use the same screen name for more than one user in the system. The screen name must be at least 1 character and no more than 30 characters. The following characters can be used in screen names: Upper and lowercase alpha numeric characters (A-Z, 10-9); (@); space ( ); colon (:); period (.); underscore (\_); hyphen (-); ampersand (&); all characters above ASCII codeset 128.

If an ECE user group is mapped to a Unified CCE skill group, and the skill group attributes are modified in Unified CCE, when the ECE user group is clicked, the modifications are automatically retrieved and synchronized in ECE.

The following fields are optional.

- **Title**
- **Middle name**
- **Suffix**
- **Peripheral:** This field is disabled.
- **Unified CCE Agent Login Name:** This field is disabled.
- **External assignment:** This field is not in use and the value of the field cannot be changed.
- **Authentication Type:** The method in which the user accesses the application. This is managed in Unified CCE and cannot be changed here.

The screenshot shows a window titled 'Properties: alex2\_ch' with a teal header. Below the header are icons for save and refresh. The main content area has three tabs: 'General' (selected), 'Relationships', and 'Permissions'. Under the 'General' tab, there is a table with columns 'Name' and 'Value'. The table lists various user properties and their current values.

	Name	Value
Business	Title	
Personal	First name *	Alex2
Miscellaneous	Middle name	
Custom	Last name *	Ch
	Suffix	
	User name *	alex2_ch
	Password	
	Authentication type	Local login
	User status	Logged in
	External assignment	No
	Screen name	Alex2 Ch
	Peripheral	AgentPG_1
	Unified CCE Agent Login N...	alex2_ch

*Set general properties*

- Next go to the Business section, and provide the following information. All the fields are optional.



- **Company**
- **Division**
- **Department**
- **Job title**
- **Email address**
- **Work phone**
- **Extension**
- **Mobile number 1**
- **Employment status:** The options available are - Customer, Employee, Partner, and Reseller.

The screenshot shows a window titled 'Properties: Ashley' with a teal header. Below the header are icons for save and refresh. There are three tabs: 'General', 'Relationships', and 'Permissions'. The 'General' tab is active and contains a table with the following data:

General	Name	Value
Business	Company	TCS
Personal	Division	
Miscellaneous	Department	Support
Custom	Job title	User Manager
	Manager	
	Email address	ashley@tcs.com
	Work phone	4086502345
	Extension	
	Mobile number 1	
	Employment status	Employee

*Set business properties*

- c. Next, go to the Personal section, and provide the following information. All the fields are optional.
- **Home address line 1**
  - **Home address line 2**
  - **Home city**
  - **Home state**
  - **Home zip code**
  - **Home phone**
  - **Mobile number 2**
  - **Secondary email address**

The screenshot shows the 'Properties: Ashley' window with the 'General' tab selected. The 'Personal' section is highlighted in the left-hand category list. The main table displays the following data:

	Name	Value
Business	Home address line 1	1764 Curt Lane
Personal	Home address line 2	
Miscellaneous	Home city	Cupertino
Custom	Home state	California
	Home zip code	94056
	Home phone	
	Mobile number 2	
	Secondary email address	

*Set personal properties*

- d. Next, go to the Miscellaneous section. The following information is displayed.
  - **Creation date:** This field displays the name of the user who created the user. The value is populated automatically when the user is saved and it cannot be changed.
  - **Created by:** This field displays the date and time the user is created. The value is populated automatically when the user is saved and it cannot be changed.

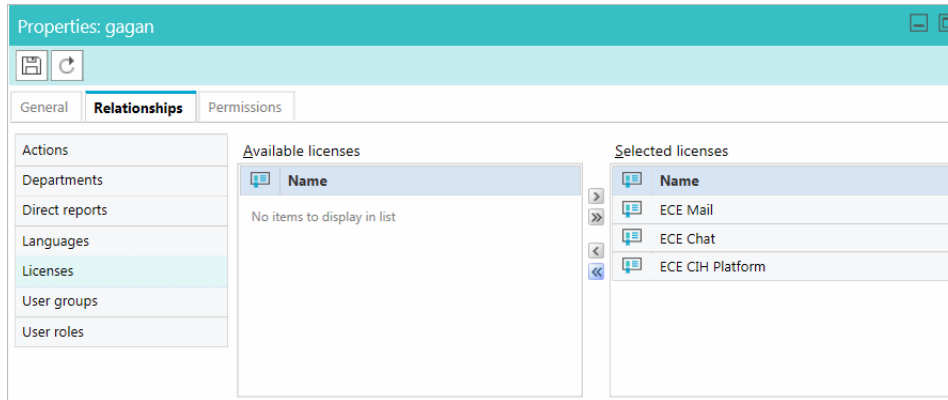
The screenshot shows the 'Properties: Ashley' window with the 'General' tab selected. The 'Miscellaneous' section is highlighted in the left-hand category list. The main table displays the following data:

	Name	Value
Business	Creation date	12/27/2014 04:16 PM
Personal	Created by	pa

*View miscellaneous properties*

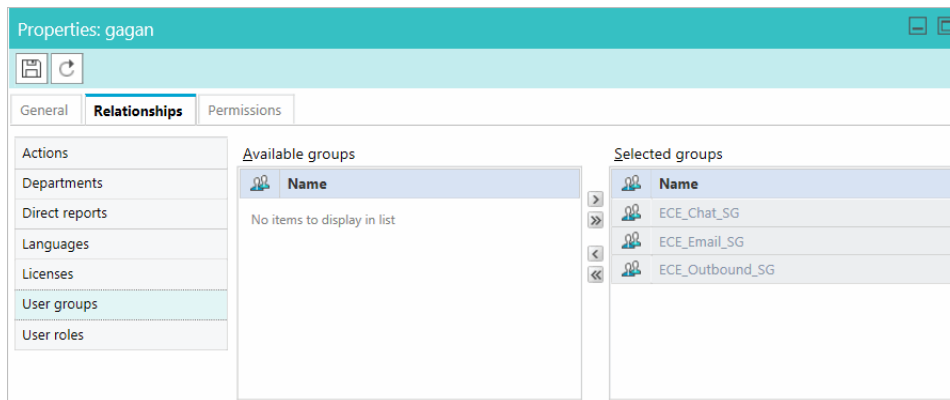
- e. Below, the Custom section is not in use.
- f. Next, go to the Relationships tab, and set the following.
  - a. First, go to the Licenses tab and assign licenses to the user. The following licenses are available:
    - ECE CIH Platform
    - ECE Mail

- ECE Chat



*Select licenses*

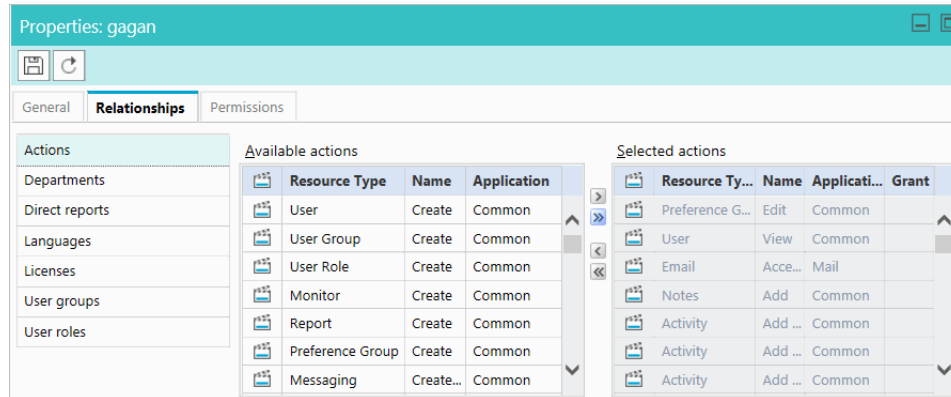
- In the User groups section you can see which user groups to which the user belongs. These groups are determined by the skill groups in which the user belongs in Unified CCE.




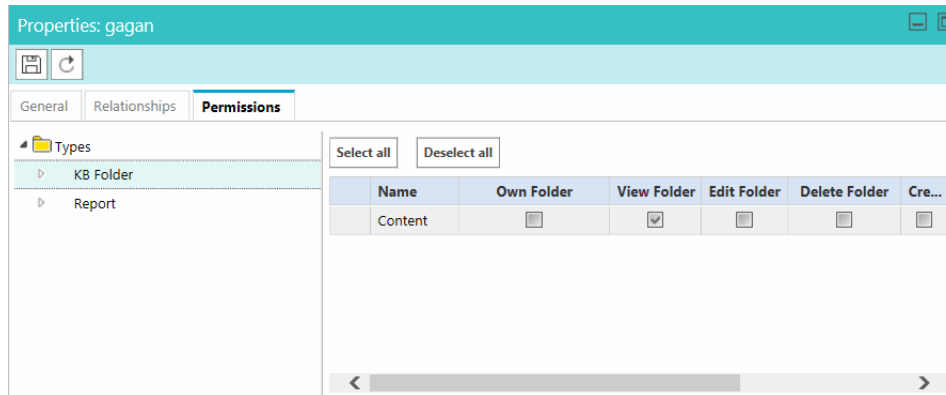
*Select user groups*

- Go to the User roles section and select the roles to be assigned to the user. If you want to view the actions that come as part of the selected role, save the user and go to the Actions tab to see the list of actions.
- Next, go to the Actions section, and view the list of actions assigned to the user. Here you can also assign additional actions to the user. You can identify how actions are assigned from the Grant field in the Selected actions section. The actions assigned explicitly show the value "Explicit". If you want to allow the user to import and export content for translations from the Knowledge Base Console, assign the "Import Translation" and "Export Translation" actions to the user.

You should not assign actions directly to user. You should always use roles with the actions and assign the roles to the user. This makes user management easier.



- e. Next, in the Languages section, select the primary KB language for the user.
4. Click the **Save**  button to enable the various options in the Permissions tab.
5. On the Permissions tab, the permissions for the following objects are assigned.
  - **KB Folder:** Own folder, View folder, Edit folder, Delete folder, Create folder, Create article, Edit article, Delete article, Suggest article, Manage suggestions, View personal folder
  - **Report:** Own, View, Edit, Delete, Schedule



*Assign permissions*


6. Click the **Save**  button.

## Deleting Users

You can delete users which are not being used. However, if a user has any open activities or cases, or suggestions in feedback state, then such a user cannot be deleted. You must reassign the cases and activities before deleting the user.

### To delete a user:

1. In the Tree pane, browse to the **Users** node. Based on where you want to delete the user from, do one of the following:

- If you are deleting a system administrator, go to the system partition and browse to **Administrator > Partition:** *Context\_Root\_Name* > **User > Users.**
  - If you are deleting a partition administrator, go to the business partition and browse to **Administrator > Partition:** *Partition\_Name* > **User > Users.**
  - If you are a department administrator, browse to **Administration > Departments >** *Department\_Name* > **User > Users.**
2. In the List pane, select the user you want to delete.
  3. In the List pane toolbar, click the **Delete**  button.
  4. A message appears asking to confirm the deletion. If the user has created any monitors in the Supervision Console, a message is displayed to inform that all the monitors created by the user will be deleted. Click **Yes** to delete the user.



# Data Masking

- ▶ [About Data Masking](#)
- ▶ [About Patterns](#)
- ▶ [Creating Patterns](#)
- ▶ [Creating Patterns in XML File](#)
- ▶ [Exporting Masking Patterns](#)
- ▶ [Importing Masking Patterns](#)
- ▶ [Copying Patterns](#)
- ▶ [Deleting Patterns](#)
- ▶ [Validating Masking Patterns](#)
- ▶ [Applying Patterns to Chat Channel](#)
- ▶ [Applying Patterns to Email Channel](#)
- ▶ [Masking Content of Completed Activities](#)

## About Data Masking

---

Data masking allows businesses to ensure that sensitive information, like credit card numbers, Social Security Numbers, bank account numbers, and so on, is not transmitted from the system to the customers and vice versa. If the customer and agent do add any sensitive data in the email content and chat messages, all such data is masked before it is displayed to customers and agents and before it is stored in the system.

Data masking is the process of scanning the content for sensitive information and applying regular expressions to mask the sensitive information and hide the original data with characters, like, \* ^ #. Data is masked using patterns, which are defined using Javascript and Java regular expressions.

Data masking is available for emails and chats.

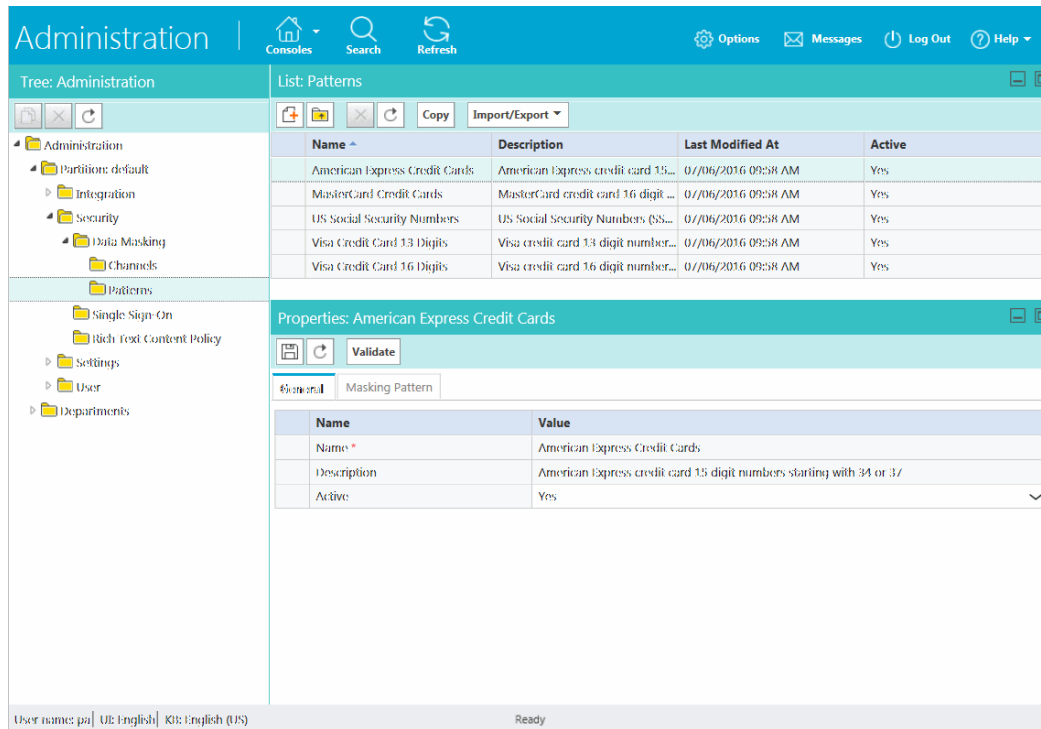
## About Patterns

---

Patterns are definitions of data masking rules that you apply to the content of emails and chat messages to hide sensitive data. Patterns are defined using JavaScript and Java regular expressions. In the pattern definition, you also define the character to use for replacing the matching data (for example, \*, X, #). You can enable the Luhn algorithm for masking credit card numbers. This algorithm distinguishes the valid credit card numbers from a random sequence of numbers.

A partition administrator with the **Manage Application Security** action can manage patterns - that is, create, delete, edit, copy, import, and export patterns.


You can either create a pattern from the user interface, or you can create patterns in an XML file and import the file using the import feature.



*Out-of-the-box patterns*

## Creating Patterns

### To create a pattern:

1. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* **> Security > Data Masking > Patterns.**
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 pattern.
  - **Description:** Provide a description for the pattern that explains what type of masking is done by the pattern.



- **Active:** Make the pattern active when it is ready for use. Only active patterns can be applied to channels. Once a pattern is made active and used in channels, it can be made inactive only after the association from the channels is removed.

Name	Value
Name *	Discover Credit Cards
Description	Discover credit card 16 digit numbers
Active	Yes

*Set the general properties*

4. In the Properties pane, on the Masking Pattern tab, set the following:
  - **Masking Character:** From the dropdown list, select the character to be used to mask the data. The default value is \*. Options available are: \*, -, #, X, x.
  - **Javascript Regular Expression:** Provide the Javascript regular expression for masking.
  - **Java Regular Expression:** Provide the Java regular expression for masking.
  - **Number of characters to unmask from right:** Provide the number of characters, from the right, that should be ignored while masking. For example, if you are masking the social security number and you do not want to mask the last 4 numbers of the SSN, the SSN shows as \*\*\*\*\*3545
  - **Number of characters to unmask from left:** Provide the number of characters, from the left, that should be ignored while masking. For example, if you are masking a 10 digit account number and you do not want to mask the first 4 numbers of the account number, the account number shows as 8765\*\*\*\*\*
  - **Apply Luhn Algorithm:** Select **Yes** to apply the Luhn algorithms to credit card numbers.

Name	Value
Masking character *	^
Javascript regular expression *	((?:4\d{3}) (?:5[1-5]\d{2}))6(?:011 5[0-9]{2})(?:-\?040?)(?:\d{4}(?:-\?0...
Java regular expression *	((?:4\d{3}) (?:5[1-5]\d{2}))6(?:011 5[0-9]{2})(?:-\?040?)(?:\d{4}(?:-\?0...
Number of characters to unmask from right	4
Number of characters to unmask from left	0
Apply Luhn algorithm	No

*Configure the pattern properties*

5. Click the **Save**  button.

# Creating Patterns in XML File

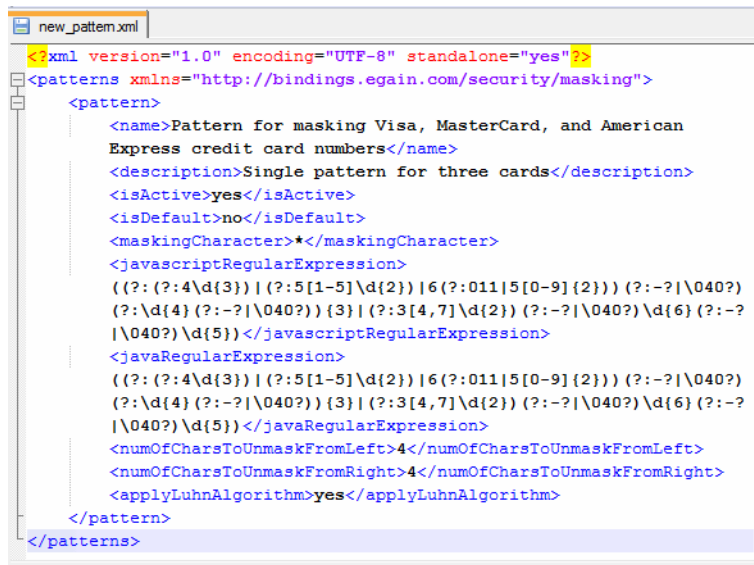
While preparing a file for importing patterns, keep in mind:

- ▶ Only XML files can be used to import patterns.
- ▶ You can name the file anything you want.
- ▶ Elements should be defined in the order specified in the pattern file exported from the application.
- ▶ Elements and values of elements in the XML file are case sensitive.
- ▶ For user created patterns, the **isDefault** element should be always set to **no**. Likewise, for default patterns, the **isDefault** element should be always set to **yes**.
- ▶ If you are importing a pattern that already exists in the system, your existing pattern will be overwritten by the import process.

The following table lists the names of the properties as they appear in the file and on the UI. For the description of each field, see [“Creating Patterns” on page 144](#).

Name on the UI	Name in the file
Name	name
Description	description
Active	isActive
Default	isDefault
Masking character	maskingCharacter
Javascript regular expression	javascriptRegularExpression
Java regular expression	javaRegularExpression
Number of characters to unmask from right	numOfCharsToUnmaskFromLeft
Number of characters to unmask from left	numOfCharsToUnmaskFromRight
Apply Luhn algorithm	applyLuhnAlgorithm

A sample pattern looks like:



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<patterns xmlns="http://bindings.egain.com/security/masking">
  <pattern>
    <name>Pattern for masking Visa, MasterCard, and American
    Express credit card numbers</name>
    <description>Single pattern for three cards</description>
    <isActive>yes</isActive>
    <isDefault>no</isDefault>
    <maskingCharacter>*</maskingCharacter>
    <javascriptRegularExpression>
      ((?: (? : 4 \d { 3 } ) | (? : 5 [ 1 - 5 ] \d { 2 } ) | 6 (? : 0 1 1 | 5 [ 0 - 9 ] { 2 } ) ) (?: - ? | \ 0 4 0 ? )
      (?: \d { 4 } (?: - ? | \ 0 4 0 ? ) ) { 3 } | (?: 3 [ 4 , 7 ] \d { 2 } ) (?: - ? | \ 0 4 0 ? ) \d { 6 } (?: - ?
      | \ 0 4 0 ? ) \d { 5 } )</javascriptRegularExpression>
    <javaRegularExpression>
      ((?: (? : 4 \d { 3 } ) | (? : 5 [ 1 - 5 ] \d { 2 } ) | 6 (? : 0 1 1 | 5 [ 0 - 9 ] { 2 } ) ) (?: - ? | \ 0 4 0 ? )
      (?: \d { 4 } (?: - ? | \ 0 4 0 ? ) ) { 3 } | (?: 3 [ 4 , 7 ] \d { 2 } ) (?: - ? | \ 0 4 0 ? ) \d { 6 } (?: - ?
      | \ 0 4 0 ? ) \d { 5 } )</javaRegularExpression>
    <numOfCharsToUnmaskFromLeft>4</numOfCharsToUnmaskFromLeft>
    <numOfCharsToUnmaskFromRight>4</numOfCharsToUnmaskFromRight>
    <applyLuhnAlgorithm>yes</applyLuhnAlgorithm>
  </pattern>
</patterns>
```

A sample XML file

## Exporting Masking Patterns

Patterns can be exported in XML format to share them across installations or if you wish to edit the patterns through an XML file. All the patterns configured in the system will be part of the exported XML file.

### To export patterns:

1. In the Tree pane, browse to **Administration > Partition: *Partition\_Name* > Security > Data Masking > Patterns**.
2. In the List pane toolbar, from the **Import/Export** button select the **Export Patterns** option.
3. A prompt appears to save the patterns XML file.

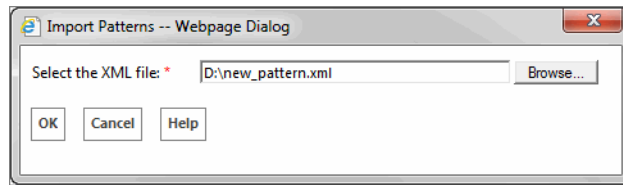
## Importing Masking Patterns

Only XML files can be used to import patterns.

### To import a pattern:

1. In the Tree pane, browse to **Administration > Partition: *Partition\_Name* > Security > Data Masking > Patterns**.
2. In the List pane toolbar, from the **Import/Export** button select the **Import Patterns** option.

3. In the Import patterns window, provide the location of the XML file. Click **OK**.



*Provide the location the location file*

The system notifies when the patterns are imported successfully. You will also be notified if the import process will over-write existing patterns.


If the file has any issues, the import process is aborted and the user is notified. Some of the issues with the file can be:

- ▶ Type of file is not XML.
- ▶ Size of the imported file is more than 10 MB.
- ▶ XML is malformed.
- ▶ The values of the name, description, Javascript Regular Expression, Java Regular Expression fields are more than the allowed size.
- ▶ A custom pattern is defined as a default pattern.
- ▶ A default pattern is not defined as a default pattern.
- ▶ The Javascript regular expression defined in the file is not correct.
- ▶ The Java regular expression defined in the file is not correct.
- ▶ You are deactivating a pattern that is in use.

## Copying Patterns

---

### To copy a pattern:

1. In the Tree pane, browse to **Administration > Partition: *Partition\_Name* > Security > Data Masking > Patterns**.
2. In the List pane, select a pattern.
3. In the List pane toolbar, click the **Copy**  button.

You are notified when the pattern is copied. All patterns are copied in the inactive state. You can make them active when you are ready to use the pattern.

## Deleting Patterns

---

Patterns cannot be deleted if they are associated with a channel. You must remove all associations before deleting the pattern.

### To delete a pattern:

1. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* **> Security > Data Masking > Patterns.**
2. In the List pane select a pattern.
3. In the List pane toolbar, click the **Delete**  button.

## Validating Masking Patterns

---

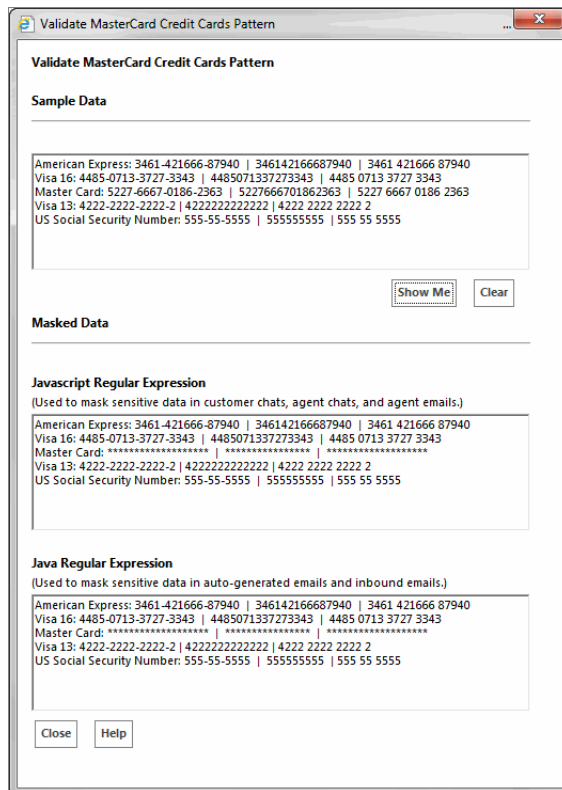
### Validating Individual Patterns

After you create a pattern, test it by using the validation option available for each pattern.

### To validate a pattern:

1. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* **> Security > Data Masking > Patterns.**
2. In the List pane, select the pattern you want to test.
3. In the Properties pane toolbar, click the **Validate** button.
4. In the Validate Pattern Name Pattern window, do the following:
  - a. In the Sample Data provide the text you want to use for testing the pattern and click the **Show Me** button.
  - b. In the Masked Data section, the Javascript regular expression and Java regular expression applied to the sample data are visible. All the settings configured in the Masking Pattern tab will be applied to the sample data.

c. After you are done testing, click the **Close** button.



Validate patterns

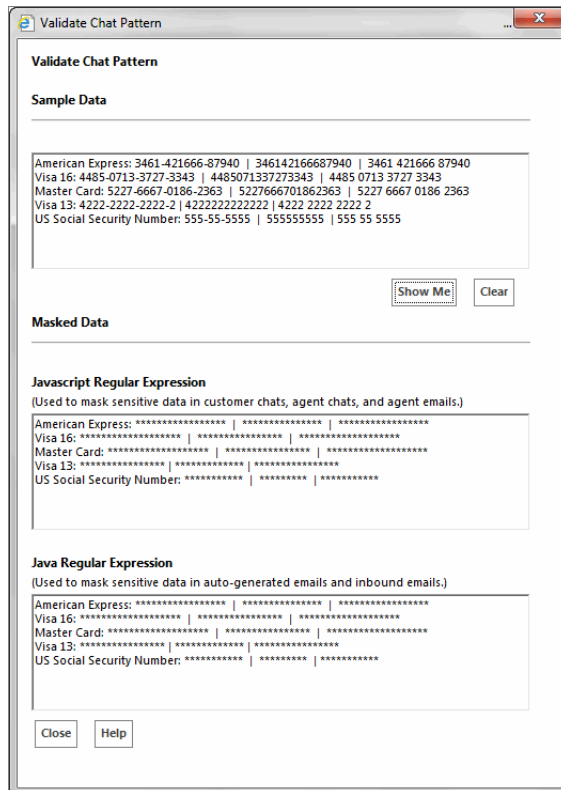
## Validating Masking Patterns Applied to Channels

In addition to validating individual patterns, you can validate the patterns selected for a channel and make sure that they work properly as a group and the order of the selected patterns is correct.

### To validate patterns applied to channels:

1. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* > **Security > Data Masking > Channels**. If you are validating from the department level, browse to **Administration > Departments > Department\_Name** > **Security > Data Masking > Channels**.
2. In the List pane select the channel you want to test.
3. In the Properties pane toolbar, click the **Validate** button.
4. In the Validate Pattern window, do the following:
  - a. In the Sample Data provide the text you want to use for testing the pattern and click the **Show Me** button.
  - b. In the Masked Data section, all the selected patterns applied to the sample data are visible.

c. After you are done testing, click the **Close** button.



*Validate the patterns selected for a channel*

## Applying Patterns to Chat Channel

### At the Partition Level

A partition administrator with the necessary actions can perform these tasks:

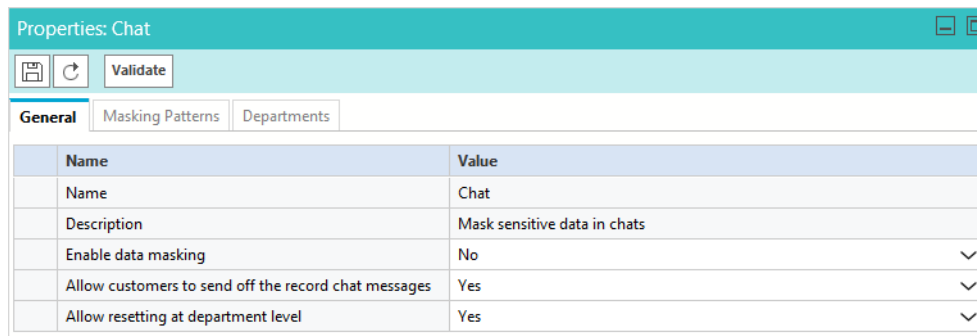
- ▶ **Manage Application Security:** Allows the administrator to view the patterns applied to channels and to apply patterns to channels.
- ▶ **View Application Security:** Gives a read-only view of the patterns applied to channels. Users with this action cannot change any configurations.

### What can the partition administrator do?

- ▶ Enable data masking for chat for all departments and manage all configurations from the partition level.
- ▶ Give control to the department administrators to configure their own settings. At this point, department administrators can choose to configure their own settings or can continue to use the settings configured by the partition administrators. Once a department administrator decides to configure their own settings, they are not affected by the changes made by the partition administrator.

## To apply patterns to the chat channel:

1. In the Tree pane, browse to **Administration > Partition: *Partition\_Name* > Security > Data Masking > Channels**.
2. In the List pane select **Chat**.
3. In the Properties pane, on the General tab, set the following:
  - **Name:** This field is read-only.
  - **Description:** This field is read-only.
  - **Enable data masking:** Select **Yes** to enable data masking for chat messages. By default this is set to **No**.
  - **Allow customers to send off the record chat messages:** Enable this setting to allow customers and agents to exchange off the record messages. Data masking rules do not apply to such messages. During a chat, only the customer has the option to enable off-the-record feature. All messages exchanged in this mode are not stored in the system. By default this is set to **Yes**.
  - **Allow resetting at department level:** Use this setting to allow department level administrators to set their own configurations and masking rules for the chat channel. When this setting is enabled, department administrators get an option to either follow the partition level settings, or to configure their own. By default this is set to **No**.



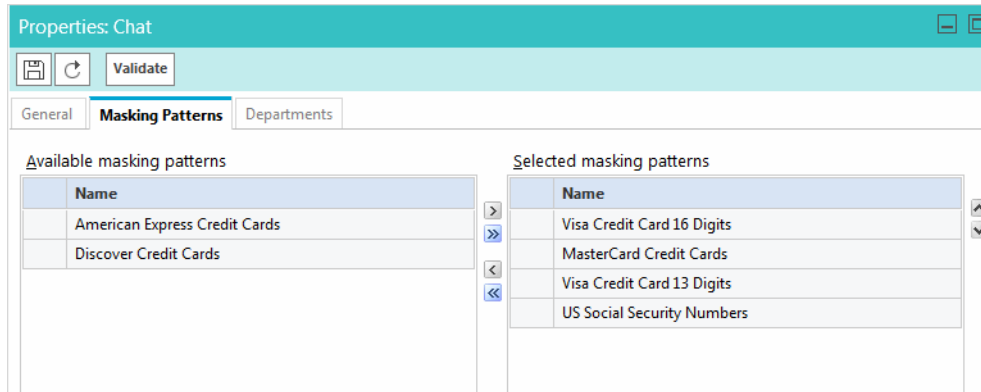
Name	Value
Name	Chat
Description	Mask sensitive data in chats
Enable data masking	No
Allow customers to send off the record chat messages	Yes
Allow resetting at department level	Yes

*Set the general properties*

4. Next, go to the Masking Patterns tab and select the patterns to be applied to the chat channel and define the order of the patterns. While defining the order make sure that the longest pattern is on top followed by the short patterns. This ensures that patterns that use smaller matches do not partially mask the text that would match the longer text. For example, if you are selecting both Visa Credit Card 16 Digits and Visa Credit Card 13 Digits, make sure the order is - Visa Credit Card 16 Digits and then Visa Credit Card 13 Digits. If

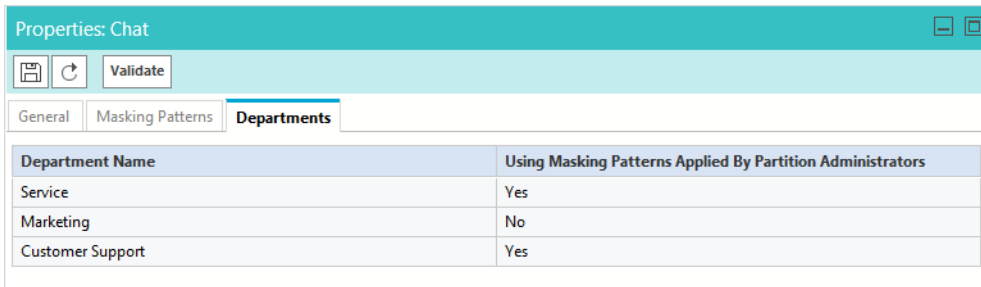


the order is not correct, and let us say you mask the following content: Visa 16: 4485-0713-3727-3343 and Visa 13: 4222-2222-2222-2, it will be masked as Visa 16: \*\*\*\*\*343 and Visa 13: \*\*\*\*\*. You will notice that the 16 digit credit card did not get masked properly.




Select masking patterns for chat

- Next, go to the Department tab to see a read-only view of the departments that are using the masking patterns applied by the partition administrator.



View the list of departments

- Click the **Save**  button.
- After saving the changes, validate the patterns selected for the channel. For details, see [“Validating Masking Patterns Applied to Channels”](#) on page 150.

## At the Department Level

A department administrator with the following actions can perform this task:

- ▶ **Manage Department Security:** Allows you to view the patterns applied to channels and to apply patterns to channels.
- ▶ **View Department Security:** Gives a read-only view of the patterns applied to channels. Users with this action cannot change any configurations.

## How much control do department administrators get?

- ▶ If the partition administrator has not given control to department administrators to configure their own settings, the department administrators get a read-only view of the settings configured by the partition administrator.
- ▶ If the department administrator has the option to configure their own settings, and they choose to do so, they are not affected by the changes made to the configurations by the partition administrators.

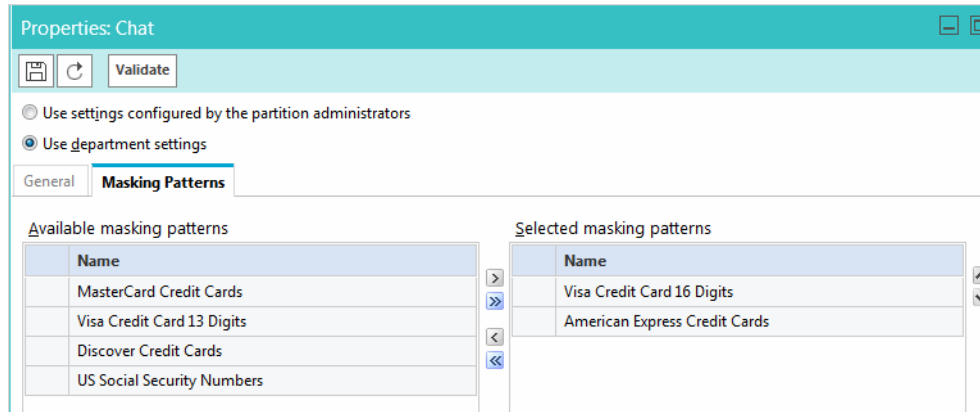
### To apply patterns to the chat channel:

1. In the Tree pane, browse to **Administration > Departments > *Department\_Name* > Security > Data Masking > Channels**.
2. In the List pane select **Chat**.
3. In the Properties pane, select from the following two options to decide if you want to continue to use the settings configured by the partition administrator, or if you want to configure data masking for your own department. These options are enabled only if the partition administrator allows department administrators to over-write the partition level settings.
  - **Use settings configured by the partition administrators:** Your department will automatically use the configurations configured at the partition level. Any changes made at the partition level will be applied to the department immediately.
  - **Use department settings:** You will manage the data masking configurations on your own and independent of the partition administrator. Any changes made by the partition administrator will not be applied to your department.
4. In the Properties pane, on the General tab, set the following:
  - **Name:** This field is read-only.
  - **Description:** This field is read-only.
  - **Enable data masking:** Select **Yes** to enable data masking for chat messages. By default this is set to **No**.
  - **Allow customers to send off the record chat messages:** Enable this setting to allow customers and agents to exchange off the record messages. Data masking rules do not apply to such messages. During a chat, only the customer has the option to enable off-the-record feature. Any messages exchanged in this mode are not stored in the system. By default this is set to **Yes**.


Name	Value
Name	Chat
Description	Mask sensitive data in chats
Enable data masking	No
Allow customers to send off the record chat messages	Yes

*Set the general properties*

- Next, go to the Masking Patterns tab and select the patterns to be applied to the chat channel and define the order of the patterns. While defining the order make sure that the longest pattern is on top followed by the short patterns. This ensures that patterns that use smaller matches do not partially mask the text that would match the longer text. For example, if you are selecting both Visa Credit Card 16 Digits and Visa Credit Card 13 Digits, make sure the order is - Visa Credit Card 16 Digits and then Visa Credit Card 13 Digits. If the order is not correct, and let us say you mask the following content: Visa 16: 4485-0713-3727-3343 and Visa 13: 4222-2222-2222-2, it will be masked as Visa 16: \*\*\*\*\*343 and Visa 13: \*\*\*\*\*. You will notice that the 16 digit credit card did not get masked properly.



Select masking patterns for the chat channel

- Click the **Save**  button.
- After saving the changes, validate the patterns selected for the channel by using the **Validate** button. For details, see [“Validating Masking Patterns Applied to Channels”](#) on page 150.

## Applying Patterns to Email Channel

### At the Partition Level

A partition administrator with the following actions can perform this task:

- ▶ **Manage Application Security:** Allows you to view the patterns applied to channels and to apply patterns to channels.
- ▶ **View Application Security:** Gives a read-only view of the patterns applied to channels. Users with this action cannot change any configurations.

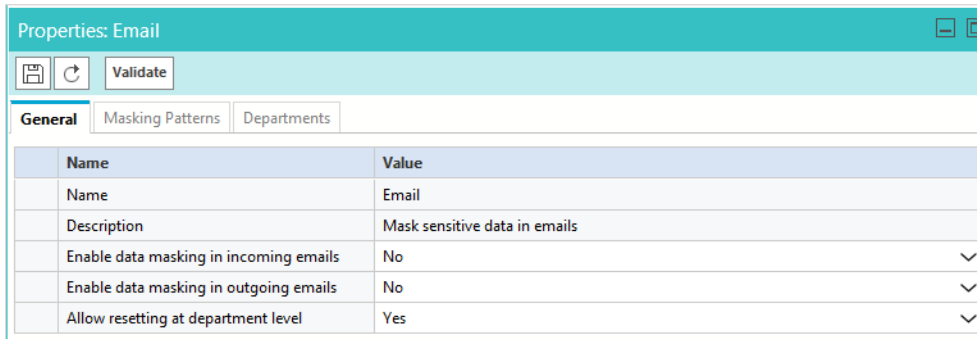
### What can the partition administrator do?

- ▶ Enable data masking for incoming and outgoing emails for all departments and manage all configurations from the partition level.

- ▶ Give control to the department administrators to configure their own settings. At this point, department administrators can choose to configure their own settings or can continue to use the settings configured by the partition administrators. Once a department administrator decides to configure their own settings, they are not affected by the changes made by the partition administrator.

### To apply patterns to the email channel:

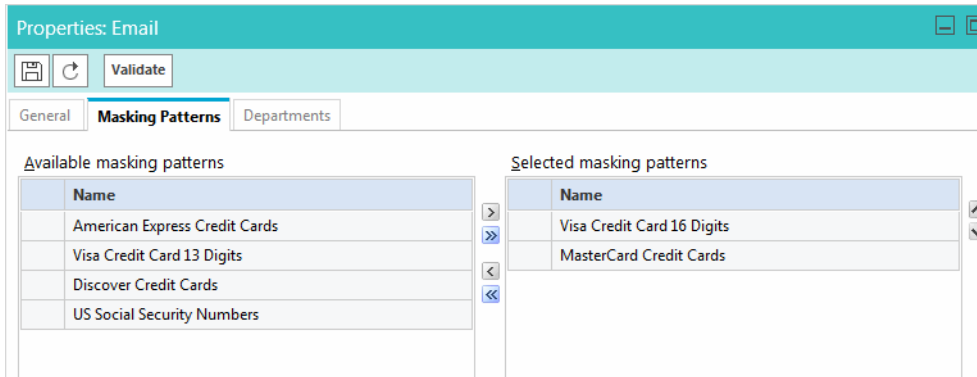
1. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* > **Security > Data Masking > Channels.**
2. In the List pane select **Email.**
3. In the Properties pane, on the General tab, set the following:
  - **Name:** This field is read-only.
  - **Description:** This field is read-only.
  - **Enable data masking in incoming emails:** Select **Yes** to enable data masking for incoming emails. By default this is set to **No**.
  - **Enable data masking in outgoing emails:** Select **Yes** to enable data masking for outgoing emails. By default this is set to **No**.
  - **Allow resetting at department level:** Use this setting to allow department level administrators to set their own configurations and masking rules for the chat channel. When this setting is enabled, department administrators get an option to either follow the partition level settings, or to configure their own. By default this is set to **No**.



*Set the general properties*

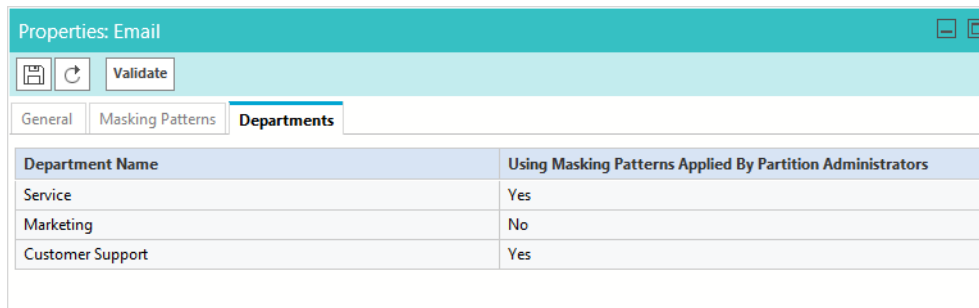
4. Next, go to the Masking Patterns tab and select the patterns to be applied to the email channel and define the order of the patterns. While defining the order make sure that the longest pattern is on top followed by the short patterns. This ensures that patterns that use smaller matches do not partially mask the text that would match the longer text. For example, if you are selecting both Visa Credit Card 16 Digits and Visa Credit Card 13 Digits, make sure the order is - Visa Credit Card 16 Digits and then Visa Credit Card 13 Digits. If

the order is not correct, and let us say you mask the following content: Visa 16: 4485-0713-3727-3343 and Visa 13: 4222-2222-2222-2, it will be masked as Visa 16: \*\*\*\*\*343 and Visa 13: \*\*\*\*\*. You will notice that the 16 digit credit card did not get masked properly.




Select masking patterns

- Next, go to the Department level tab to see a read-only view of the departments that are using the masking patterns applied by the partition administrator.



View the list of departments

- Click the **Save**  button.
- After saving the changes, validate the patterns selected for the channel by using the **Validate** button. For details, see [“Validating Masking Patterns Applied to Channels” on page 150](#).

## At the Department Level

A department administrator with the following actions can perform this task:

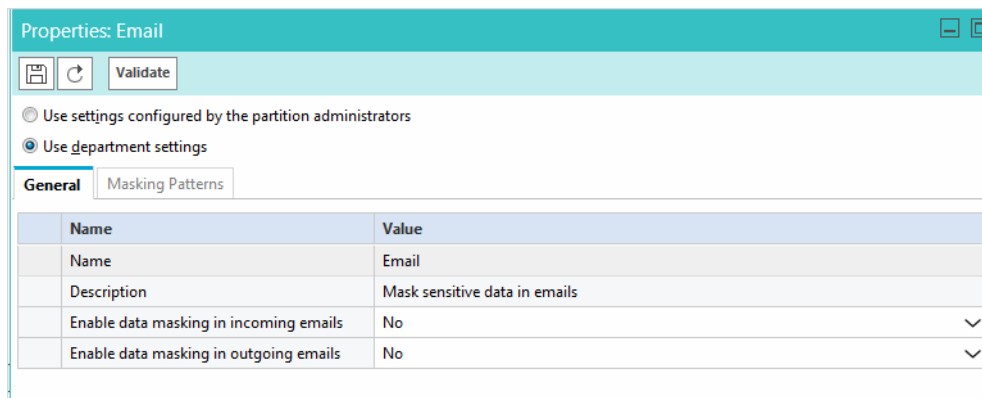
- ▶ **Manage Department Security:** Allows you to view the patterns applied to channels and to apply patterns to channels.
- ▶ **View Department Security:** Gives a read-only view of the patterns applied to channels. Users with this action cannot change any configurations.

## How much control do department administrators get?

- ▶ If the partition administrator has not given control to department administrators to configure their own settings, department administrators get a read-only view of the settings configured by the partition administrator.
- ▶ If the department administrator has the option to configure their own settings, and they choose to do so, they are not affected by the changes made to the configurations by the partition administrators.

### To apply patterns to the email channel:

1. In the Tree pane, browse to **Administration > Departments > *Department\_Name* > Security > Data Masking > Channels.**
2. In the List pane select **Email**.
3. In the Properties pane, select from the following two options to decide if you want to continue to use the settings configured by the partition administrator, or you want to configure data masking for your own department. These options are enabled only if the partition administrator allows department administrators to over-write the partition level settings.
  - **Use settings configured by the partition administrators:** Your department automatically uses the configurations configured at the partition level. Any changes made at the partition level will be applied to the department immediately.
  - **Use department settings:** You manage the data masking configurations on your own and independent of the partition administrator. Any changes made by the partition administrator will not be applied to your department.
4. In the Properties pane, on the General tab, set the following:
  - **Name:** This field is read-only.
  - **Description:** This field is read-only.
  - **Enable data masking in incoming emails:** Select **Yes** to enable data masking for incoming emails. By default this is set to **No**.
  - **Enable data masking in outgoing emails:** Select **Yes** to enable data masking for outgoing emails. By default this is set to **No**.



Properties: Email

Validate

Use settings configured by the partition administrators

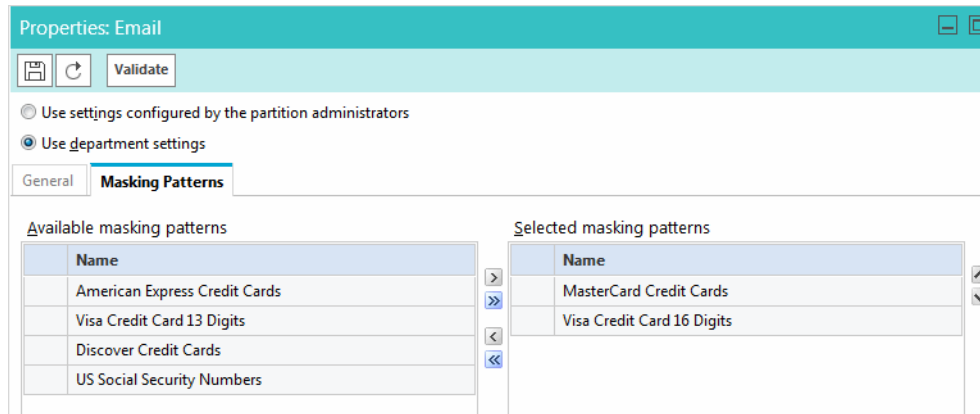
Use department settings

General | Masking Patterns


Name	Value
Name	Email
Description	Mask sensitive data in emails
Enable data masking in incoming emails	No
Enable data masking in outgoing emails	No

*View the general properties*

- Next, go to the Masking Patterns tab and select the patterns to be applied to the email channel and define the order of the patterns. While defining the order make sure that the longest pattern is on top followed by the short patterns. This ensures that patterns that use smaller matches do not partially mask the text that would match the longer text. For example, if you are selecting both Visa Credit Card 16 Digits and Visa Credit Card 13 Digits, make sure the order is - Visa Credit Card 16 Digits and then Visa Credit Card 13 Digits. If the order is not correct, and let us say you mask the following content: Visa 16: 4485-0713-3727-3343 and Visa 13: 4222-2222-2222-2, it will be masked as Visa 16: \*\*\*\*\*343 and Visa 13: \*\*\*\*\*. You will notice that the 16 digit credit card did not get masked properly.



Select patterns for the email channel

- Click the **Save**  button.
- After saving the changes, validate the patterns selected for the channel by using the **Validate** button. For details, see [“Validating Masking Patterns Applied to Channels” on page 150](#).

## Masking Content of Completed Activities

The types of edits that can be made to completed activities is limited. For example, the content of an email or chat cannot be changed or removed. However, there is a utility available to mask the content of activities if there was some personally identifiable information in the activity’s content that should have been masked but was not due to an error or oversight of configuring masking conditions.



**Important:** This utility can only be run by a department administrator.

### To mask content of completed activities:

- While signed in to the Tools Console as a department administrator, click the **Utilities** button.
- In the Utilities window, in the Mask Content of Chat and Email Activities field, click the **Go** button.

3. In Activity IDs field, provide the ID of the activity and click the **Show Details** button.

### Mask Content of Chat and Email Activities [Back to Utilities](#)

This utility will mask emails and completed chat activities only.  
The Data Masking Rules defined in the Administration Console will be used to mask the content.  
Provide comma separated activity IDs to mask.

Activity IDs:

No	Activity ID	Activity Type	Department Name	Status	Content
1	260159	Chat	Service	Completed	<a href="#">Show Content</a>

*Use the Show Details button to search for activities*

4. Once the activity has been located and selected, click one of the following:
  - **Mask:** Masks the content of the activity using the data masking rules defined in the Administration Console.
  - **Reset:** Resets the search and clears the Activity IDs field.
  - **Show Content (link):** This link, located in the Content column of the activity, displays the content and details of the activity.





# Cross-Origin Resource Sharing

- ▶ [About Cross-Origin Resource Sharing](#)
- ▶ [Enabling Cross-Origin Resource Sharing](#)

# About 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.

A partition administrator with the following actions can perform this task:

- ▶ **Manage Application Security:** Allows you to enable or disable CORS and configure the list of allowed websites for CORS.
- ▶ **View Application Security:** Gives a read-only view of the CORS settings. Users with this action cannot change any configurations.

## Enabling Cross-Origin Resource Sharing

### To enable cross-origin resource sharing:

1. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* > **Security > CORS**.
2. In the List pane, select Cross Origin Resource Sharing.
3. In the Properties pane, set the following:
  - **Enable Cross Origin Resource Sharing:** Select **Yes** to enable CORS. By default, CORS is disabled 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`

Name	Value
Name	Cross Origin Resource Sharing
Description	Cross Origin Resource Sharing configuration
Enable Cross Origin Resource Sh...	Yes

Allow all origins for CORS  
 Allow following origins for CORS

Access-Control-Allow-Origins (Allowed Websites)	
http://www.healthcare.gov	X

Enable CORS

4. Click the **Save**  button.



# Agent Single Sign-On

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

# About Single Sign-On (SSO)

Single Sign-On (SSO) for Enterprise Chat and Email is required for users to access the application. However, depending on the users, the consoles, and the access method, the configuration steps may vary.

- ▶ Consoles can be accessed outside of Finesse, but Single Sign-On (SSO) must be enabled to allow agents and supervisors to log in to the Agent Console through Finesse. For more information, see [“Configuring Agent Single Sign-On \(SSO\)” on page 169](#).
- ▶ Supervisors or administrators can log in to ECE supervisory and administrative consoles outside of Finesse using Cisco IDS and an Identity Provider (IdP). For more information, see [“Configuring Agent Single Sign-On \(SSO\)” on page 169](#).
- ▶ ECE partition administrators for Packaged CCE configurations can also be enabled for SSO. For more information, see [“Configuring SSO for Partition Administrators” on page 174](#).

The following SSO methods can be enabled in the ECE application:

- ▶ LDAP (Lightweight Directory Access Protocol) This method is configured for Partition Administrators that are auto-provisioned in ECE when they access the ECE gadget in the CCE Admin Web interface. For more information, see [“Configuring SSO for Partition Administrators” on page 174](#).
- ▶ SAML 2.0 This method of SSO is configured as the identity provider for customer SSO. For more information, see [“Customer Single Sign-On” on page 178](#). Supervisors and administrators can use SAML 2.0 as the identity provider when SSO is configured for Cisco IDS to access the application outside of Finesse. For more information, see [page 172](#).



**Important:** The SAML 2.0 configuration steps in this guide are explained using ADFS as the identity provider as an example, however, any SAML 2.0 compliant identity provider is also supported.

---

- ▶ Cisco Identity Service (IDS) ([page 170](#))



**Important:** While Unified CCE can be configured to use multiple different SSO options, this guide discusses how to configure SSO for ECE agents using Cisco IDS and partition administrators using LDAP.

---

## Preparing to Configure Single Sign-On in ECE

There are some important pre-configuration tasks that must be completed before configuring SSO for Cisco IDS in the Administration Console.

### Integrating with Unified CCE

The application must already be properly integrated with Unified CCE or Packaged CCE.

- ▶ For more information about integrating with Unified CCE, see [“Unified CCE Integration” on page 31](#).

- ▶ For more information about integrating with Packaged CCE, see the *Enterprise Chat and Email Installation Guide for Packaged Contact Center Enterprise*.

## Configuring an Identity Provider

For users that are accessing ECE consoles outside of Finesse, 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:



**Important:** These steps are applicable for systems using ADFS as the identity provider. Other identity providers may have different methods to configure public key certificate.

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.

## Generating and Importing a Java Keystore Certificate

If the system is being configured to allow for single sign-on outside of Finesse, a Java keystore certificate is required. A self-signed certificate is valid. A Java keystore file is required to generate a Java keystore certificate.

### Generating a Java Keystore File

Before generating the file, ensure that the JAVA\_HOME and Java path environment variable are set to the java installation directory.

#### To generate a Java keystore file:

1. In command prompt, execute the following command:

```
keytool -genkey -keyalg RSA -alias alias_name -keystore java keystore location -keysize 2048 -validity 1825
```

where *alias\_name* is name of alias for key entry, for example `ecesaml`

and *java keystore filename* is the jks filename where keystore to be stored. For example. `saml.jks`

2. The following inputs are then required:
  - Keystore password:
  - Re-enter new password:

- First and Last name  
The First name should be the FQDN of the ECE Application or Web server.
  - Name of your organizational unit
  - Name of your organization
  - Name of your City or Locality
  - Name of your State or Province
  - The two-letter country code for this unit
  - Is CN=, OU=, O=, L=, ST=, C= correct?
  - Key password for *alias\_name*
  - Re-enter new password:
3. The Java keystore file is generated with this information. The keystore password, alias name, and key password entered here will be used while configuring assertion decryption certificate in Administration Console ([page 172](#)).

## Generating a Certificate with a Java Keystore File

Before generating the certificate with a Java keystore file, ensure that the JAVA\_HOME and Java path environment variable are set to the Java installation directory and Open SSL is installed on the machine.

### To generate a certificate using a Java keystore file:

1. In command prompt, execute the following command:
 

```
keytool -v -importkeystore -srckeystore keystore_filename -srcalias alias_name -destkeystore p12_file_name -deststoretype PKCS12 -destkeypass key_pass
```
2. When prompted, provide the following:
  - Destination keystore password
  - Re-enter the new password
  - Source keystore password:
  - Key password for *alias\_name*
3. Go to the open\_ssl/bin directory. Execute following command to generate the pem file which contains the Identity Provider certificate.
 

```
openssl pkcs12 -in p12_file_name -out pem_file_name -nodes -nokeys
```

This is the same certificate which is required for populating Identity Provider Certificate parameter the Administration Console ([page 172](#)).
4. Use the following commands to export the Java keystore certificate: `keytool -keystore c:\java keystore location -alias alias_name -export -file c:\java keystore location\mycert.cer`  
 For example: `keytool -keystore c:\temp\mykeystore -alias ecesaml -export -file c:\temp\mycert.cer`

## Importing a Java Keystore Certificate

### To import the Java keystore certificate:

1. The generated certificate should be copied to the ADFS server.
2. In the Identity Provider, such as ADFS, edit the Relying Party Trust created for ECE.
3. Navigate to the Signature tab, and click **Add**.
4. Browse to and select the certificate you created.
5. Import the `c:\java\keystore\file` into ECE and configure it as a Request Signing Certificate. The store password and key password will be the one you chose.

## Importing the SSL Certificate

Before configuring SSO, the Secure Sockets Layer (SSL) certificate of the Cisco IDS server must be imported to ECE File servers for Unified CCE installations. The certificate can be imported to an existing keystore or a new keystore can be created on the ECE File server.

The SSL certificate can be used in [“Configuring Agent Single Sign-On \(SSO\)” on page 169](#) and in [“Configuring SSO for Partition Administrators” on page 174](#).

### To obtain the SSL certificate:

1. Launch Internet Explorer on the ECE Application Server.
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:

If running a distributed installation with multiple File servers, perform these steps on the Active Node. These steps explain how to import SSL certificate in the default Java Keystore named “cacerts”.



**Important:** Perform these steps for both the primary and secondary Cisco IDS server.

---

1. Copy the certificate file to the File server directory: `file_server\ECE_installation_directory\env\jdk\bin`



If you have 2 IdS servers, each with their own certificate, copy each into this location.

2. Open Command prompt on the server where you copied the certificate file and provide the directory.



**Important:** If you use DFS for your File server role, you can make this change from any server. Simply map a network drive to the File server path, then use Command prompt as instructed below.

---

3. Run following command to import the certificate: `keytool -import -trustcacerts -alias eg_custom_<alias name> -keystore file_server\ECE_installation_directory\env\jdk\lib\security\cacerts -file file_server\ECE_installation_directory\env\jdk\bin\ciscoins.cer`

If you have 2 IdS servers, change the alias and filename for the second server. The alias name does not need to match the server or certificate name, but this makes it easier to find in the future.



**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 provide the desired password 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 Agent Single Sign-On (SSO)

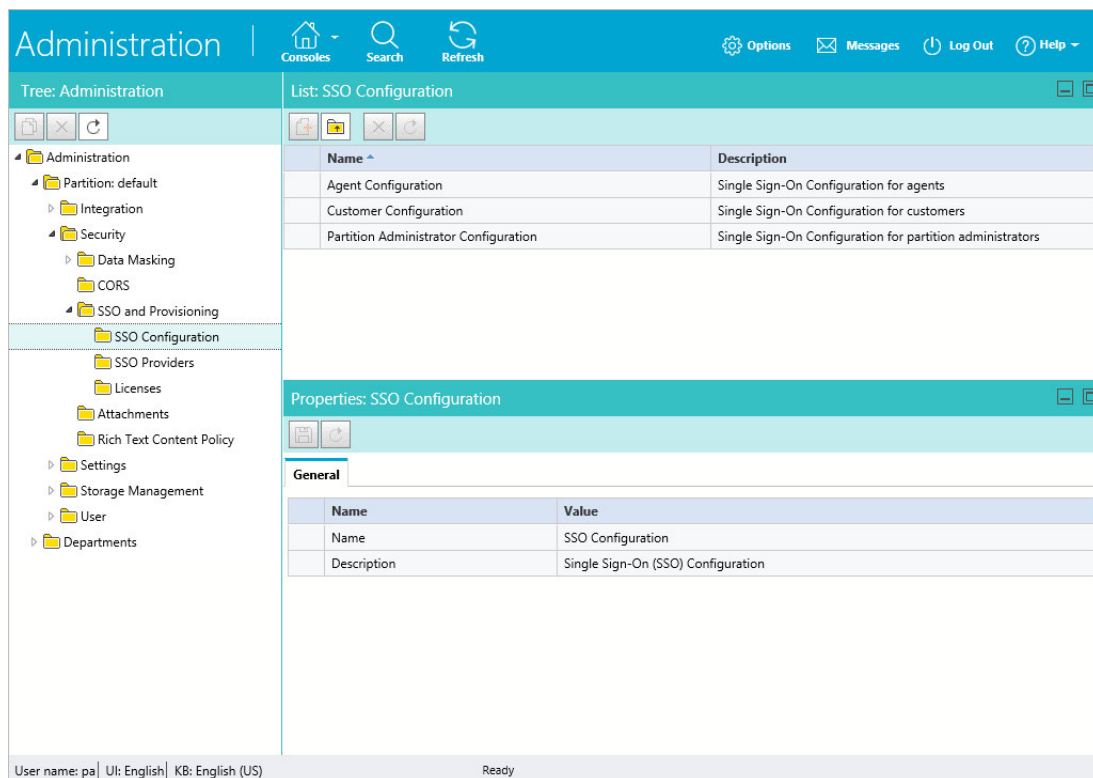
### Important things to note about agent Single Sign-On

- ▶ 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.
- ▶ If Encrypted Assertion is enabled and/or Service Provider initiated authentication is enabled and it does not use the default java keystore (for example, `cacerts`) available in the JDK, a Java Keystore (JKS) certificate is needed in the SSO configuration process to allow users to sign in to ECE outside of Finesse. The default java keystore is available in the JDK that is installed during the ECE installation process.
- ▶ In order for agents who sign in to ECE in Finesse to access the application, ensure that you have imported the SSL certificate used in Cisco IDS userinfo URL into `cacerts`. For more information about importing the certificate, see [“Importing the SSL Certificate” on page 168](#).
- ▶ 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 50 for more information.
- ▶ Depending on what type of users are accessing the application and which consoles are being accessed, the SSO configuration requirements may be different.
  - When configuring the application for agents to access the Agent Console through Finesse, refer to steps 1 (page 170) through 5 (page 171).
  - When configuring the application for users to access the Agent Console or other consoles outside Finesse:
    - Refer to the steps after step 6 (page 172).
    - Refer to the steps in the *Enterprise Chat and Email Installation Guide* for configuration of an Identity Provider, for example, ADFS.

### To configure agent SSO in ECE:

1. In the Tree pane, browse to **Administration > Partition: *Partition\_Name* > Security > Single Sign On**.



*Browse to single sign-on node*

2. In the List pane, select **Agent Configuration**.
3. In the Properties pane, set the following:
  - **Enable Single Sign-On:** Select **Yes** to enable SSO.
  - **Single Sign-On Type:** **Cisco IDS**.

4. Click the **SSO Configuration** tab. Refer to [“Preparing to Configure Single Sign-On in ECE” on page 165](#) for more details.

5. In the OpenID Connect Provider section, 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.

- **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 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.

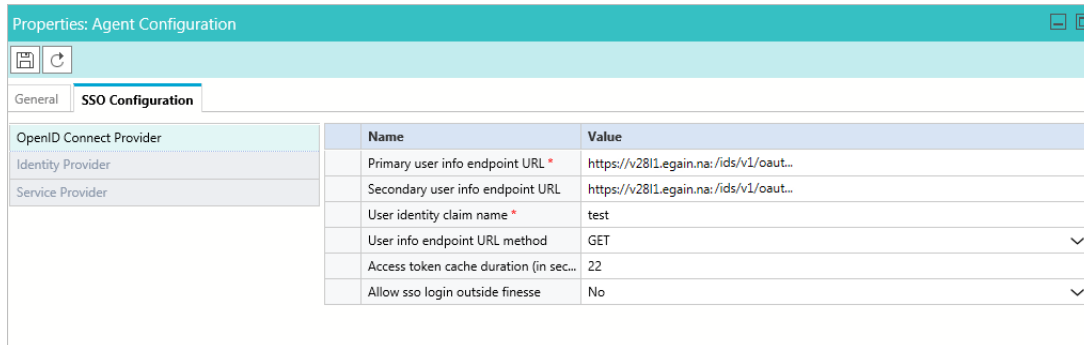
- **User info endpoint URL method:** The HTTP method used by ECE for making Bearer token validation calls to the User Info Endpoint URL. Select one of the options:

- **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 (in 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 to **Yes** 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 via the identity provider or service provider.

If set to **Yes**, you must provide the necessary information under the **Identity Provider** and **Service Provider** sections. This requires that if you are using an ADFS configuration, it allows for an ADFS server.



*Provide the Cisco IDS details*

6. If **Allow SSO login Outside of Finesse** is set to **Yes**, provide the following details in the Identity Provider section:
  - **Entity ID:** Entity ID of the Shared or Single ADFS server. This should be the ADFS trust URL, for example: `http://FQDN_OF_ADFS/adfs/services/trust`.
  - **Identity provider certificate:** This is the public key portion of the token signing certificate from ADFS. The certificate must start with “-----BEGIN CERTIFICATE-----” and end with “-----END CERTIFICATE-----”
  - **User Identity Location:** Select **SAML Subject Identifier** to set the identity location in the certificate to the default SAML subject identifier, as in the subject in the SAML assertion, for example the username in the `<saml:Subject>`. Select **SAML Attribute** to assign the identity location to a specific attribute in the certificate, for example, `email.address`. Provide the attribute in the **User Identity Attribute Name** field.
  - **User Identity Attribute Name:** Applicable only when User ID Location value is an SAML attribute. This can be adjusted within the SAML assertion and used to select a different attribute for the authentication of users, such as an email address. It can also be used to create new users with a SAML Attribute. For example, if a user is identified through the value provided in the email.address attribute, and the value of email address provided doesn't match any user in the system, a new user is created with the provided SAML attributes.
  - **Enable encrypted assertion:** If you wish to enable SAML assertion for console login, set the value to **Enable**. If not, set the value to **Disable**.
  - **Assertion decryption certificate:** If **Enable encrypted assertion** is set to **Enable**, click the **Assistance** button and provide the following in the Assertion Decryption Certificate window:
    - **Java keystore file:** Provide the file path of your Java Keystore File. This file will be in .jks format and contains the decryption key the system needs to access files secured by the Identity Provider.
    - **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.

Name	Value
Entity ID *	http://psadfs01.egdemo.info/adfs/services/trust
Identity provider certificate *	-----BEGIN CERTIFICATE----- MIIC0JCCAbqgAwIBAgIQf56a6fiQ2YJLPf...
User identity location	SAML Subject Identifier
User identity attribute name *	
Enable encrypted assertion	Disable
Assertion decryption certifi...	

*Provide the identity provider details*

7. If **Allow SSO login Outside of Finesse** is set to **Yes**, provide the following the Service Provider section:
  - **Service provider initiated authentication:** Set to **Enable**.
  - **Entity ID:** The Web Server or Load Balancer FQDN of ECE.
  - **Request signing certificate:** A Java Keystore (JKS) certificate is needed to provide the necessary information. For more information about obtaining a JKS, see [“Generating and Importing a Java Keystore Certificate” on page 166](#). Click the **Assistance** button and provide the following information in the next window and click **OK**.
    - **Java Keystore File:** Provide the file path of your Java Keystore File. This file will be in .jks format and contains the decryption key the system needs to access files secured by SAML.
    - **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.





**Important:** The request signing certificate should be converted to a public key certificate and configured in the Relying party trust created on the Shared IdP server. For more information, see [“Generating and Importing a Java Keystore Certificate” on page 166](#) and [“Configuring an Identity Provider” on page 166](#).

- **Signing algorithm:** Set the signing algorithm for the service provider. You may set the value to **SHA-256**. If using ADFS, this value should match with the algorithm selected in the relying party trust created on the ADFS server in the ADFS Relying Party Trust properties, under the Advanced tab.
- **Identity provider login URL:** The URL for SAML authentication. For example, for ADFS, this would be `http://FQDN_OF_ADFS/adfs/ls`.

- **Logout URL:** The URL to which users are redirected upon logging out. This is optional and can be any URL. For example, agents can be redirected to <https://www.cisco.com> after SSO logout.

Name	Value
Service provider initiated auth...	Enable
Entity ID *	https://uslewm02.eng.na/
Request signing certificate *	-----BEGIN ENCRYPTED PRIVATE KEY----- MIIE6TAbBgoqhkIG9w0BD...
Identity provider login URL *	https://psadfs01.egdemo.info/adfs/ls/
Logout URL	https://psadfs01.egdemo.info/adfs/ls/?wa=wsignoutcleanup1.0&wreply=...

*Provide the service provider details*

8. Click the **Save**  button.
9. In the Tree pane, browse to **Administration** > *Partition\_Name* > **Settings** > **Partition**.
10. In the List pane, select the partition settings group.  
The Properties pane refreshes to show the attributes of the group.
11. Next, in the Properties pane, go to the Attributes tab to configure values for settings. From the list, select the **Web server URL or Load Balancer URL** setting to modify. In the **Value** field provide the web server or load balancer FQDN. See “[Web Server URL or Load Balancer URL](#)” on page 50 for more information.
12. Click the **Save**  button.

## Configuring SSO for Partition Administrators

### Important things to note about configuring SSO for partition administrators:

- ▶ Configuring 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 is for the ECE gadget and it is 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 keystore mentioned in the **Keystore location** field.
- ▶ The location of the Java Keystore is required to configure SSO for partition administrators when SSL is enabled. The location is accessed on Application Server by the Service Account. Therefore, upon obtaining the Java Keystore, it should be placed in a location that is accessible by all Application servers.
  - For single-server or split-server setups, the Java Keystore location can be an absolute path, such as `C:\temp\keystore`
  - For distributed server setups, the Java Keystore location can be a UNC path on the File server which is accessible by all Application servers. For example: `File_Server\temp\keystore`
- ▶ This should be the same LDAP server where users logging in to CCE Web Admin interface are configured. Make sure that the ECE Application server can access this LDAP server URL to avoid connectivity issues.

## To configure SSO for LDAP systems:

1. Sign in to the 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. For more information about the keystore location, see [“Important things to note about configuring SSO for partition administrators:”](#) on page 174.

Name	Value
LDAP URL *	ldap://rmlab-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 1 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`

- ▶ Once SSO has been configured for Cisco IDS, agents configured for SSO and with the Authentication Type set to **Local Login** can sign into the Agent Console with the following URL:

`https://ece_web_server/system/web/apps/liteagent?locallogin=true`. For more information about configuring users, see [“Editing Department Users”](#) on page 135.



## 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](#)
- ▶ [Troubleshooting](#)

## 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, etc) 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 180](#).
- ▶ **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 181](#).

## 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`.

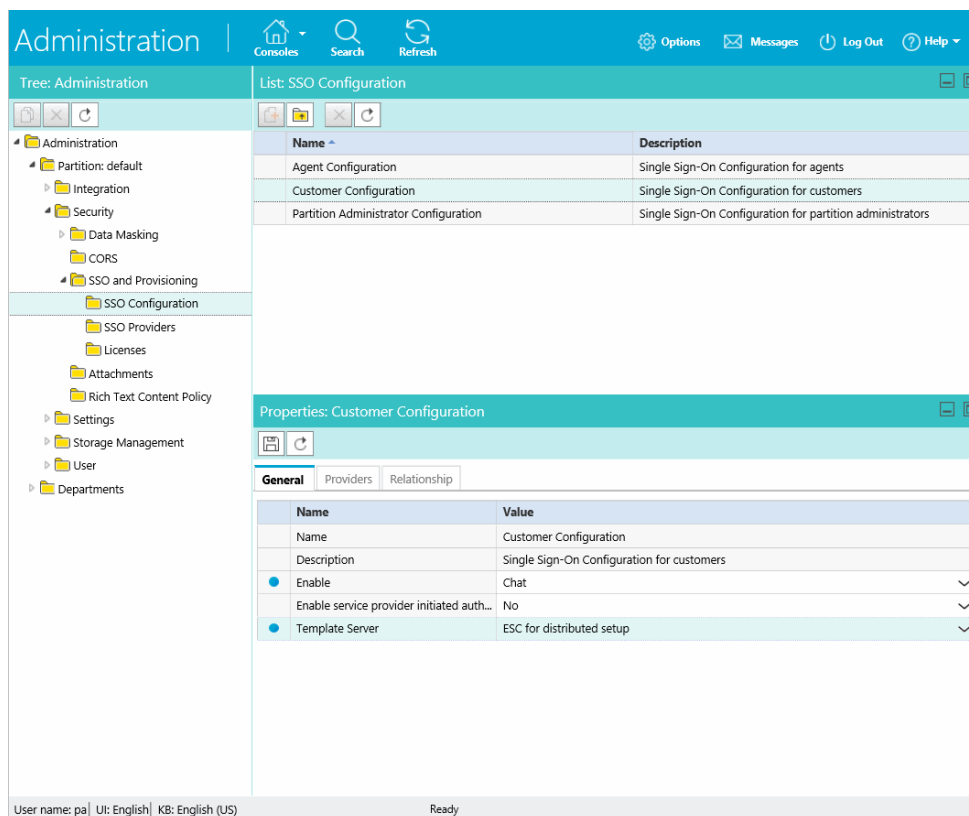
Note: the `providerId` query parameter is optional. If it is omitted, the service exposed at the specified URL assumes default provider ID configured in Enterprise Chat and Email.

## 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 181](#)
- ▶ [“Configuring Customer Single Sign-On” on page 185](#)


## 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.

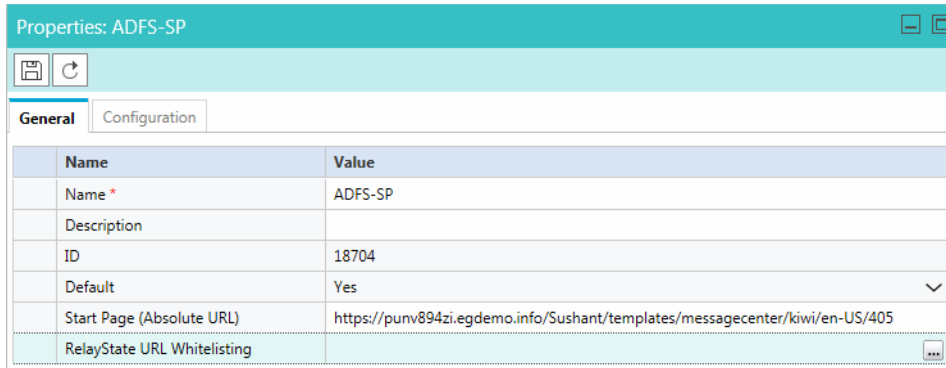
- ▶ Encrypted SAML assertion is supported. If you wish to enable encrypted SAML assertion, you will need a Java Keystore (JKS) file for the decryption certificate.
- ▶ A Java Keystore (JKS) file is necessary if the service provider is enabled to authenticate users in SAML 2.0, as well. Contact your IT 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. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* **> Security > SSO and Provisioning > SSO Providers.**
3. In the List pane, click the **New**  button.
4. In the Properties pane, under the General tab, provide the following:
  - **Name:** The name of the identity provider
  - **Description:** A description of the identity provider
  - **ID:** This field is automatically updated and cannot be changed.
  - **Default:** Select **Yes** to make this the default identity provider for customer single sign-on configurations. If not, select **No**.
  - **Start Page (Absolute URL):** Provide the URL for the page on which web-based customers should land when successfully logging in with single sign-on.
  - **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 **Assistance** button and select one of the following options from the pop-up window:
    - **Allow all RelayState URLs:** Whitelists all RelayState URLs of the service provider.

- **Allow RelayState(s) that start with the following URL(s):** Provide the URLs in the field below the option and press **Enter**.



*Provide the general information*

5. Click the **SSO Configuration** tab. 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 50](#).
  - 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.
    - **Identity provider certificate:** The public key certificate. The certificate must start with “-----BEGIN CERTIFICATE-----” and end with “-----END CERTIFICATE-----”
    - **Enable encrypted assertion:** Select **Yes** to enable assertion encryption or **No** to disable encryption.
    - **Assertion decryption certificate:** If **Enable Encrypted Assertion** is set to **Yes**, click the **Assistance** button and provide the following in the Assertion Decryption Certificate window:
      - **Java keystore file:** Provide the file path of your Java Keystore File eg:  
C:\keystore\version\_number\SS0\keystore.jks. This file is in .jks format and contains the decryption key the system needs to access files secured by SAML.
      - **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.

	Name	Value
Identity Provider	SAML Version	SAML 2.0
Service Provider	Entity ID *	chatenc1
	Identity provider certificat...	-----BEGIN CERTIFICATE----- MIIDUTCCAjmgAwIBAgIEdhfs... [...]
	Enable encrypted assertion	Yes [v]
	Assertion decryption certif...	-----BEGIN ENCRYPTED PRIVATE KEY----- MIIE6jAcBgoqhki... [...]

Provide the identity provider SAML configuration information

- Under the Service Provider option, provide the following:
  - **Enable identity provider initiated logout service:** Set to **Yes** to allow the application to accept logout requests from the 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:** Set to **Yes** to allow the IdP 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.

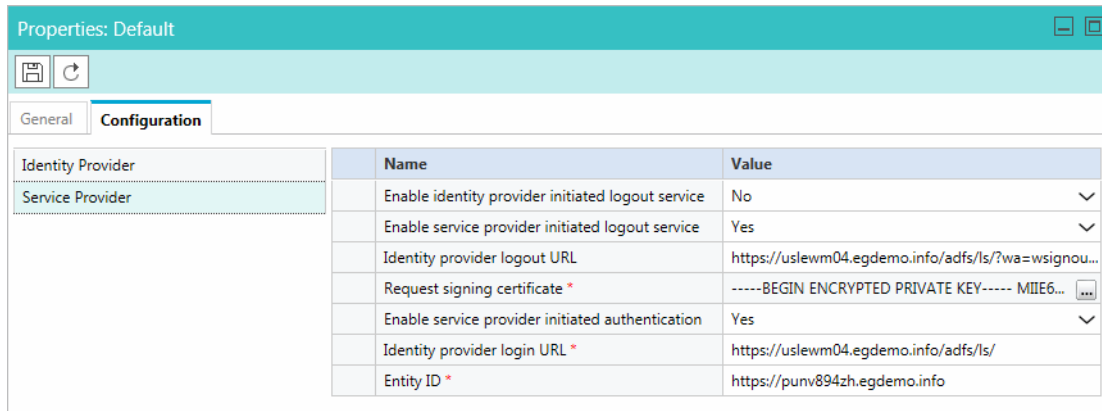


**Important:** In default portal and secure message center templates, the logout request is sent to the default provider configured in the application. If a different provider is necessary, the templates should be reconfigured to use the new provider.

- **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 **Assistance** [?] button, provide the following information in the next window, and click **OK**.
  - **Java keystore file:** Provide the file path of your Java Keystore File eg:  
`C:\keystore\version_number\SS0\keystore.jks`. This file is in .jks format and contains the decryption key the system needs to access files secured by SAML. On distributed installations, this should be stored on the file server.
  - **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:** Set to **Yes** to Enable. Setting this field to **Yes** enables the **Identity provider login URL** field and the **Entity ID** field.
- **Identity provider login URL:** The URL for SAML authentication.



- **Entity ID:** Entity ID of the service provider.



Name	Value
Enable identity provider initiated logout service	No
Enable service provider initiated logout service	Yes
Identity provider logout URL	https://uslewm04.egdemo.info/adfs/ls/?wa=wsignou...
Request signing certificate *	-----BEGIN ENCRYPTED PRIVATE KEY----- MIE6...
Enable service provider initiated authentication	Yes
Identity provider login URL *	https://uslewm04.egdemo.info/adfs/ls/
Entity ID *	https://punv894zh.egdemo.info

Provide the service provider SAML configuration information

6. Click the **Save**  button.

## Configuring Customer Single Sign-On

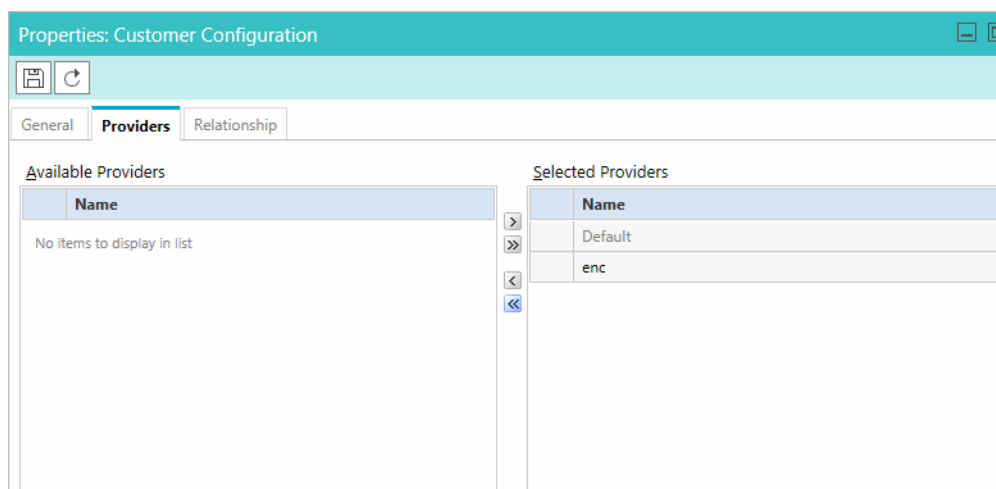
### To configure customer single sign-on:

1. Sign into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* **> Security > SSO and Provisioning > SSO Configuration.**
3. In the List pane, select **Customer Configuration.**
4. In the Properties pane, under the General tab, set the **Enable** field to one of the following options:
  - **Customer 360:** Enables customer single sign-on for Customer 360, which can be used by customers when accessing secure messaging centers.
  - **Chat:** Enables customer single sign-on for Secure Chat.
  - **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 setting the **Enable service provider initiated authentication** field to **Yes**. If you want to disable it, set the field to **No**.

5. In the Template Server field, select the server that holds the templates that are used for chats. By default, the option available for ECE is **ESC for distributed setup.**
6. In the Properties pane, under the Providers tab, move the identity providers that have been configured for single sign-on from the Available Providers list to the Selected Providers list. For more information about configuring identity providers, see [“Creating Identity Providers” on page 181.](#)

- 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*.



Select the identity providers for the customer SSO configuration

- 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*.

## Troubleshooting

Chat creation requests can be denied due to various conditions. In such cases, the customer is shown an error message along with an error code. The error code varies based on the cause of the issue and helps narrow down the root cause.

Error Code	Cause
400-101	'Apply Customer Chat Single Sign On' is enabled for the entry point, but SAML assertion is missing in the chat request. Make sure that you are passing the SAML assertion in the chat creation request.
400-102	If there is an expiration date time set in the SAML assertion, the assertion has expired by the time it reaches the application.
400-103	EntityId present in the SAML assertion does not match the EntityId configured in the 'Chat Customer Single Sign On' in the Administration Console.

Error Code	Cause
400-104	Public key certificate configured for SAML in 'Chat Customer Single Sign On' in the Administration Console has expired.
400-105	SAML assertion could not be validated using the public key configured in 'Chat Customer Single Sign On' in the Administration Console. Either the public key is incorrect or the SAML assertion has been tampered with.
400-106	An attribute configured in 'loginParameters' in eGainLiveConfig.js file has the property 'secureAttribute' set to '1', but it is missing from SAML assertion.
400-107	Field validation failed for one or more chat attributes transferred in SAML assertion. The validation is configured for chat attributes in the 'loginParameters' in the eGainLiveConfig.js file.
400-108	Any other miscellaneous errors such as 'malformed XML'.
400-109	Chat SSO is disabled in Admin configuration but SAML assertion is coming with chat creation request.
400-110	Encrypted assertion is disabled for Chat SSO in Administration Console and encrypted assertion is coming with chat session creation request. (For Encrypted assertion only.)
400-111	Decryption of SAML assertion using provided private key failed. (For Encrypted assertion only.)



# Attachments

- ▶ [About File Attachments](#)
- ▶ [Blocking Attachment File Types](#)
- ▶ [Allowing Attachment File Types](#)
- ▶ [Enabling Chat Attachments](#)

## About File Attachments

---

As a partition administrator, you can specify the file types that can be attached to chat messages. 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*.

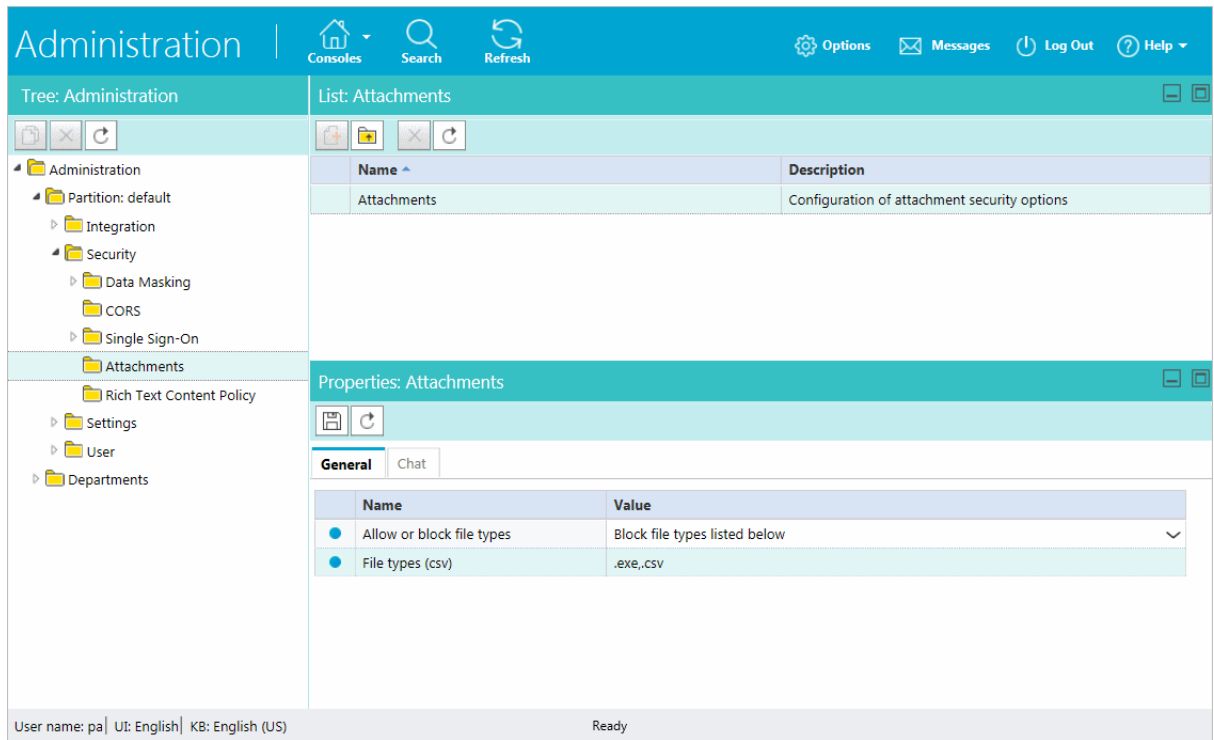
## Blocking Attachment File Types

---

### To block file types for attachments:

1. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* **> Security > Attachments**.
3. In the List pane, select **Attachments**.
4. In the Properties pane, under the General tab, set the **Allow or block file types** field to **Block file types listed below**.

- In the File types (csv) field, enter the file extensions you wish to block. 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`




Select the file types to block

- Click the **Save**  button.

## Allowing Attachment File Types

### To allow file types for attachments:

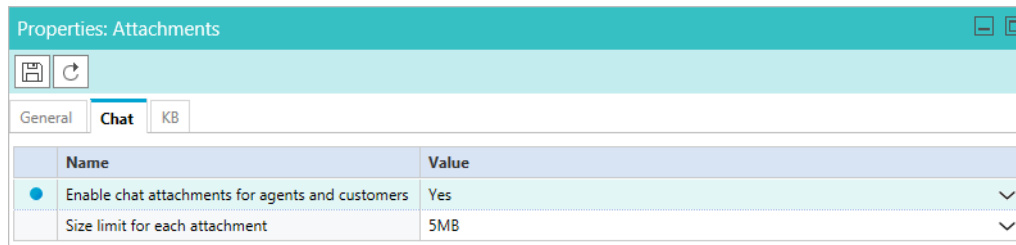
- Log into the business partition and go to the Administration Console.
- In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* **> Security > Attachments**.
- In the List pane, select **Attachments**.
- In the Properties pane, under the General tab, set the **Allow or block file types** field to one of the following:
  - Allow all file types**
  - Allow file types listed below**
- If **Allow file types listed below** is selected, in the File types (csv) field, enter the file extensions you wish to specifically 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`
- Click the **Save**  button.

# Enabling Chat Attachments

Customers and agents can send files to each other during a chat interaction once chat attachments have been enabled and configured by an administrator. Customers and agents can browse to a file and attach it to their chat messages.

## To enable chat attachments for agents and customers:

1. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* > **Security > Attachments**.
3. In the List pane, select **Attachments**.
4. In the Properties pane, under the General tab, set the file types you wish to allow for attachments. See [“Allowing Attachment File Types” on page 190](#) for details.
5. In the Properties pane, click the Chat tab and adjust the following fields:
  - **Enable chat attachments for agents and customers:** Set the value to **Yes** to enable chat attachments for the partition. Set the value to **No** to disable.
  - **Size limit for each attachment:** 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.



The screenshot shows the 'Properties: Attachments' dialog box with the 'Chat' tab selected. The 'General' tab is also visible. The 'Chat' tab contains two fields: 'Enable chat attachments for agents and customers' with a value of 'Yes' and 'Size limit for each attachment' with a value of '5MB'. Both fields have dropdown arrows on the right side.

Name	Value
Enable chat attachments for agents and customers	Yes
Size limit for each attachment	5MB

*Enable chat attachments for agents and customers*

6. Click the **Save**  button.

# 10 Rich Text Content Policies

- ▶ [About 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](#)



# About 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 messages sent by agents to customers
- ▶ Chat messages sent by customers to agents
- ▶ Content of standard and secure incoming emails
- ▶ Content of standard and secure outgoing emails
- ▶ Knowledge article content created by authors

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 199.

The screenshot displays the Administration Console interface. On the left, a tree view shows the navigation structure: Administration > Partition: default > Integration > Security > Rich Text Content Policy. The main area is divided into two panes. The top pane, titled 'List: Rich Text Content Policy', contains a table with the following data:

Name	Description	Enabled
Chat - Agent Policy	Policy for chat messages sent by agents	Yes
Chat - Customer Policy	Policy for chat messages sent by customers	Yes
Email - Inbound Policy	Policy for content of incoming emails	No
Email - Outbound Policy	Policy for content of outgoing emails	No
Knowledge - Author Policy	Policy for content created in application	Yes

The bottom pane, titled 'Properties: Chat - Agent Policy', shows the configuration for the selected policy. It includes a 'General' tab with a table of properties:


Name	Value
Name	Chat - Agent Policy
Description	Policy for chat messages sent by agents
Enable	Yes

At the bottom of the console, the status bar shows 'User name: pa | Ut: English | KB: English (US) Ready'.

*Set the Rich Text Content Policies*

## Enabling and Disabling Rich Text Content Policies


### To enable or disable rich text content policies:

1. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* > **Security > Rich Text Content Policy**.
3. In the List pane, select one of the content policies.
4. In the Properties pane, under the General tab, set the Enable field to **Yes** to enable, and **No** to disable.
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. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* > **Rich Text Content Policy**.
3. In the List pane, select one of the content policies.
4. In the Properties pane, click the **Import/Export** button.
5. In the dropdown menu, 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 195](#).
7. Return to the Administration Console and select the **Import Policy** option from the same dropdown menu.
8. Locate the updated XML file and import it.
9. 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 `<span>` 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 `<span>` 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 `<span>` 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 `<img>`. 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. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition\_Name* **> Rich Text Content Policy.**
3. In the List pane, select the policy you wish to restore.
4. In the Properties pane, click the **Restore** button.
5. In the window that opens, click **Yes**.





# 11

# Blocked Visitors

- ▶ [About Blocked Visitors](#)
- ▶ [Configuring Blocked Visitor Settings](#)

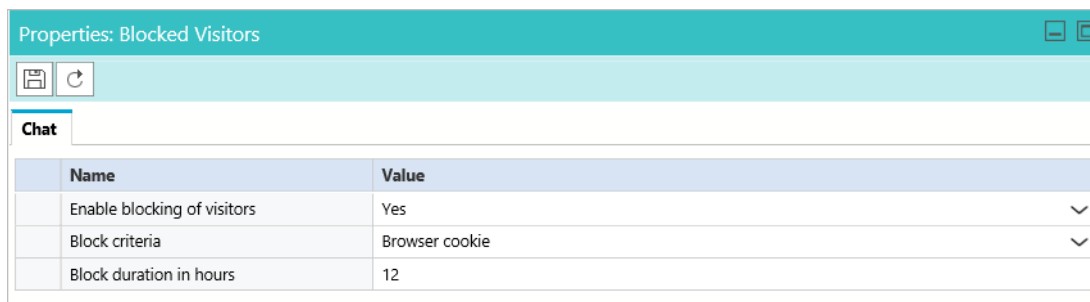
# About Blocked Visitors

In some instances, it may be necessary for agents to block chat customers, such as spambots or abusive customers. Administrators at the partition level can enable this ability for agents, as well as configure the length and criteria of the ban.

## Configuring Blocked Visitor Settings

### To enable visitor blocking:

1. In the Tree pane, browse to **Administration > Partition: *Partition\_Name* > Security > Blocked Visitors**.
2. In the List pane, select **Blocked Visitors**.
3. In the Properties pane, set the following:
  - **Enable blocking of visitors:** Select **Yes** to enable the ability for agents to block customers and **No** to disable it.
  - **Block criteria:** Select the method in which the user is identified for the ban. Select **Browser cookie** to use cookies to identify and ban the user or select and **Visitor IP address** to ban the user based on the IP address.
  - **Block duration in hours:** Provide the number of hours in which the visitor is banned when an agent blocks the them. The minimum value for this field is 1 hour. The maximum value for this field is 87,600 hours (3650 days).



Name	Value
Enable blocking of visitors	Yes
Block criteria	Browser cookie
Block duration in hours	12

*Enable the ability for agents to block users*

4. Click the **Save**  button.

# 12 Departments

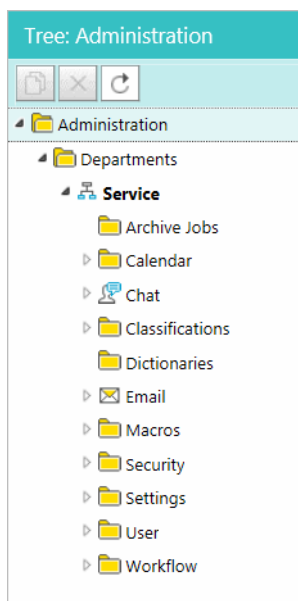
- ▶ [About Departments](#)
- ▶ [Creating Departments](#)
- ▶ [Configuring Activity Transfer Between Departments](#)
- ▶ [Copying Departments](#)

This chapter will assist you in understanding departments and how to set them up according to your business requirements.

## About Departments

Every organization needs to form various departments to meet their requirements, and divide their workforce accordingly. Departments enable you to form a mirror of the departments in your company. Departments and department administrators are created by the partition administrator. All departments that are created will be formed under a Partition. A partition level user will be able to view all departments under it. Whereas, a department level user can only view his own departments.

As a department administrator, you have the power to control and manage your department. This is made possible via the resources available in each department. Each department has twelve types of resources for use in your department. The Administration tree has an individual node for each type of resource.



*The Administration Console tree*

The following business objects are available in departments:

- ▶ Calendars: For more information, see [“Business Calendars” on page 209](#).
- ▶ Chat: For more information, see, *Enterprise Chat and Email Administrator’s Guide to Chat and Collaboration Resources*.
- ▶ Classifications: For more information, see [“Classifications” on page 217](#).
- ▶ Dictionaries: For more information, see [“Dictionaries” on page 224](#).
- ▶ Email infrastructure: For more information, see, *Enterprise Chat and Email Administrator’s Guide to Email Resources*.
- ▶ Data Masking for emails and chat: For more information, see [“Data Masking” on page 142](#).
- ▶ Macros: For more information, see [“Macros” on page 228](#).

- ▶ Settings: For more information, see “Settings” on page 39.
- ▶ Users: For more information, see “Users” on page 125.
- ▶ Workflows: For more information, see *Enterprise Chat and Email Administrator’s Guide to Routing and Workflows*.


## Creating Departments

Only a partition administrator can create departments. ECE integrated with Packaged CCE and Unified CCE supports up to a maximum of 200 departments.



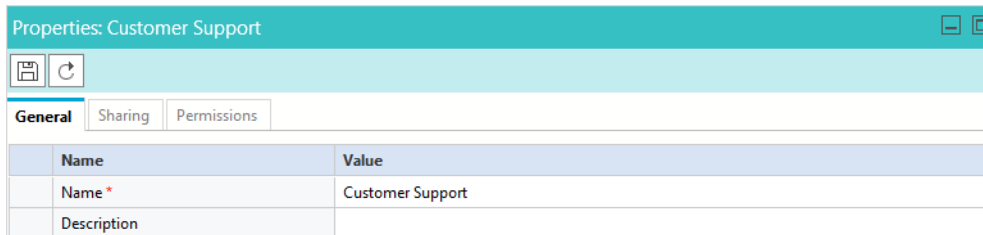
**Important:** Once a department is created in ECE, it cannot be deleted.

### To create a department:

1. In the Tree pane, browse to **Administration > Departments**.
2. In the list pane toolbar, click the **New**  button.
3. In the Properties pane, on the General tab, provide the name and general description for the department.



**Note:** The following characters are not allowed in the name: < , . ? : > \$ \* \ / #



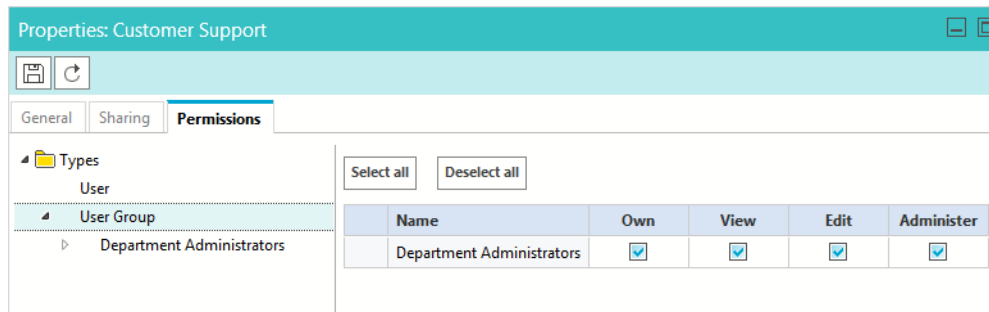
Name	Value
Name *	Customer Support
Description	

*Set general properties*




**Note:** Department sharing is not supported in ECE and the sharing section is currently not in use.

4. Lastly, on the Permissions tab, assign permissions to the users and user groups to own, view, edit, and administer the department that you have created.



Assign permissions

5. Click the **Save**  button, to save the department you have created.

## 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** partition level setting (page 45). 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.

## Copying Departments


You can copy an existing department. By copying a department, you get a ready structure, and you can edit any of the resources available in the department according to your requirements. This is a time saver and eases your task of creating multiple departments.

The following table describes how objects in a department get copied.

#	Object name	Notes
<b>Objects in the Administration Console</b>		
1.	Aliases	Copied as in original department with following exceptions: <b>Email address</b> is copied as <i>address_new_department_name</i> <b>Status</b> is always set as Inactive <b>User name</b> is copied as <i>username_new_department_name</i>
2.	Blocked Addresses	Copied as in original department
3.	Blocked file extensions	Copied as in original department

#	Object name	Notes
4.	Calendars, day labels, shift labels	Copied as in original department
5.	Classifications	Copied as in original department
6.	Chat entry points	Copied as in original department
7.	Customer Associations	Copied as in original department
8.	Data masking for email and chat channels	Not copied
9.	Delivery Exceptions	Copied as in original department
10.	Dictionaries	Copied as in original department
11.	Macros	Copied as in original department
12.	Monitors	Copied as in original department
13.	Queues	Copied as in original department
14.	Service levels	Copied as in original department
15.	Settings	Copied as in original department
16.	Transfer codes	Copied as in original department
17.	User groups	Copied as in original department
18.	User roles	Copied as in original department
19.	Users	<p>Copied as in original department with following exceptions:</p> <p><b>User name</b> is copied as <i>username_new_department_name</i></p> <p><b>Licenses</b> of users are not copied</p> <p><b>Actions, Roles, and Permissions</b> are copied.</p> <p>Note: Permissions are disabled for the copied users until licenses are assigned to them.</p>
20.	Workflows	<p>Copied as in original department with following exception:</p> <p>The <b>Active</b> field of workflows is set to <b>No</b>.</p>
<b>Objects in the Knowledge Base Console</b>		
21.	Knowledge Base	<p>Copied as in original department with following exception:</p> <p>User created folders and articles within are copied and same as original department.</p>
<b>Objects in the Tools Console</b>		
22.	Screen Attribute Settings	Copied as in the original department
23.	User Attribute Settings	Copied as in the original department
24.	Relationships - Customer Associations	Copied as in the original department
25.	Activity Types	Copied as in the original department

**To copy a department:**

1. In the Tree pane, browse to **Administration > Departments**.
2. In the Tree pane, select the department you want to copy.
3. In the Tree pane toolbar, click the **Copy**  button.
4. In the Copy department window that appears, provide the name of the new department and click **OK** to create a copy of the department.



# 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 working hours of the contact center. Calendars are primarily used in:

- ▶ Setting due dates for activities routed through workflow. When activities are routed through a workflow that has an SLA node, due date is set according to the calendar.
- ▶ Building reports. For example, reports like Email volume by queue, Email age by queue, and Email volume by alias.

In a calendar, you set up the working and non-working times of users. This enables the functioning of service levels. Service levels are used for setting due dates for activities, cases, and tasks, and trigger alarms to alert supervisors.

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 Tree pane, browse to **Administration > Departments** > *Department\_Name* > **Calendar > Shift Labels**.
2. In the List pane toolbar, click the **New**  button.  
The Properties pane refreshes to show the properties of the new shift label.
3. In the Properties pane, in the General tab, 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 default **Yes** is selected. Select **No** if agents do not work in this shift.



Name	Value
Name *	Morning shift
Description	
Agents work this shift	Yes 


*Set general properties*

4. 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 Tree pane, browse to **Administration > Departments** > *Department\_Name* > **Calendar > Shift Labels**.
2. In the List pane, select the shift label you want to delete.
3. In the List pane toolbar, click the **Delete**  button.

# Managing Day Labels


## Creating Day Labels

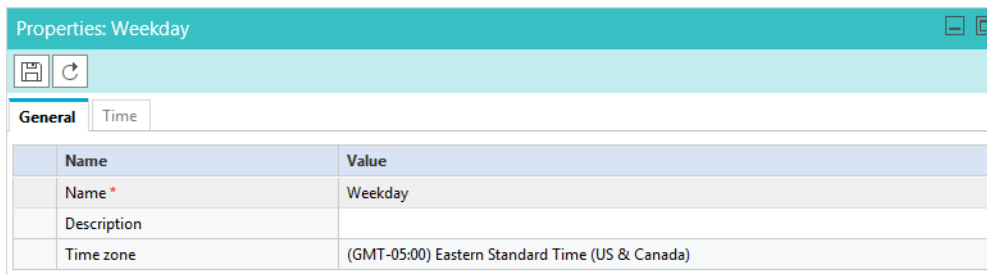
In day labels, you can set the work time for each shift. For example, you can divide the 24 hours available in a day into working shifts of eight hours each. Therefore, each day would have three shifts.



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

### To create a day label:

1. In the Tree pane, browse to **Administration > Departments > *Department\_Name* > Calendar > Day Labels**.
2. In the List pane toolbar, click the **New**  button.  
The Properties pane refreshes to show the properties of the new day label.
3. In the Properties pane, go to the General tab and 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 **Business calendar timezone** setting. For details on how to change this setting, see, [“Setting the Time Zone”](#) on page 213.



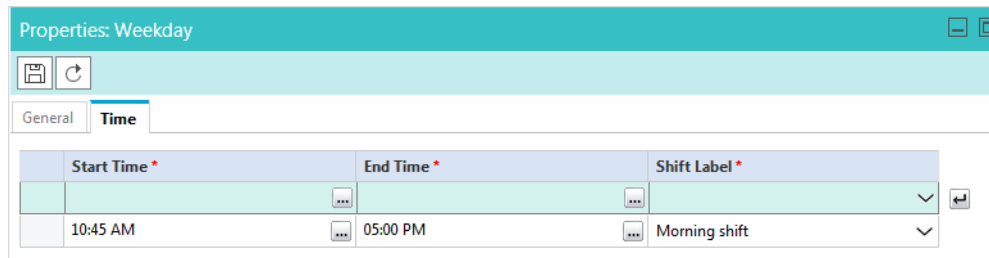
The screenshot shows a dialog box titled "Properties: Weekday" with a teal header. Below the header is a toolbar with a save icon and a refresh icon. The "General" tab is selected, and a table displays the following properties:

Name	Value
Name *	Weekday
Description	
Time zone	(GMT-05:00) Eastern Standard Time (US & Canada)

*Set general properties*

4. 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.



Start Time *	End Time *	Shift Label *
10:45 AM	05:00 PM	Morning shift


Set start times and end times for day labels

5. 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 Tree pane, browse to **Administration > Departments > *Department\_Name* > Calendar > Day Labels**.
2. In the List pane, select the day label you want to delete.
3. In the List pane toolbar, 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, **Business calendar timezone**. 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 Tree pane, browse to **Administration > Departments > *Department\_Name* > Settings > Department**.

2. In the List pane, select the department settings group.
3. In the Properties pane, go to the Attributes tab.
4. In the Attributes tab, select the **Business calendar timezone** setting. From the available time zones, select the time zone for your department.
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 Tree pane, browse to **Administration > Departments > *Department\_Name* > Calendar > Calendars**.
2. In the List pane toolbar, click the **New**  button.



The Properties pane refreshes to show the properties of the new calendar.

3. In the Properties pane, go to the General tab, and provide the following details.
  - **Name:** Type a name for the calendar.
  - **Description:** Type a brief description.
  - **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 **Business calendar timezone** setting. For details on how to change this setting, see, [“Setting the Time Zone” on page 213](#).

Properties: Customer Support Calendar ⌵ ⌵

General
Normal Week
Exception days

Name	Value
Name *	Customer Support Calendar
Description	
Effective start date *	01/01/2015 <span style="float: right;"></span>
Effective end date *	12/27/2015 <span style="float: right;"></span>
Time zone	(GMT-05:00) Eastern Standard Time (US & Canada)

*Set general properties*

- Now, go to the Normal Week tab, and select the day label to be used for each day of the week.

Day Of Week	Day Label *
Sunday	Weekend
Monday	Weekday
Tuesday	Weekday
Wednesday	Weekday
Thursday	Weekday
Friday	Weekday
Saturday	Weekend

*Configure the calendar for a normal week*

- Lastly, go to the Exceptions 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.



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


Date *	Day Label *
07/04/2015	Holiday
11/26/2015	Holiday
12/25/2015	Holiday

*Configure the calendar for the exception days, like holidays*

- Click the **Save**  button.

## Deleting Business Calendars

### To delete a calendar:

- In the Tree pane, browse to **Administration > Departments > *Department\_Name* > Calendar > Calendars**.
- In the List pane, select the calendar you want to delete.
- In the List pane toolbar, 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.

- ▶ In the department setting, **Business calendar timezone**, change the time zone.
- ▶ In the day labels, in the Times tab, adjust the start times and end times for all shifts.



# 14 Classifications

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

This chapter will assist you in understanding what classifications are and how to configure them.

## About Classifications

---

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:

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

You can create and assign classifications to incoming activities or to knowledge base articles. Categories and resolution codes can be assigned to incoming activities in two ways:

- ▶ Manually, from the Agent Console
- ▶ Automatically, through workflows

## Managing Transfer Codes

---

While transferring chats, agents can assign transfer codes to chats. A department level setting **Reason for chat transfer** is available to make this a mandatory field in the Transfer window.

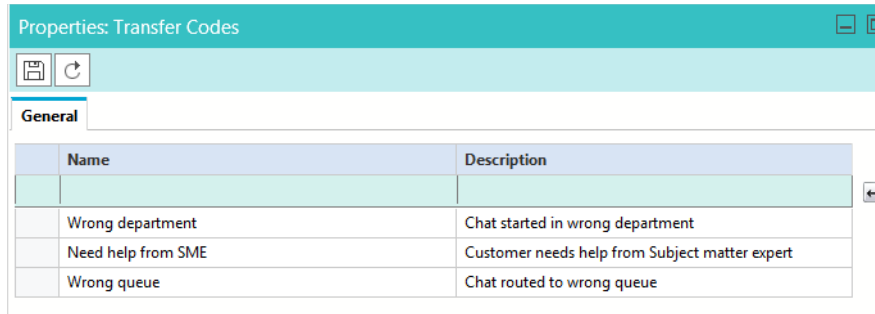
- ▶ [Creating Transfer Codes on page 218](#)
- ▶ [Deleting Transfer Codes on page 219](#)

## Creating Transfer Codes

**To create transfer codes:**

1. In the Tree pane, browse to **Administration > Departments > *Department\_Name* > Classifications > Transfer Codes**.

2. In the Properties pane, on the General tab, provide the name and description of the transfer code. Press **Enter** on the keyboard and likewise you can add multiple transfer codes.




Create new transfer codes

3. Click the **Save**  button.

## Deleting Transfer Codes

### To delete transfer codes:

1. In the Tree pane, browse to **Administration > Departments > *Department\_Name* > Classifications > Transfer Codes**.
2. In the Properties pane, on the General tab, click the transfer code that you want to delete. Press **Delete** on the keyboard to delete the transfer code. Likewise, you can delete multiple transfer codes.
3. Click the **Save**  button.

## Managing Not Ready Codes

To help supervisors and administrators track agent activity, Not Ready 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. You can map the Not Ready Codes in ECE with the Not Ready Reason Codes configured in Unified CCE or Packaged CCE.

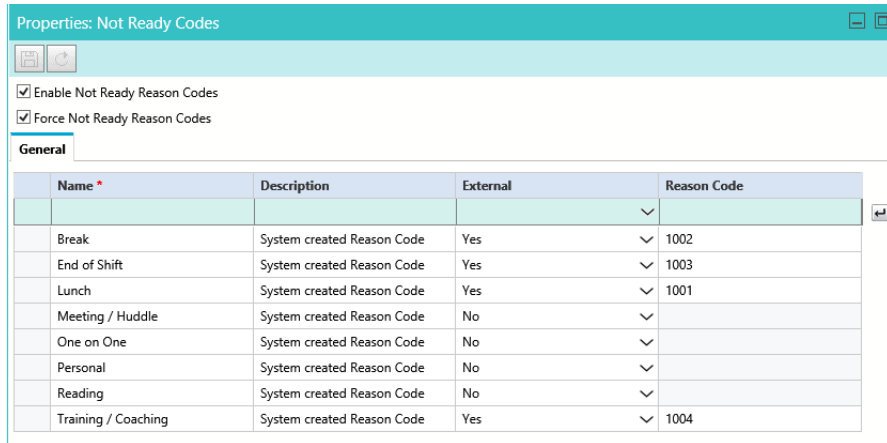
- ▶ [Creating Not Ready Codes on page 219](#)
- ▶ [Deleting Not Ready Codes on page 221](#)

## Creating Not Ready Codes

### To create a not ready code:

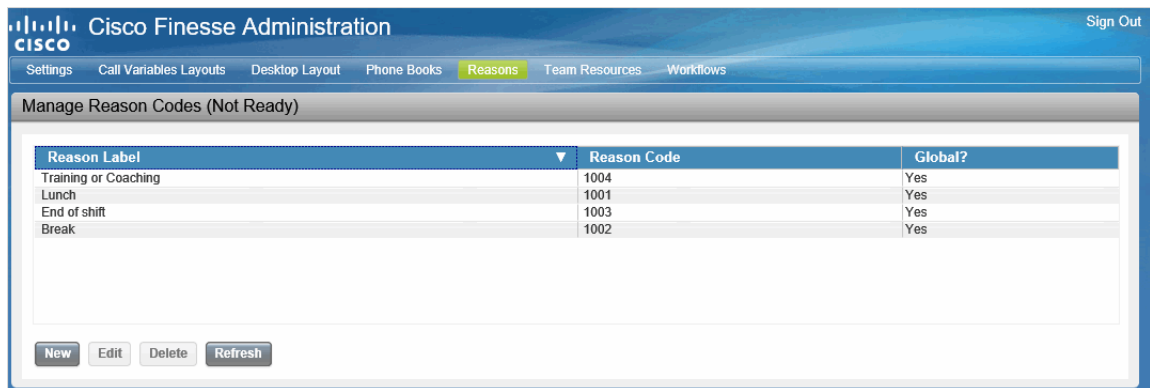
1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Classifications > Not Ready Codes**.

- Click the **Enable Not Ready Reason Codes** option to enable the use of the codes. If you wish to force agents to use the reason codes when they become unavailable, click the **Force Not Ready Reason Codes option**.



*Enable the reason codes*

- In the Properties pane, on the General tab, provide the following details.
  - Name:** Type the name of the Not Ready Code.
  - Description:** Provide a brief description.
  - External:** Select **Yes** if you are mapping the reason codes to the codes created in Unified CCE or Packaged CCE.
  - 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.




*Sample codes in Unified CCE*

- Click the **Save**  button.

## Deleting Not Ready Codes

### To delete a not ready code:

1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Classifications > Not Ready Codes**.
2. In the Properties pane, under the General tab, select the reason code you want to delete.
3. Push the **Delete** button on your keyboard to remove the reason code.
4. Click the **Save**  button.

## 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 221](#)
- ▶ [Deleting Categories on page 222](#)


## Creating Categories

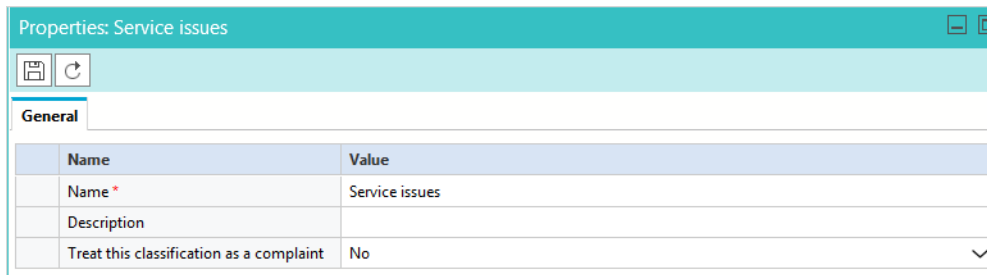
Categories and resolution codes can only be nested 3 levels deep.



**Important:** Up to 500 categories are supported per department.

### To create a category:

1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Classifications > Categories**.
2. In the List pane toolbar, click the **New**  button.
3. In the Properties pane, on the General tab, provide the following details.
  - **Name:** Type the name of the category.
  - **Description:** Provide a brief description.
  - **Treat the classification as a complaint:** Select **Yes** to create a complaint type of category.



The screenshot shows the 'Properties: Service issues' window. It has a teal header with window control buttons. Below the header is a toolbar with a Save icon and a Refresh icon. The 'General' tab is selected, showing a table with the following data:


Name	Value
Name *	Service issues
Description	
Treat this classification as a complaint	No

*Set general properties*

4. Click the **Save**  button.

## Deleting Categories

### To delete a category:

1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Classifications > Categories**.
2. In the List pane, select the category you want to delete.
3. In the List pane toolbar, click the **Delete**  button.

## Managing Resolution Codes


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

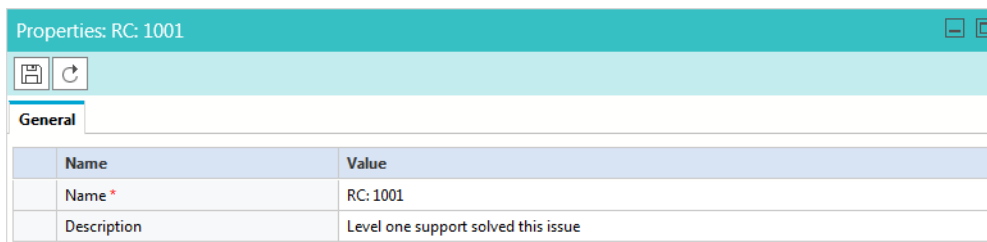
- ▶ [Creating Resolution Codes on page 222](#)
- ▶ [Deleting Resolution Codes on page 223](#)

## Creating Resolution Codes

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

### To create a resolution code:

1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Classifications > Resolution Codes**.
2. In the List pane toolbar, click the **New**  button.
3. In the Properties pane, on the General tab, provide the following details.
  - **Name:** Type the name of the resolution code.
  - **Description:** Provide a brief description.




Name	Value
Name *	RC: 1001
Description	Level one support solved this issue

*Set general properties*

4. Click the **Save**  button.

## Deleting Resolution Codes

### To delete a resolution code:

1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Classifications > Resolution Codes**.
2. In the List pane, select the resolution code you want to delete.
3. In the List pane toolbar, click the **Delete**  button.

# 15 Dictionaries

- ▶ [About Dictionaries](#)
- ▶ [Choosing a Default Dictionary](#)
- ▶ [Creating Dictionaries](#)
- ▶ [Adding Blocked Words](#)
- ▶ [Approving Suggested Words](#)
- ▶ [Viewing Approved Words](#)



This chapter will assist you in understanding what dictionaries are and how to configure them.

## 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 13 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 (Simplified), Chinese (Traditional), Czech, Greek, Japanese, Korean, Norwegian (Nynorsk), Portuguese (Brazilian), and Turkish.

---

## Choosing a Default Dictionary

---

**To choose a default dictionary:**

1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Dictionaries**.
2. In the List pane, select a dictionary.

- In the Properties pane, on the General tab, in the **Default** field, choose **Yes** from the drop down list.

Name	Value
Name *	English (UK) Dictionary
Description	English (UK) Dictionary
Language *	English (UK) <span>▼</span>
Default	No <span>▼</span>
	No
	Yes


*Set a dictionary as the default dictionary for a department*


- Click the **Save**  button.

## 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:

- In the Tree pane, browse to **Administration > Department > *Department\_Name* > Dictionaries**.
- In the List pane toolbar, click the **New**  button.
- In the Properties pane, on the General tab, provide the following details.
  - Name:** Provide the name of the dictionary.
  - Description:** Provide a brief description.
  - Language:** From the drop down list, select a language for the dictionary.

Click the **Save**  button to enable the **Default** field.

- Default:** Select **Yes** to make this the default dictionary of the department.

Name	Value
Name *	Custom dictionary
Description	
Language *	English (US) <span>▼</span>
Default	No <span>▼</span>

*Configure the general properties*



- Click the **Save**  button.

## 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, irrespective 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 add blocked words:



1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Dictionaries**.
2. In the List pane, select a dictionary.
3. In the Properties pane, on the Special words tab, go to the Blocked section.
4. Add the list of blocked words. If you want to delete a blocked word, select the word and click the **Delete**  button.
5. Click the **Save**  button.

## Approving 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 suggested words:

1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Dictionaries**.
2. In the List pane, select a dictionary.
3. In the Properties pane, on the Special words tab, go to the Suggested section.
4. 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 **Delete**  button.
5. Click the **Save**  button.

## Viewing Approved Words

---

### To view the approved words:

1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Dictionaries**.
2. In the List pane, select a dictionary.
3. In the Properties pane, on the Special words tab, go to the Suggested section.
4. View the list of approved words. To delete an approved word, select the word and click the **Delete**  button.
5. Click the **Save**  button.

# 16 Macros

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

This chapter will assist you in understanding what macros are and how to configure them.

## 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. For example, Activity data, Customer data, User data, and so on. You have to define an attribute to a macro from the list of system provided attributes. Please note that you can define only a single attribute for each macro.
2. **Combination macros:** In Combination Macros you can create 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.

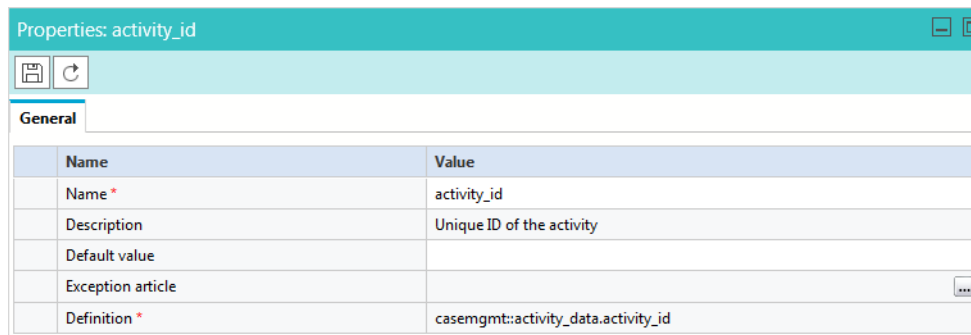
## Creating Business Object Macros


---

**To create a business object macro:**

1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Macros > Business Objects > *Business Object Name***.
2. In the List pane toolbar, click the **New**  button.
3. In the Properties pane, on the General tab, provide the following details.
  - **Name:** Type a name for the macro.
  - **Description:** Provide a brief description.
  - **Default value:** Provide the default value for the macro.
  - **Exception article:** Click the **Assistance**  button and from the Select Article window, select the exception article for the macro.

- **Definition:** Click the **Assistance**  button and from the Select Attribute window, 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.






Name	Value
Name *	activity_id
Description	Unique ID of the activity
Default value	
Exception article	
Definition *	casemgmt::activity_data.activity_id

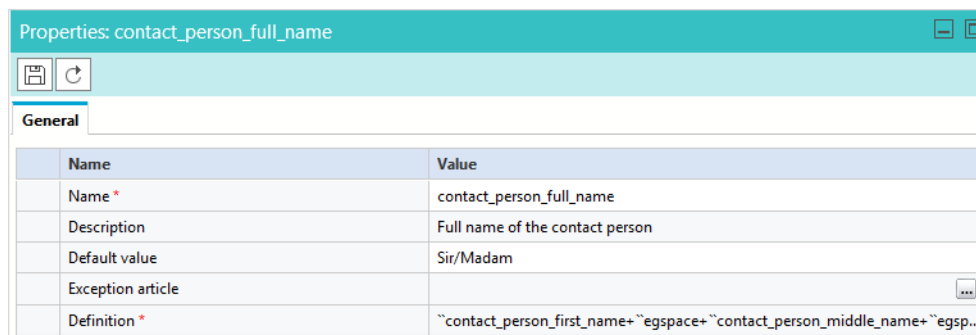
*Set general properties*


4. Click the **Save**  button.

## Creating Combination Macros

### To create a combination macro:

1. In the Tree pane, browse to **Administration > Department > Department\_Name > Macros > Combinations**.
2. In the List pane toolbar, click the **New**  button.
3. In the Properties pane, on the General tab, provide the following details.
  - **Name:** Type the name of the macro.
  - **Description:** Provide a brief description.
  - **Default value:** Provide the default value for the macro.
  - **Exception article:** Click the **Assistance**  button and from the Select Article window, select the exception article for the macro.
  - **Definition:** Click the **Assistance**  button and from the Select Definition window, select the attributes that define this macro.



Name	Value
Name *	contact_person_full_name
Description	Full name of the contact person
Default value	Sir/Madam
Exception article	
Definition *	``contact_person_first_name+``egspace+``contact_person_middle_name+``egsp...

*Set general properties*

4. Click the **Save**  button.

## Deleting Macros


---



**Important:** Macros used in workflows cannot be deleted.

---

### To delete a macro:

1. In the Tree pane, browse to **Administration > Department > *Department\_Name* > Macros**.
2. Select the type of macro you want to delete.
3. In the List pane, select the macro you want to delete.
4. In the List pane toolbar, click the **Delete**  button.

# Storage Management

- ▶ [About Storage Management](#)
- ▶ [Creating Purge Jobs](#)
- ▶ [Deleting Purge Jobs](#)



# 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 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.