



# **Enterprise Chat and Email Administrator's Guide to Administration Console, Release 12.6**

**For Unified and Packaged CCE**

First Published: May, 2021

Last Updated: March, 2026

## **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

## Copyrights and Trademarks

---

### **Enterprise Chat and Email Administration Console Help March 03, 2026**

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 <http://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)

© 2016-2025 Cisco Systems, Inc. All rights reserved.

# Contents

Copyrights and Trademarks.....	2
Preface.....	3
About This Guide.....	4
Change History.....	4
Related Documents.....	7
Communications, Services, and Additional Information.....	7
Cisco Bug Search Tool.....	7
Field Alerts and Field Notices.....	8
Documentation Feedback.....	8
Document Conventions.....	8
Integration.....	9
About CCE Integration.....	10
Configuring Integration.....	10
Configuring DRASR.....	12
Preparing to Create Dynamic Messages.....	13
Creating Dynamic Messages.....	13
Importing Data.....	15
Importing Media Routing Domains.....	15
Importing Users.....	16
CCE Integration Settings.....	17
Allow Transfer of Activities to Integrated Queues in Other Departments.....	17
Proactive Monitoring Refresh Interval (seconds).....	18
Reason Code for Agent Not Ready.....	18
Maximum Wait Time for Login Response From UCCE (seconds).....	18
Allow Transferring Email Activities to Agents Who Are Not Available.....	18
Allow Transferring Chats to Agents Who Are Not Available.....	19
Allow Transferring Email Activities to Agents Who Are Not Logged in.....	19
Allow Supervisor to Join an Ongoing Chat Session.....	19

Maximum Assignment Beyond Concurrent Task Limit .....	19
Manage Agent Availability for Call .....	20
Chat Watchdog Settings .....	20
Starvation Time for Activities .....	20
Media Class Names .....	21
Agent Availability Settings After Completion of Call .....	21
Concurrent Task Limit Mappings by Media .....	21
Popover Display Settings .....	22
Make Agent Unavailable For All Activities When Agent is Made Unavailable for Chat After Chat Auto-Pushback .....	22
Chat Auto-Complete Settings .....	23
Automatic Agent State Resynchronization .....	23
Calltrack Settings .....	24
Enable Chat Queueing .....	25
Manage Agent Availability for Call .....	25
<b>Partitions</b> .....	<b>26</b>
About the Partition .....	26
<b>Departments</b> .....	<b>27</b>
About Departments .....	29
Creating Departments .....	29
Copying Departments .....	31
Configuring Activity Transfer Between Departments .....	33
<b>User Management</b> .....	<b>34</b>
About User Roles and Actions .....	35
User Roles .....	35
Actions .....	35
Permissions .....	35
Partition Administrator Role .....	38
Administrator Role .....	39
Agent Role .....	41
Agent (Read Only) Role .....	51

Supervisor Role.....	52
Supervisor (Read Only) Role.....	54
Creating User Roles.....	55
Copying Roles.....	58
Restoring Roles.....	58
Creating User Subroles.....	59
About User Groups.....	60
Editing User Groups in Departments.....	60
Managing User Groups in the Business Partition.....	62
Creating User Groups in the Business Partition.....	62
Deleting User Groups in the Business Partition.....	65
About Users.....	65
Types of Department Users.....	66
Creating Partition Administrators.....	67
Editing User Details in Departments.....	72
Specifying a User's Manager in Departments.....	76
Deleting Users.....	78
<b>Access Restrictions.....</b>	<b>79</b>
About Blocking Visitors.....	80
Chat Block Visitors.....	80
IP Based Customer Throttling.....	80
Enabling Visitor Blocking.....	80
<b>Attachments.....</b>	<b>82</b>
About File Attachments.....	83
Blocking Attachment File Types.....	83
Allowing Attachment File Types.....	84
Enabling and Disabling Chat Attachments.....	84
Enabling and Disabling Email Template Attachments.....	85
Configuring File Attachment Settings.....	85
<b>Audit Log.....</b>	<b>87</b>
About Audit Log.....	88

Audit of Administration Objects .....	88
Viewing the Audit Log .....	89
<b>Certificate Management .....</b>	<b>91</b>
About Certificate Management .....	92
Creating Certificates .....	92
Deleting Certificates .....	93
<b>Cross-Origin Resource Sharing .....</b>	<b>94</b>
About Cross-Origin Resource Sharing .....	95
Enabling Cross-Origin Resource Sharing .....	95
Deleting Cross-Origin Resource Sharing Websites .....	96
<b>Rich Text Content Policies .....</b>	<b>97</b>
About Rich Text Content Policies .....	98
Enabling and Disabling Rich Text Content Policies .....	98
Configuring the Rich Text Content Policy File .....	99
Adding a Common Regular Expression .....	99
Allowing a New Tag .....	100
Allowing a New Attribute for a Tag .....	100
Adding a Rule for an Attribute Value .....	100
Adding Validation for Attributes .....	101
Allowing a New CSS Property .....	101
Adding a Rule for a CSS Property Value .....	102
Allowing Links in the Source Attribute of an iframe Tag .....	102
Using a Plain Text Policy .....	103
Exporting and Importing Rich Text Content Policies .....	103
Restoring Rich Text Content Policies .....	104
<b>Customer Single SignOn .....</b>	<b>105</b>
About Customer Single Sign-On .....	106
Customer Single Logout .....	106
Planning Your Configuration .....	107
Creating Identity Providers .....	107
Configuring Customer Single Sign-On .....	111

Enabling Chat Entry Points for Customer SSO.....	112
Configuring Your Website for Chat Customer SSO .....	112
Troubleshooting Chat Customer SSO.....	114
<b>Agent Single Sign-On.....</b>	<b>115</b>
About Agent Single Sign-On (SSO) .....	116
Preparing to Configure Single Sign-On.....	116
Integrating with Unified CCE or Packaged CCE .....	117
Configuring an Identity Provider .....	117
Creating and Importing Certificates.....	117
Configuring Agent Single Sign-On.....	117
Configuring SSO for Partition Administrators.....	121
Signing In with Single Sign-On .....	123
<b>Data Adapters.....</b>	<b>125</b>
About Data Adapters .....	126
Do You Need Data Links? .....	126
How Do Data Adapters Work?.....	126
Where and How Can You Use Data Links?.....	127
About Data Adapter Authentication.....	127
Configuring Basic Authentication.....	127
Configuring OAuth 2.0 Authentication .....	128
Deleting Authentication Configurations.....	130
About Access Links.....	131
Creating Web Service RESTful Links .....	131
Testing Access Links .....	134
Deleting Access Links .....	134
About Data Usage Links.....	135
Creating Usage Links.....	135
Configuring the Display of Results.....	138
Assigning Permissions on Usage Links .....	138
Testing Usage Links.....	139
Deleting Usage Links.....	139

About Usage Link Groups .....	140
Creating Usage Link Groups .....	140
Configuring the Display of Results.....	141
Assigning Permissions on Usage Link Groups.....	142
Deleting Usage Link Groups.....	143
Example One – Get Weather Information for a City.....	143
Example Two – Extract Stock Information From a Website.....	145
Configure Basic Authentication .....	145
Create the Access Link .....	146
Example Three – Shorten URLs Using Google API.....	148
Configure OAuth 2.0 Authentication .....	148
Create the Access Link .....	149
<b>Calendars.....</b>	<b>152</b>
About Business Calendars .....	153
Shift labels .....	153
Day labels.....	153
Managing Shift Labels.....	154
Creating Shift Labels.....	154
Deleting Shift Labels .....	154
Managing Day Labels.....	155
Creating Day Labels .....	155
Deleting Day Labels.....	157
Managing Business Calendars .....	157
Setting the Time Zone.....	157
Creating Business Calendars.....	157
Deleting Business Calendars.....	160
<b>Codes &amp; Classifications.....</b>	<b>161</b>
About Classifications .....	162
Categories.....	162
Resolution Codes.....	162
Transfer Codes.....	162

Not Ready Codes .....	162
Creating Categories .....	162
Deleting Categories .....	163
Creating Resolution Codes .....	163
Deleting Resolution Codes .....	164
Creating Not Ready Reason Codes .....	165
Enabling and Enforcing Not Ready Reason Codes .....	165
Deleting Not Ready Reason Codes .....	166
Creating Transfer Codes .....	166
Deleting Transfer Codes .....	167
<b>Macros</b> .....	<b>168</b>
About Macros .....	169
Creating Business Object Macros .....	169
Creating Combination Macros .....	170
Deleting Macros .....	171
<b>Dictionaries</b> .....	<b>172</b>
Setting Language Options for the User Interface .....	173
About Dictionaries .....	174
Creating Dictionaries .....	175
Choosing a Default Dictionary .....	176
Deleting Dictionaries .....	176
Viewing and Adding Blocked Words .....	177
Approving and Rejecting Suggested Words .....	177
Viewing and Adding Approved Words .....	178
Choosing a Default Dictionary .....	179
<b>Supervision Monitors</b> .....	<b>181</b>
About Supervision Monitors .....	182
Settings to View Bar Charts .....	182
Queue Attributes .....	183
General Attributes .....	183
Chat Activity Attributes .....	183

Email Activity Attributes .....	184
User Group Attributes .....	184
General Attributes .....	184
Chat Activity Attributes .....	184
Email Activity Attributes .....	184
User Attributes .....	185
General Attributes: .....	185
Chat Activity Attributes .....	185
Email Activity Attributes .....	185
Creating Supervision Monitors .....	186
Starting Monitors .....	189
Deleting Supervision Monitors .....	190
<b>Storage</b> .....	<b>191</b>
About Storage .....	192
Who Can Manage Storage? .....	192
View Data Storage .....	192
About Purge Jobs .....	192
What Can You Purge? .....	193
Planning Schedule of Purge Jobs .....	193
Creating Purge Jobs .....	194
Viewing Purge Job History .....	196
Deleting Purge Jobs .....	197
<b>System Resources</b> .....	<b>198</b>
About Process Logs .....	199
Processes Available in the System .....	200
Managing Logging for Processes .....	202
Viewing Logging Details for Processes .....	202
Changing the Logging for Processes .....	203
<b>Services</b> .....	<b>206</b>
About Services .....	207
Unified CCE .....	207

Email Services .....	207
General Services.....	207
Workflow Services .....	208
About Service Processes .....	208
Creating Service Processes.....	208
Deleting Service Processes .....	210
Starting Service Processes.....	211
Stopping Service Processes.....	211
Increasing the Number of Instances.....	211
About Service Instances.....	212
Creating Service Instances.....	212
Starting Service Instances.....	214
Stopping Service Instances.....	215
Deleting Service Instances .....	215
Adding Aliases to Retriever Instances.....	216
Configuring EAAS Service Instance.....	216
Configuring the MR Connection Port for an EAAS Service Instance .....	216
Configuring Security Settings for an EAAS Service Instance.....	217
Configuring EAMS Service Instance.....	219
Configuring Peripheral Gateway and CTI Server Details .....	219
Configuring Security Settings for an EAMS Service Instance.....	220
<b>Partition Tools .....</b>	<b>222</b>
About System Attributes.....	223
Creating Custom Attributes.....	223
Modifying System Attributes.....	226
Enabling Custom Attributes for Analytics.....	227
About Utilities .....	227
List User Sessions.....	228
Terminate Sessions .....	229
<b>Department Tools .....</b>	<b>230</b>
About Screen Attributes .....	231

Modifying Screen Attributes .....	232
About User Attribute Settings.....	233
Creating User Attribute Settings.....	233
Accessing Utilities .....	235
Complete Activities .....	235
Mask Content of Chat and Email Activities .....	236
<b>Settings.....</b>	<b>238</b>
About Settings.....	239
Configuring Partition Settings.....	239
Configuring Department Settings.....	240
Configuring Settings for a Department.....	240
Configuring Language Settings for a Department .....	240
Editing User Setting Groups.....	240
General Partition Settings .....	241
Common Settings.....	241
Security Settings.....	242
Search Settings .....	243
Proxy Server Settings.....	243
Default SMTP Server Settings.....	245
General Department Settings.....	248
General Department Settings.....	248
Activity Assignment Settings.....	248
Common Settings.....	249
Supervisor Monitor Settings.....	251
Activity Handling Settings.....	251
Agent Guidance Notifications .....	252
Chat Settings .....	253
Activity Assignment Settings.....	253
Inbox Settings.....	254
Activity Handling Settings.....	255
Common Chat Settings .....	257

Chat Service Level Settings .....	257
Preferred Agent Assignment for Activity Settings.....	258
Email Settings .....	260
Common Email Settings .....	260
Inbox Settings.....	262
Dispatcher and Retriever Settings .....	263
Workflow Settings.....	265
Activity Assignment Settings.....	267
Activity Handling Settings.....	269
Knowledge Settings .....	271
eGain Knowledge System.....	271
KB Primary Language.....	272
Custom Language Label.....	272
Language Settings.....	272
Ignore Words with Only Upper Case Letters.....	272
Ignore Words with a Mixture of Upper and Lower Case Letters .....	273
Ignore Words with Only Numbers or Special Characters .....	273
Ignore Words that Contain Numbers.....	273
Ignore Web Addresses and File Names .....	273
Auto Spellcheck.....	274
Auto Blockcheck .....	274
Split Contracted Words .....	274
Include Original Message Text During Spell Check.....	274
Chat Auto Blockcheck.....	275
Chat Auto Spellcheck .....	275
Preferred Dictionary of the User .....	275
Security Settings.....	276
Allow users to Change Password.....	276
Inactive Time Out (Minutes).....	276
Session Time Out (Minutes) .....	276
Allow Local Login for Partition Administrators .....	276
Customer Departmentalization.....	277

Appendix.....	278
Maximum Limits .....	279
Chat.....	279
Email.....	279
Administration.....	280

# Preface

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

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

## About This Guide

---

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

## Change History

---

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

Change	See	Date
Added a new note	<a href="#">Enabling and Disabling Rich Text Content Policies</a>	March, 2026
Added a new note	<a href="#">Configuring EAAS Service Instance</a>	February, 2026
Updated certificate instructions for domain-signed certificates.	<a href="#">Configuring EAAS Service Instance</a> <a href="#">Configuring EAMS Service Instance</a>	September 2025
Added a note for creating custom attributes for chat and callback templates	<a href="#">Creating Custom Attributes</a>	April 2025
Added a note about adding custom attributes to search screens	<a href="#">Modifying Screen Attribute Settings</a>	March 2025
Added details about 'Allowed MR Servers' field	<a href="#">Configuring EAAS Service Instance</a>	February 2025
Updated 'Default SMTP Server Settings' to include OAuth 2.0 authentication type	<a href="#">General Partition Settings</a>	January 2025
Added a new action <b>Show Email Redirect Option</b> for the agent role	<a href="#">Agent Role</a>	December 2024

Updated values for the Chat Watchdog Settings	<a href="#">CCE Integration Settings</a>	December 2024
Made changes for process logs description	<a href="#">About Process Logs</a>	November 2024
Added a new settings field for configuring Agent SSO outside of Finesse	<a href="#">Configuring Single Sign-On for Agents</a>	August 2024
Added a new setting for System Administration	System Settings	May 2024
Added the following field for configuring security settings for EAAS service instance: <b>Allowed MR Servers</b>	<a href="#">Configuring EAAS Service Instance</a>	April 2024
Removed note for using custom attributes	<a href="#">Creating Custom Attributes</a>	January 2024
Added missing screen attributes for the department	<a href="#">About Screen Attribute Settings</a>	December 2023
Added Automatic Agent State Resynchronization setting	<a href="#">CCE Integration Settings</a>	December 2023
Changed the values for the Number of days field while creating a Purge Job	<a href="#">Creating Purge Jobs</a>	July 2023
Added the Manage Agent Availability for Call setting	<a href="#">CCE Integration Settings</a>	June 2023
Added the following Calltrack settings: Enable Automatic Calltrack Activity Creation and Enable Call Related Events	<a href="#">CCE Integration Settings</a>	June 2023
Added a note about Packaged CCE installation	<a href="#">About CCE Integration</a>	March 2023
Added Require Activity Note on Transfer setting	<a href="#">Chat Settings</a>	March 2023
Added Proxy Server settings	<a href="#">General Partition Settings</a>	March 2023

Added Inactive Timeout setting (Minutes)	<a href="#">Security Settings</a>	March 2023
Added Maximum Assignment beyond Concurrent Task Limit setting	<a href="#">CCE Integration Settings</a>	March 2023
Added Enable Chat Queueing setting	<a href="#">CCE Integration Settings</a>	March 2023
Added a section on setting language options for the User Interface	<a href="#">Setting Language Options for the User Interface</a>	January 2023
Added details about the roles required to use Department Utilities	<a href="#">Complete Activities</a> <a href="#">Mask Content of Chat and Email Activities</a>	January 2023
Added details about User Attribute settings	<a href="#">About User Attribute Settings</a>	January 2023
Added details about the permissions for the Partition Administrator	<a href="#">About Service Instances</a> <a href="#">About Service Instances</a> <a href="#">Managing Logging for Processes</a>	January 2023
Added two new Chat Auto-Complete settings	<a href="#">CCE Integration Settings</a>	November 2022
Added a note about department sharing being disabled in ECE	<a href="#">Creating Departments</a>	October 2022
Added the maximum limits for creating various objects	<a href="#">Maximum Limits</a>	September 2022
Updated details about Expiry Time for Auto-Pushback of Chats setting	<a href="#">Chat Settings</a>	June 2022
Removed invalid Direct Reports references regarding user management chapter	<a href="#">User Management</a>	December 2021
Added details about generating an ECDSA certificate to configure	<a href="#">Configuring EAAS Service Instance</a>	September 2021

security settings for an EAAS service instance.		
Added details about generating an ECDSA certificate to configure security settings for an EAMS service instance.	<a href="#">Configuring EAMS Service Instance</a>	
Updated details about Expiry Time for Auto-Pushback of Chats setting	<a href="#">Chat Settings</a>	June 2022

## 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.

# Integration

- [About CCE Integration](#)
- [Configuring Integration](#)
- [Configuring DRASR](#)
- [Importing Data](#)
- [CCE Integration Settings](#)

## About CCE Integration

---

ECE comes equipped with out-of-the-box integration capabilities with Cisco's leading enterprise telephony software, Cisco Unified Contact Center Enterprise. The integrated solution enables businesses to extend their phone infrastructure to include email and chat. It enables a full view of the customer across phone and online channels, while ensuring end-to-end interaction tracking and consistent answers.

The process of integrating with Cisco Unified CCE can be easily performed from within the Administration Console by an administrator with partition permissions.

The partition administrator should have the following actions to perform these tasks:

- Integration - Create
- Integration - Edit
- Integration - View
- Integration - Delete

Before integrating your installation with Cisco Unified CCE, make sure Cisco Unified CCE is installed and prepared for integration.

For Packaged CCE, the Context Root Name is set as `system` by default and should not be changed. For more information, see *Enterprise Chat and Email Installation and Configuration Guide*.

For more information on how to configure and prepare your setup, see the *Enterprise Chat and Email Deployment and Maintenance Guide*.

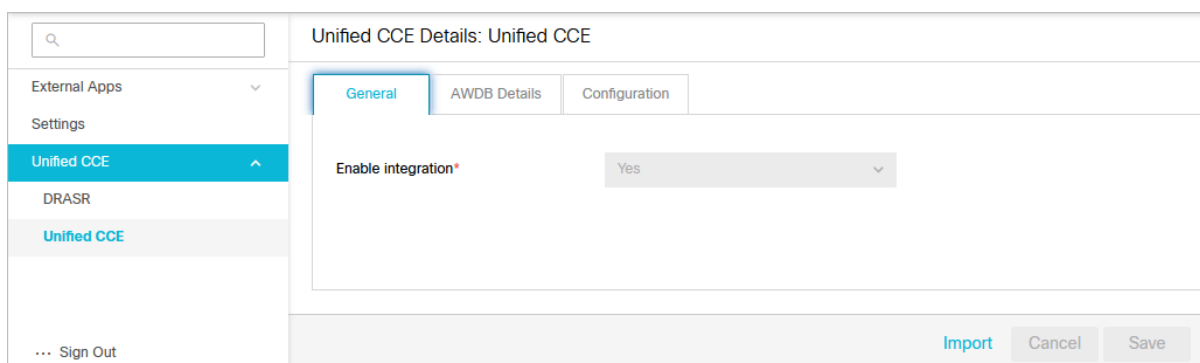
## Configuring Integration

---

**Note:** 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*.

To integrate ECE with Unified CCE:

1. In the global-level Top Menu, click the **Integration** option.
2. In the Left menu, navigate to **Unified CCE > Unified CCE**.



The screenshot shows the 'Unified CCE Details: Unified CCE' configuration page. On the left is a navigation menu with 'Unified CCE' selected. The main content area has three tabs: 'General', 'AWDB Details', and 'Configuration'. The 'General' tab is active, showing a form with a field 'Enable integration\*' set to 'Yes'. At the bottom right are 'Import', 'Cancel', and 'Save' buttons.

3. In the Unified CCE Details space, on the AWDB Details tab, provide information for the following fields under the Primary AWDB section:

- **Authentication:** From the dropdown menu, select the desired authentication type. Options include: **SQL Server Authentication** and **Windows Authentication**.
- **Unified CCE administration host name:** The server name or IP address of the host on which Packaged CCE or Unified CCE is installed.
- **Active:** Click the Toggle button to enable the configuration.
- **SQL server database name:** The name of the AWDB database.
- **Port number:** Set the value to match the database port configured in MSSQL for this database. By default the value is set to 1433.
- **Database administrator login name:** The database administrator user name.
- **Database administrator login password:** The database administrator password.
- **Maximum capacity:** The maximum number of allowed connections to be made to the AWDB. By default, this is set to 360.

4. Scroll down to the **Secondary AWDB** section and provide the necessary details.

The Secondary AWDB details must be provided to complete the integration process. The only instance in which it is optional to provide these details is while performing these integration steps on a test installation.

Unified CCE Details: Unified CCE

General | **AWDB Details** | Configuration

Primary AWDB

Authentication\* Windows Authentication

Unified CCE Administration Host Name\* ggnv70w8a.egeng.info

Active

SQL Server Database Name\* icm12\_awdb

Port Number\* 1433

Database Administrator Login Name\*

Database Administrator Login Password\* \*\*\*\*\*

Maximum Capacity\* 360

Secondary AWDB

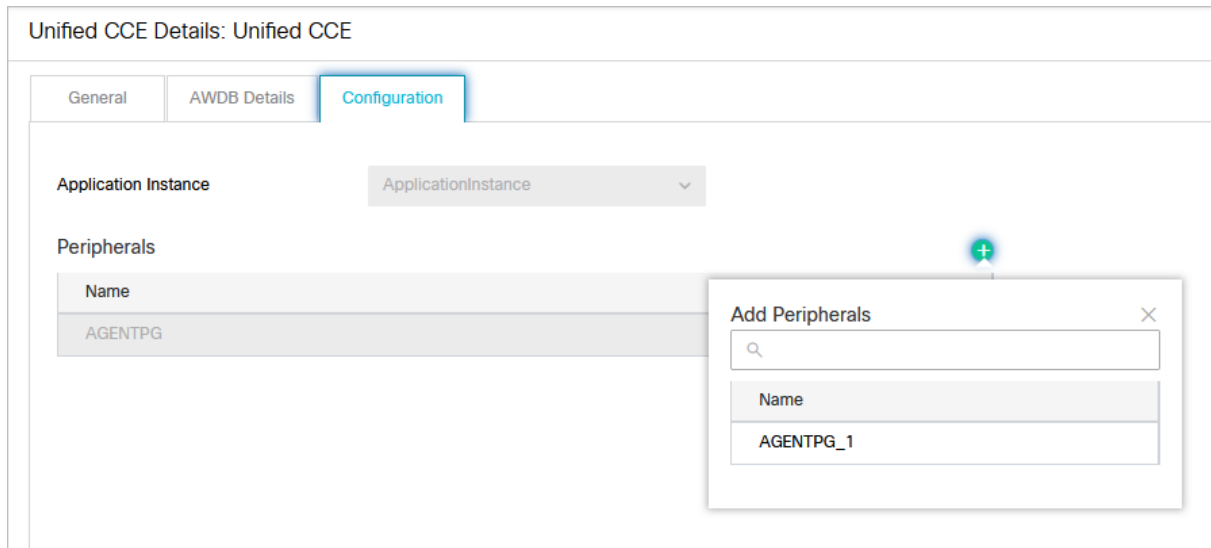
5. Click the **Save** button.

6. Click the **Configuration** tab and set the following:

- **Application Instance:** Select an instance from the dropdown field.

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

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



7. Click the **Save** button. Your system is now connected with Unified CCE.

Note that to complete the integration you must import the MRDs users and skill groups from the Unified CCE system and assign your media classes. For more information, see [Importing Data](#) and [CCE Integration Settings](#).

## Configuring DRASR

Dynamic Run Application Script Request (DRASR) allows you to display messages with dynamic text (such as expected wait time) to customers while chat and call requests are being processed by the ECE and Unified CCE integrated systems. While ECE provides wait time messages for chat customers to be handled by ECE agents by default, DRASR should be used if:

- You do not want to use the default wait time string.
- You wish to display wait time value that is calculated in Unified CCE at the time of the Unified CCE script being run.

External Apps		Unified CCE			
Name	Status	Display Message Is URL	Script Name	Description	
DRASR	● Enabled	Yes	Dynamic		

## Preparing to Create Dynamic Messages

---

You can use ECC variables and call variables to display the dynamic content. Dynamic messages can be displayed for chats and callback activities. The following steps elaborate the necessary configurations for creating dynamic messages for chat and callback activities:

- From Unified CCE, identify the ECC variables that you want to use in the dynamic messages. If these variables are not available, you can create them. For details about these objects and how they are used in Unified CCE, see the Scripting and Media Routing Guide for Cisco Unified ICM/ Contact Center Enterprise, Release 12.6(1), available here: [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cust\\_contact/contact\\_center/icm\\_enterprise/icm\\_enterprise\\_12\\_6\\_1/User/guide/ucce\\_b\\_scripting-and-media-routing-guide\\_12\\_6.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/User/guide/ucce_b_scripting-and-media-routing-guide_12_6.html).
- From Unified CCE, configure the Network VRU scripts and use them in the Unified CCE scripts used for chat or callback activities. You will need the name of the Network VRU script for configuring the dynamic messages. For details about doing these tasks, see the Scripting and Media Routing Guide for Cisco Unified ICM/ Contact Center Enterprise, Release 12.6(1), available here: [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cust\\_contact/contact\\_center/icm\\_enterprise/icm\\_enterprise\\_12\\_6\\_1/User/guide/ucce\\_b\\_scripting-and-media-routing-guide\\_12\\_6.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/User/guide/ucce_b_scripting-and-media-routing-guide_12_6.html).
- From the ECE Administration Console, identify the integrated chat queues for which you want to display the dynamic messages. To display the dynamic content using ECC variables, perform the following:

- The macro will be added in the format `%ECC <Variable_Name>%`. For example, `%ECCuser.ece.activity.id%` or `%ECCuser.ece.estimatedwaittime%`.

While selecting ECC variables to be used in macros, make sure that the variables have valid values. If you use a variable that does not have a value, a run application script failure will occur and the customer will not be able to chat. The error template is displayed to the customer.

- To display the dynamic content using call variable macros, prepare your macros by doing the following: From the Administration Console, from the Call Variables tab of the queue properties, identify the call variables you want to use in the message and note down the number associated with the call variable. For example, in the following figure the number for `customer_phone_no` is 1 and for `activity_id`, the number is 2. The macro is added in the format `%CVNumber%`. For example, `%CV1%` for `customer_phone_no`.

## Creating Dynamic Messages

---

To create dynamic messages:

1. In the global-level Top menu, click the **Integration** option.
2. In the Left menu, navigate to **Unified CCE > DRASR**.
3. Click the **New** button.
4. In the Create DRASR space, set the following:
  - **Name:** The name of the script as it will be identified in the application.

- **Script name:** From the dropdown, select the Network VRU script configured in Unified CCE. A script can be associated with only one message.
- **Enabled:** Click the Toggle button to enable DRASR.
- **Display message is URL:** If the message is a URL, set to **Yes**.

If enabled, the message must be a valid URL or it will not display properly.

- **Display message:** Provide the message that will be displayed to users upon accessing the entry point. If you have set the message to be a URL, provide a valid URL. In such cases, only provide the URL in the message and do not provide any text. A sample text message, with variable macros: An agent is expected to be available in approximately %ECCuser.wait.time% minutes. While you are waiting, checkout the latest offers on our website. For your record, please save the case number %CVcase\_ID%
- **Description:** The description of the script.

Create DRASR

Name*	<input type="text" value="DRASR_Custom"/>
Script Name*	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; width: 100%;" type="text" value="more.morecharactersent"/>
Enable	<input type="checkbox"/>
Display Message Is URL	<input type="checkbox"/>
Display Message*	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">An agent is expected to be available in approximately %ECCuser.wait.time% minutes.</div>
Description	<input type="text" value="DRASR with scripts in message"/>

5. Click the **Save** button.

After creating the dynamic message, in order for the value of the ECC variable that is populated by the Unified CCE (For example, the actual wait time as calculated by Unified CCE) to be reflected, you must map the ECC variable in the appropriate ECE Queue.

## Importing Data

Before the system can become fully integrated with your Unified CCE deployment, data from 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.


Make sure the integration settings have been configured before importing any data. For more information, see [Configuring Integration](#)

## 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 (see [CCE Integration Settings](#)). If you do not see the correct MRDs available for importing, check to make sure that the Media Classes names configured in the setting match the configuration in Unified CCE. Note that media class names are case sensitive.

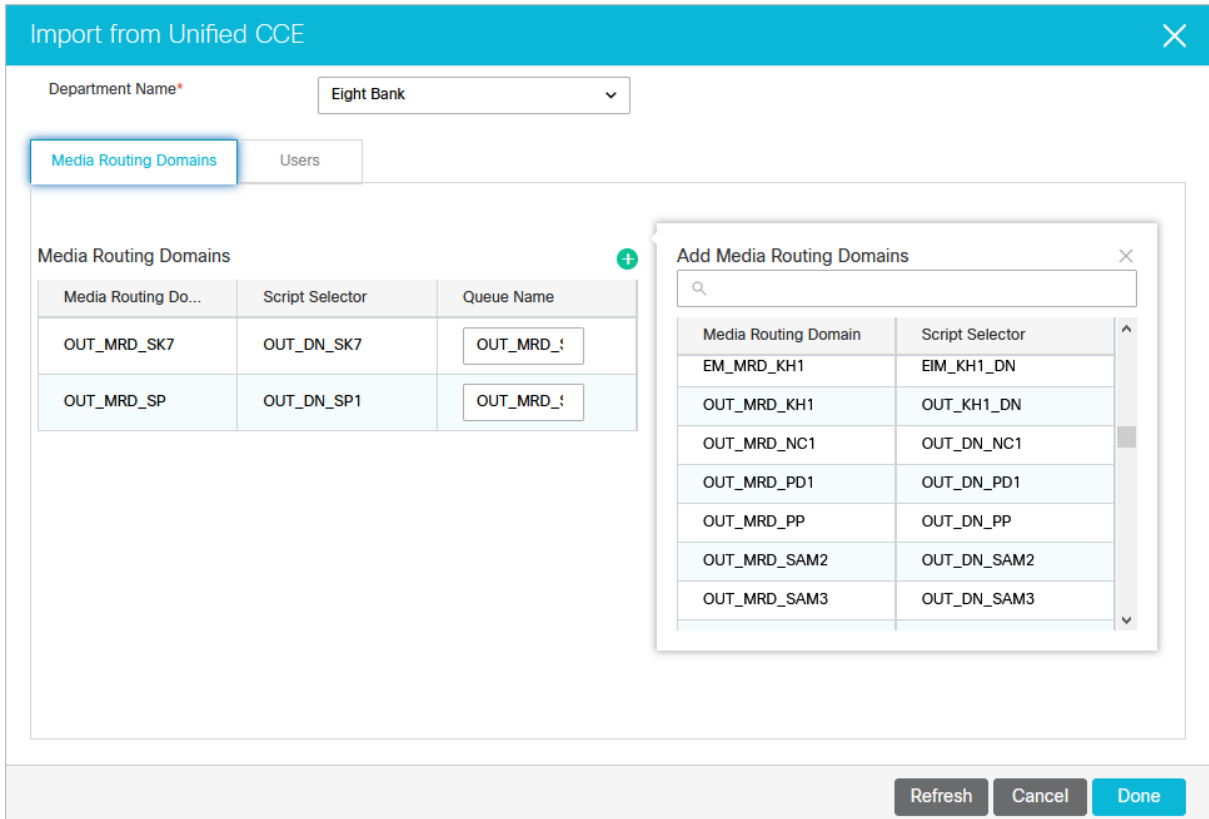
### To import MRDs:

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

5. Under the Media Routing Domains tab, click the **Search and Add**  button and select the MRDs you wish to import.

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

6. 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. All skill groups and precision queues that are mapped to the imported MRD are also automatically imported to the application.



Media Routing Do...	Script Selector	Queue Name
OUT_MRD_SK7	OUT_DN_SK7	OUT_MRD_!
OUT_MRD_SP	OUT_DN_SP1	OUT_MRD_!

Media Routing Domain	Script Selector
EM_MRD_KH1	EIM_KH1_DN
OUT_MRD_KH1	OUT_KH1_DN
OUT_MRD_NC1	OUT_DN_NC1
OUT_MRD_PD1	OUT_DN_PD1
OUT_MRD_PP	OUT_DN_PP
OUT_MRD_SAM2	OUT_DN_SAM2
OUT_MRD_SAM3	OUT_DN_SAM3

7. Click the **Done** button.

## Importing Users

The process outlined in this section is only for importing Unified CCE users to the ECE application. The process of integrating Packaged CCE users to the ECE application is different. For more details about enabling Packaged CCE users for ECE, consult your Packaged CCE documentation.

### To import Unified CCE users:

1. In the global-level Top Menu, click the **Integration** option.
2. In the Left menu, navigate to **Unified CCE > Unified CCE**.
3. In the Unified CCE Details space, click the **Import** button. The Create Import from Unified CCE window appears.

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

The screenshot shows the 'Import from Unified CCE' dialog box. The 'Department Name' dropdown is set to 'Eight Bank'. Under 'Media Routing Domains', the 'Users' tab is selected. The 'Peripheral Gateway' dropdown is set to 'AGENTPG' and the 'Peripheral' dropdown is set to 'AGENTPG\_1'. A pop-up window titled 'Add Users in this Department' is open, showing a search for 'Alex' and a table of results.

First Name	Last Name	User Name
Alex	Chestak	achestak
Alex1	Ch	alex1_ch

6. Click the **Done** button.

Once users have been imported to ECE, they can log into the application using their Unified CCE login credentials. The login credentials of a user in ECE is case-sensitive and must match their Unified CCE credentials.

Newly imported users may still need to have user roles assigned. For more information about user roles, see [About User Roles and Actions](#).

## CCE Integration Settings

### Allow Transfer of Activities to Integrated Queues in Other Departments

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

This setting applies to email and chat activities.

- **Access Level:** Partition settings
- **Default value:** Yes
- **Value options:** Yes, No

## Proactive Monitoring Refresh Interval (seconds)

---

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

- **Access Level:** Partition settings
- **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. This setting must be changed only if the default reason code 2 is currently used to track some other agent status.

- **Access Level:** Partition settings
- **Default value:** 2
- **Minimum value:** 0
- **Maximum value:** 32767

## 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.

- **Access Level:** Partition settings
- **Default value:** 20
- **Minimum value:** 20
- **Maximum value:** 120

## Allow Transferring Email Activities 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.

- **Access Level:** Partition settings
- **Default value:** Yes

- **Value options:** Yes, No

## Allow Transferring Chats to Agents Who Are Not Available

---

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

- **Access Level:** Partition settings
- **Default value:** Yes
- **Value options:** Yes, No

## Allow Transferring Email Activities to Agents Who Are Not Logged in

---

Use this setting to allow email activities to be transferred to agents who are not logged in. **Note:** If you are wish to enable this setting, the **Enable Autopushback** setting must first be disabled. The two settings cannot be enabled simultaneously.

- **Access Level:** Partition settings
- **Default value:** No
- **Value options:** Yes, No

## Allow Supervisor to Join an Ongoing Chat Session

---

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

- **Access Level:** Partition settings
- **Default value:** No
- **Value options:** Yes, 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 details, see Picking, Pulling, and Transferring Activities.

- **Access Level:** Partition settings
- **Default Value:** 0
- **Minimum:** 0

- **Maximum:** 2

## Manage Agent Availability for Call

---

- **Access Level:** Partition settings
- **Default value:** No
- **Value options:** Yes, No

## Chat Watchdog Settings

---

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

- **Access Level:** Partition settings
- **Default values:**
  - **Web Chat (in seconds):** 70
  - **Messaging Chat (in minutes):** 210
- **Value options:**
  - **Web Chat (in seconds):** 70-12601
  - **Messaging Chat (in minutes):** 5-210
- **Maximum value (Web Chat):** 12601 (3.5 hours)

## 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. The 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 the chat activity, it will process the chat activity first before processing the next call activity.

- **Access Level:** Partition settings
- **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

## 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.

- **Access Level:** Partition settings
- **Default value:** Custom
- **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.

## Agent Availability Settings After Completion of Call

---

### 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.

- **Access Level:** Partition settings
- **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 must change this setting only if the default reason code 32767 is currently used to track some other status in Finesse.

- **Access Level:** Partition settings
- **Default value:** 32767
- **Value options:** -

## 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 details, see [Creating Queues](#).

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

- **Access Level:** Partition settings
- **Default values:**
  - **Chat Media Class:** 1
  - **Email Media Class:** 1
  - **Outbound Media Class:** 1
- **Minimum values:**
  - **Chat Media Class:** 1
  - **Email Media Class:** 1
  - **Outbound Media Class:** 1
- **Maximum value:**
  - **Chat Media Class:** 10
  - **Email Media Class:** 10
  - **Outbound Media Class:** 10

## Popover Display Settings

---

Use this setting to configure counter type and display time for popover notifications.

- **Access Level:** Partition settings
- **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

## Make Agent Unavailable For All Activities When Agent is Made Unavailable for Chat After Chat Auto-Pushback

---

Use this setting to make agent unavailable for email, and voice activities if agent is marked unavailable for chat once chat activity is auto pushed back from the agent's inbox.

- **Access Level:** Partition settings

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

## Chat Auto-Complete Settings

---

### Autocomplete unselected and abandoned real time chat activity

Use this setting to auto-complete real time chats from the agent's inbox that are unselected and have been abandoned by the customer. The time after which the chat is completed from the agent's inbox is determined by the Expiry Time for Auto-Pushback of Chat setting.

- **Access Level:** Partition settings
- **Default values:** Yes
- **Value options:** Yes, No

### Autocomplete unselected and abandoned async chat activity

Use this setting to auto-complete messaging APIs initiated chats from the agent's inbox that are unselected and have been abandoned by the customer. The time after which the chat is completed from the agent's inbox is determined by the Expiry Time for Auto-Pushback of Chat setting.

- **Access Level:** Partition settings
- **Default values:** No
- **Value options:** Yes, No

## Automatic Agent State Resynchronization

---

Use this setting to forcefully resync the agent availability states for UCCE integrated deployments in events when there are any agent state synchronization issues between eGain and UCCE. This is helpful when invalid agent state mismatch responses are sent by UCCE against task assignments. To enable this setting, configure the following:

You need to restart the EAMS process and instance from the Partition level for these settings to take effect.

### Enable Automatic Agent State Sync

Enables or disables automatic synchronization of agent availability states.

- **Access Level:** Partition settings
- **Default value:** Disable
- **Value options:** Enable, Disable

## Frequency of Agent State Sync (minutes)

Duration of time between the last sync and next sync. This is the time in minutes, the system waits after the last successful sync, before resyncing the agent states. This option is available only if the **Enable Automatic Agent State Sync** setting is enabled.

- **Access Level:** Partition settings
- **Default value:** 10
- **Minimum value:** 10
- **Maximum value:** 1440 (24 hours)

## Failure threshold for invalid agent state reason code

Number of invalid agent state failure occurrences, after which the system resyncs the agent availability states. This option is available only if the **Enable Automatic Agent State Sync** setting is enabled.

- **Access Level:** Partition settings
- **Default value:** 10
- **Minimum value:** 10
- **Maximum value:** 1000

## Calltrack Settings

---

### Enable Automatic Calltrack Activity Creation

Calltrack activities can be created automatically or manually. To enable automatic creation of calltrack activities, this setting should be enabled along with the **Enable call related events** setting.

- **Access level:** Partition settings; Department settings
- **Default value:** Disable
- **Value options:** Enable, Disable
- **Editable at a lower level:** Yes

### Enable Call Related Events

Calltrack activities can be created automatically or manually. To enable automatic creation of calltrack activities, this setting should be enabled along with the **Enable automatic calltrack activity creation** setting.

- **Access level:** Partition settings
- **Default value:** Disable
- **Value options:** Enable, Disable

## 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** setting.

- **Access level:** Partition settings
- **Default value:** Yes
- **Value options:** Yes, No
- **Editable at lower level:** Yes

## Manage Agent Availability for Call

---

This setting allows customers to determine whether or not to submit agent availability state to Unified CCE after the completion of a call. If this setting is enabled, then the agent availability is submitted to Unified CCE after the call is completed. If this setting is disabled, then the agent availability is not submitted to Unified CCE after the completion of the call.

- **Access level:** Partition settings
- **Default value:** No
- **Value options:** Yes, No
- **Editable at lower level:** No

# Partitions

- [About Departments](#)

## About the Partition

---

The partition is the global space where all elements that apply to the complete system reside. In the partition space, you can:

- [Manage partition administrators.](#)
- [Create new departments.](#)
- Manage security configurations for the system, such as [blocked visitors](#), [attachment restrictions](#), or [audit logs](#).
- [Manage storage usage for the system.](#)
- Configure [partition](#) and [department](#) settings.
- [Manage screen attributes.](#)

# Departments

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



## About Departments

---

As organizations grow, they may need to form various departments to meet their requirements and divide their workforce accordingly. Departments within the application enable administrators to divide the resources as they choose, or even form a mirror of the departments in their company if necessary.

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 department.

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 following business objects are available in departments:

- Calendars
- Chat
- Classifications
- Dictionaries
- Email infrastructure
- Data adapters
- Macros
- Security
- Data Masking
- Settings
- Users
- Workflows

## Creating Departments

---

The process outlined in this section is only for installations that are integrated with Unified CCE. The process of creating departments in ECE installations that are integrated with Packaged CCE is different. For more details, consult your Packaged CCE documentation.

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

Only a partition administrator can create or copy departments. Once a department is created in ECE, it cannot be deleted.

You can create a department in two ways:

- Create a new department

- [Create a copy of an existing department](#)

To create a department:

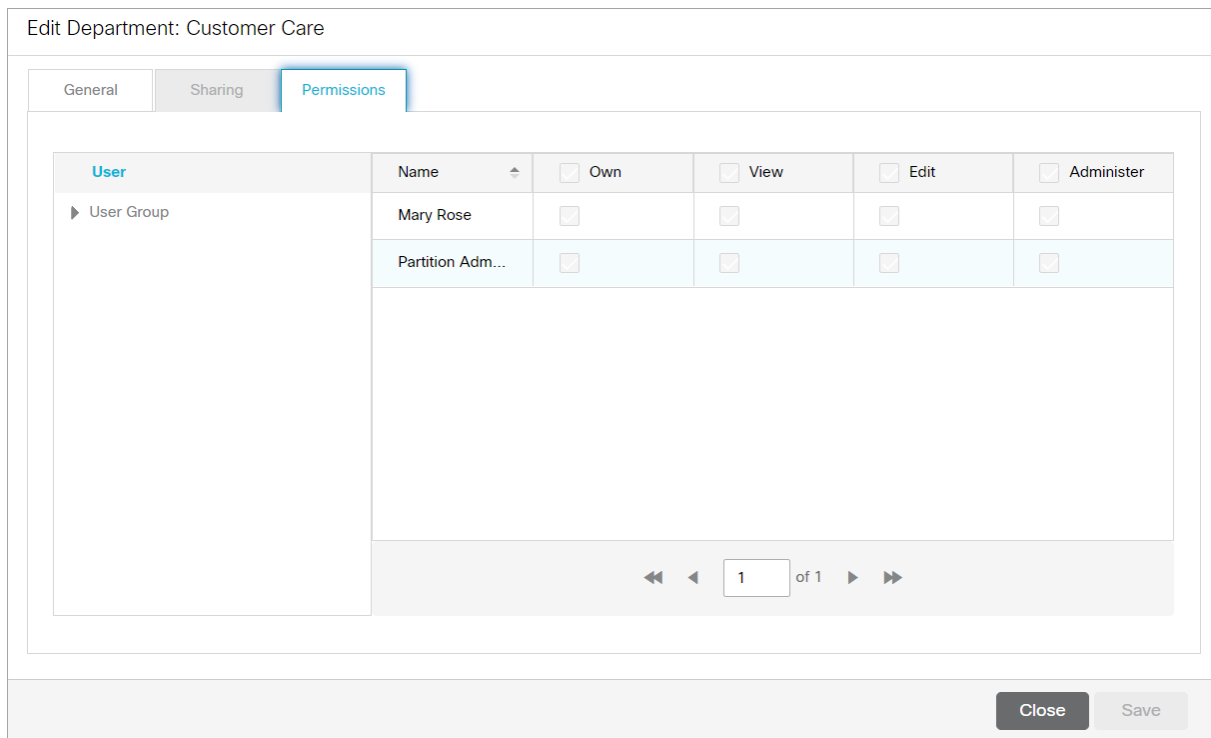
1. In the partition-level Top menu, click the **Departments** option.
2. On the Departments space, click the **New** button.
3. In the Create Department space, go to General tab and provide the following details:
  - **Name:** Type a name for the job.
  - **Description:** Provide a description for the job.

The following characters are not allowed in the name: ~ ` ! # \$ % ^ \* = ( ) [ ] ; : ' " | < > , / ? + \ { \}

The screenshot shows a 'Create Department' dialog box with three tabs: 'General', 'Sharing', and 'Permissions'. The 'General' tab is active. It contains two input fields: 'Name\*' with the value 'Customer Care' and 'Description' which is empty. At the bottom right, there are 'Close' and 'Save' buttons.

Department sharing is not supported in ECE and the Sharing tab is disabled by default.

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.



5. Click the **Save** button.

## 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>	
<b>Aliases</b>	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>
<b>Blocked file extensions</b>	Copied as in original department
<b>Calendars, day labels, shift labels</b>	Copied as in original department

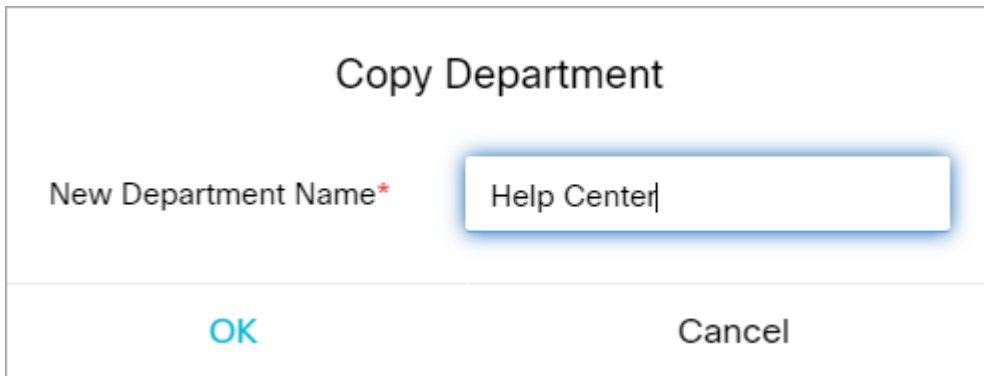
<b>Object name</b>	<b>Notes</b>
<b>Chat entry points</b>	Copied as in original department
<b>Classifications</b>	Copied as in original department
<b>Data Adapter Links (Access and Usage)</b>	Copied as in original department
<b>Data masking for email and chat channels</b>	Not copied
<b>Delivery Exceptions</b>	Copied as in original department
<b>Dictionaries</b>	Copied as in original department
<b>Macros</b>	Copied as in original department
<b>Monitors</b>	Copied as in original department
<b>Queues</b>	Copied as in original department
<b>Service levels</b>	Copied as in original department
<b>Settings</b>	Copied as in original department
<b>Transfer codes</b>	Copied as in original department
<b>User groups</b>	Copied as in original department
<b>User roles</b>	Copied as in original department
<b>Users</b>	<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><b>Note:</b> Permissions are disabled for the copied users until licenses are assigned to them.</p>
<b>Workflows</b>	<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>Screen Attribute Settings</b>	Copied as in the original department

Object name	Notes
Quick Links	Copied as in the original department
Quick Responses	Copied as in the original department
Headers	Copied as in the original department
Footers	Copied as in the original department
Greetings	Copied as in the original department
Signatures	Copied as in the original department

To copy a department:

1. In the partition-level Top menu, click the **Departments** option.
2. On the Departments space, select the department you want to copy.
3. Click the **Actions** button  and select the **Create Copy** option.
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.

The following characters are not allowed in the name: ~ ` ! # \$ % ^ \* = ( ) [ ] ; : ' " | < > , / ? + \ { \ }



## Configuring Activity Transfer Between Departments

In integrated 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. Mapped agents now see mapped queues (that belong to the same MRD) in their home department and in all foreign departments in the Transfer window in the Agent Console.

# User Management

- [About User Roles and Actions](#)
- [Partition Administrator Role](#)
- [Administrator Role](#)
- [Agent Role](#)
- [Agent \(Read Only\) Role](#)
- [Supervisor Role](#)
- [Supervisor \(Read Only\) Role](#)
- [Creating User Roles](#)
- [Copying User Roles](#)
- [Restoring Roles](#)
- [Creating User Subroles](#)
- [About User Groups](#)
- [Editing User Groups in Departments](#)
- [Creating User Groups in the Business Partition](#)
- [About Users](#)
- [Creating Partition Administrators](#)
- [Editing User Details in Departments](#)
- [Deleting Users](#)

# About User Roles and Actions

---

## User Roles

---

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

The default user roles are:

1. **Administrator:** The administrator is the manager of system and has access to the Administration Console. The administrator is automatically created while installing the application. Additional administrators in ECE can be created when an administrator from Unified CCE logs in to the ECE Administration Console.
2. **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 created by the administrator of the department.
3. **Agent (Read Only):** An agent (read only) will have access to the Agent Console, but he cannot compose replies for the customer queries. He can only view them. This role can be assigned to trainees.
4. **Supervisor:** A supervisor creates monitors for queues, user groups, and users in a department. They can also create and run reports from the Administration Console. The supervisor role cannot be assigned to users manually but are assigned by default if the user is a supervisor in Unified CCE.
5. **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.

## Actions

---

When you create a user role, you need to specify 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.

Partition administrators that are created in ECE and access the application through the Cisco Administration Console, cannot change permissions of users in the ECE application. These users must have an ECE administrator account that was created during the installation or imported.

Queue permissions are assigned automatically based on the MRDs that were imported. These permissions cannot be changed in ECE.

## Important Things to Note About Permissions to Pick and pull 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 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.
- 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.
- Agents with the **Administrator Role** or the **Supervisor Role** can pick from the Default exception queue.

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.

For installations that have upgraded from a version prior to 12.0(1) and are integrated with Unified or Packaged 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 or Packaged 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.

### 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** setting is enabled, agents can transfer activities to queues of other departments.
- If the **Allow email transfer to agents who are not available** 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** 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** setting is enabled, agents can transfer activities to queues of other departments.
- A chat can be transferred to any queue that belong to the same media class. From there, the activity is routed based on the queue-to-script mapping.

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

### Transferring Chats to Agents:

- Agents who do not meet these conditions are not displayed in the transfer window.
- Agents can transfer chats to other agents that belong to the same set of skill groups.
- Only agents who are part of a skill group that is associated with a queue can transfer chats to that queue.
- The receiving agent must be logged in to the application.
- The receiving agent must be available, depending on how the **Allow chat transfer to agents who are not available setting** is configured.
- The receiving agent should not have met the concurrent task limit, unless you are working on non-interruptible chat activities. This may be affected by the **Maximum assignment beyond concurrent task limit** setting.
- Based on the **Maximum assignment beyond concurrent task limit** setting, agents can transfer additional activities to agents who have reached their concurrent task limit. The maximum number of activities is defined as part of the setting.
- If the **Allow chat transfer to agents who are not available** 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.

## Partition Administrator Role

---

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

<b>Resource Name</b>	<b>Actions Permitted</b>
System Attribute Profiles	View, Edit
Application Security	Manage Application Security, View Application Security
System Resources	View Reports, View Administration
Report	Create, Delete, View, Run, Edit, Schedule
Reference Objects	Create, View, Edit
Preference Group	Create, View, Edit, Delete
Storage	View Data Storage, Manage Data Storage
Partition	Administer, View, Edit, Own
Integration	Create, View, Edit, Delete
Monitor	Create, Edit, Delete, Run
Messaging	Create Message, Delete Message
Instance	Create, View, Edit, Delete, Start, Stop
Activity Shortcuts	Create, Read, Edit, Delete
Department	Create, View, Own, Edit, Administer, Copy

## Administrator Role

---

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

<b>Resource Name</b>	<b>Actions Permitted</b>
Administration Console	View
Agent Console	View
Reports 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

<b>Resource Name</b>	<b>Actions Permitted</b>
User Group	Create, Own, View, Edit, Delete
Role	Create, View, Edit, Delete
User Attribute Profiles	Create, View, Edit, Delete
Department Security	Manage Department Security, View Department Security
Screen Attributes Profiles	View, Edit
Category	Create, View, Edit, Delete
Customer	Create, View, Edit, Delete, Change
Contact Person	Create, Edit, Delete
Contact Details	Create, Edit, Delete
Association	Create, View, Edit, Delete
Inbox Folder	Create, Delete
Notes	View, Delete
Resolution Codes	Create, View, Edit, Delete
Customer Associations	Create, View, Edit, Delete
Macro	Create, View, Edit, Delete
Product Catalog	Create, View, Edit, Delete
Business Objects	Create, View, Edit, Delete
Case	Edit, Print, Close
Monitors	Create, Edit, Delete, Run
Reports	Create, Delete, View, Run, Edit, Schedule
Queue	Create, Own, View, Edit, Delete
Workflow	Create, View, Edit, Delete
Settings	Create, View, Edit, Delete
Shift Label	Create, View, Edit, Delete
Day Label	Create, View, Edit, Delete

<b>Resource Name</b>	<b>Actions Permitted</b>
Calendar	Create, View, Edit, Delete
Dictionary	Create, View, Edit, Delete
Search Console	View
Partition Search	Create, Edit, Delete
Service Levels	Create, Read, Edit, Delete
Personal Search	Create
Alias	Create, View, Edit, Delete
Blocked Addresses	Create, View, Edit, Delete
Delivery Exceptions	Create, View, Edit, Delete
Blocked File Extensions	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
Blocked Attachment	Restore
Incoming Attachment	Delete
KB Folder	Create Article, Edit Article , Print Article, Delete Article

## Agent Role

---

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

<b>Resource Name</b>	<b>Actions Permitted</b>
Agent Console	View

<b>Resource Name</b>	<b>Actions Permitted</b>
User	View
Category	View
Customer	Create, View, Edit, Delete, Change
Contact Person	Create, Edit, Delete
Contact Details	Create, Edit, Delete
Association	Create, View, Edit, Delete
Inbox Folder	Create, Delete
Notes	View, Add, Delete
Resolution Codes	View
Folder	View
Personal Folders	Manage
Macro	View
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
Queue	View
Personal Dictionary	Create
Search Console	View
Personal Search	Create
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, Show Email Redirect Option (This

Resource Name	Actions Permitted
	is an explicitly assigned action that enables the <b>Redirect</b> button in the agent console)
Blocked Attachment	Restore
Incoming Attachment	Delete

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

Resource Name	Actions Permitted	Description
Activity	Create	Enables the <b>Create activity</b> button in the Main Inbox toolbar.
	Complete	Enables the <b>Complete</b> button in the Reply pane toolbar when working on email or custom activities.
	Send and Complete	Enables the <b>Send and Complete</b> button in the Reply pane toolbar when working on email activities.
	Pin	Enables the <b>Pin</b> option in the <b>More</b> button in the Main Inbox toolbar.
	Print	<p>Enables the <b>Print</b> button in the following toolbars:</p> <ul style="list-style-type: none"> <li>▪ The Main Inbox toolbar</li> <li>▪ The toolbar in the Activity Body section of the information pane</li> <li>▪ The toolbar in the Case Details section of the information pane</li> <li>▪ The Search Console toolbar, while searching for activities</li> </ul> <p><b>Note:</b> In the Print window (which opens on clicking the <b>Print</b> button), only the <b>Summary of activities assigned to me</b> and <b>Currently selected activity contents</b> options are enabled. The <b>Currently selected case contents</b> is enabled only when the <b>Print Case</b> action is assigned to an agent.</p>

Resource Name	Actions Permitted	Description
	Unpin	Allows an agent to pull pinned activities from other agents.
	Pull Activities	<p>Enable the <b>Pull</b> button in the Main Inbox toolbar. To be able to pull activities using this button, the agent needs:</p> <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>
	Pick Activities	<p>Enable the <b>Pull Activities</b> button in the Main Inbox toolbar. To be able to pull activities (other than chats) using this button, an agent needs:</p> <ul style="list-style-type: none"> <li>▪ <b>Pick Activities</b> action for routing queues.</li> <li>▪ <b>Pick Activities</b> action for users.</li> <li>▪ <b>Pick Activities</b> permission on queues.</li> <li>▪ <b>Pick Activities</b> permission on users.</li> </ul>
	Transfer Activities	<p>Enable the Transfer button in the Main Inbox toolbar, the Chat Inbox toolbar, and the Reply pane toolbar. To be able to transfer activities using this button, an agent needs:</p> <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 Classifications section of the Information pane, so that agents can assign categories and resolution codes to activities.
	Edit	Allows an agent to edit the case details. Enables the <b>Save</b> button in the Information pane, Case Details section. The <b>Case status</b> field is enabled only if the agent has the <b>Close Case</b> action.
	Print	Enables the Print preview button in the following toolbars:

Resource Name	Actions Permitted	Description
		<ul style="list-style-type: none"> <li>▪ The Main Inbox toolbar</li> <li>▪ The toolbar in the Activity Body section of the information pane</li> <li>▪ The toolbar in the Case Details section of the information pane</li> <li>▪ The Search Console toolbar, while searching for cases</li> <li>▪ Inbox Tree pane &gt; My Work &gt; Cases &gt; My Cases &gt; Open and Closed</li> </ul> <p><b>Note:</b> In the Print Preview window (which opens on clicking the <b>Print preview</b> button), only the <b>Currently selected case contents</b> option is enabled. The <b>Summary of activities assigned to me</b> and <b>Currently selected activity contents</b> options are enabled only when the <b>Print Activity</b> action is assigned to an agent.</p>
	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 Details 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 Details 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 Details section.
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.

Resource Name	Actions Permitted	Description
	Pull Chat Activities	<p>Allows an agent to pull chat activities from queues. To be able to pull chat activities the agent also needs:</p> <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>
	Transfer Chat Activity	<p>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:</p> <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>
Customer	Create	<p>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 Customer</b> button) from the Information pane, Customer section.</p> <p>Agents can also create new customers while creating new activities. In the New Activity Window (which opens on clicking the <b>Create Activity</b> button in the Inbox pane toolbar), it displays the <b>New</b> option in the <b>Customer</b> field.</p>
	Edit	<p>Allows an agent to edit the details of a customer. It enables the <b>Save</b> button in the Information pane &gt; Customer section toolbar.</p>
	Delete	<p>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.</p>
	Change Customer	<p>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.</p>

Resource Name	Actions Permitted	Description
	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>

Resource Name	Actions Permitted	Description
		button in the Information pane, Customer section when an association is selected.
Email	Send Email	Enables the <b>Send</b> button in the Reply pane toolbar.
	Show Email Redirect Option	Enables the <b>Redirect</b> button for agents in the Reply pane toolbar.
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 clicks the <b>Attachment</b> button in the Information pane, Activity Body section toolbar.
	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 clicks the <b>Attachment</b> button in the Information pane, Activity Body section toolbar.
Filter Folder (Inbox folder)	Create	Agents can create and edit search folders and personal folders in their inbox.
	Delete	Enables the Delete button in the Inbox Tree pane toolbar. Using this button, agents can delete search folders and personal folders from their inbox.
KB Folder	Suggest Article	This is not in use.
	View Folder	This is not in use.
	View Personal Folder	This is not in use.
	Add Notes	This is not in use.
Macro	View	Allows agents to view and use macros in emails, chats, phone logs, and custom activities.
Notes	View	<p>Allows an agent to view notes associated with cases, activities, customers, and customer associations. It enables the <b>View notes</b> option in the <b>Notes</b> button in the following panes:</p> <ul style="list-style-type: none"> <li>▪ Main Inbox toolbar</li> <li>▪ Chat Inbox toolbar</li> </ul>

Resource Name	Actions Permitted	Description
		<ul style="list-style-type: none"> <li>▪ Reply pane</li> <li>▪ Chat pane</li> <li>▪ Information pane, in the following sections: Activity Body, Activity Details, Case Details, Customer History, and Customer.</li> </ul>
	Add	<p>Allows an agent to add notes to cases, activities, customers, and customer associations. It enables the <b>Add notes</b> option in the <b>Notes</b> button in 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 Body, Activity Details, Case Details, Customer 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 View Notes window. The View Notes window can be accessed by selecting the <b>View notes</b> option in the <b>Notes</b> button in 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 Body, Activity Details, Case Details, Customer History, and Customer.</li> </ul>
	Delete	<p>Allows an agent to delete the notes associated with cases, activities, customers, and customer associations. It enables the <b>Delete</b> button in the View Notes window. The View Notes window can be accessed by selecting the <b>View notes</b> option in the <b>Notes</b> button in the following panes:</p>

Resource Name	Actions Permitted	Description
		<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 Body, Activity Details, Case Details, Customer History, and Customer.</li> </ul> <p>The View Notes window can only be accessed by agents with the <b>View Notes</b> action.</p>
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>
Search Console	View Search Console	<p>Allows agents to access the Search Console and run searches for objects in the system, such as cases, activities, or customers.</p>
System Resource	View Agent Console	<p>Allows an agent to access the Agent Console.</p>
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>

Resource Name	Actions Permitted	Description
		<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>

## Agent (Read Only) Role

---

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
Inbox Folder	Create, Delete
Notes	View
Resolution Codes	View
Folder	View
Article	Suggest
Macro	View
Product Catalog	View
Activity	Print
Search Console	View
Case	Print
Queue	View

## Supervisor Role

---

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

Resource Name	Actions Permitted
System Resource	View Administration Console
Reports	Create, Delete, View, Run, Edit, Schedule <b>Note:</b> With these actions, users can manage reports.
Monitors	Create Edit, Delete, Run <b>Note:</b> With these actions, users can manage monitors from the Administration Console.
Activity	Create, Print, Edit Subject, Pin, Complete, Edit, Transfer Activities, Unpin, Add Greetings, Add Header, Add Attachment, Add Folder, Add Signature, Assign Classification, Pull Activities, Pick Activities
Case	Edit, Print, Close Case, Change Case, Create Case
Categories	View
Chat	Complete Chat Activity, Leave Chat Activity, Transfer Chat Activities, Pull 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 ReplyType, Edit From field, Edit CC field, Edit BCC field, Edit To field, Show Email Redirect Option (This is an explicitly assigned action that enables the <b>Redirect</b> button in the agent console)

Resource Name	Actions Permitted
	<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
Messaging	Create Message, Delete Message  These actions also apply to use in the Agent Console, allowing users to use the Ask option when right-clicking on highlighted text in the Reply pane.
Macros	View
Notes	View, Add, Delete
Personal Dictionary	Personal Dictionary
Product Catalog	View
Resolution	View
Routing Queue	View, Transfer Activities, Pull Activities
Saved Search	Edit, Create, Delete
Text Editor	Edit HTML source in reply pane, Edit HTML source for articles
Usage links	View, Execute
Users	View, Transfer Activities, Pull Activities
<b>Note:</b> The following actions are part of the Supervisor role but can be used only if the <b>View Administration</b> action is explicitly added to it.	
Alias	Create, View, Edit, Delete
Blocked Address	Create, View, Edit, Delete
Blocked File Extension	Create, View, Edit, Delete

<b>Resource Name</b>	<b>Actions Permitted</b>
Delivery Exceptions	Create, View, Edit, Delete
Chat Entry Point	Create, View, Edit, Delete
Chat Template Set  (Not in use)	Create, View, Edit, Delete

## Supervisor (Read Only) Role

---

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

<b>Resource Name</b>	<b>Actions permitted</b>
Administration Console	View
User	View
Usage links	View, Execute
Category	View
Customer	View
Association	View
Inbox Folder	Create, Delete
Notes	View
Resolution Codes	View
Folder	View
Article	Suggest
Macro	View
Product Catalog	View
Activity	Print
Case	Print
Monitors	Create Edit, Delete, Run
Reports	View, Run

Resource Name	Actions permitted
Queue	View

## Creating User Roles

To create a user role:

- Based on where you want to create a user role, do one of the following:
  - If you are a partition administrator, from the partition-level Top menu, go to **User**.
  - If you are a department administrator, from the department-level Top menu, go to **User**.
- From the Left menu, navigate to **Roles**.
- In the workspace, click the **New** button.

You can create a maximum of 25 user roles.

- In the Create Role space, on the General tab, set the following:
  - Name:** Provide a name for the role.
  - Description:** Provide a brief description.
  - Template:** From the dropdown list, select an available template or select **Custom Template** to start with a blank role. The template cannot be changed once you save the role.

Create Role

General

Relationships

Name\*

User Administrator


Description

Template\*

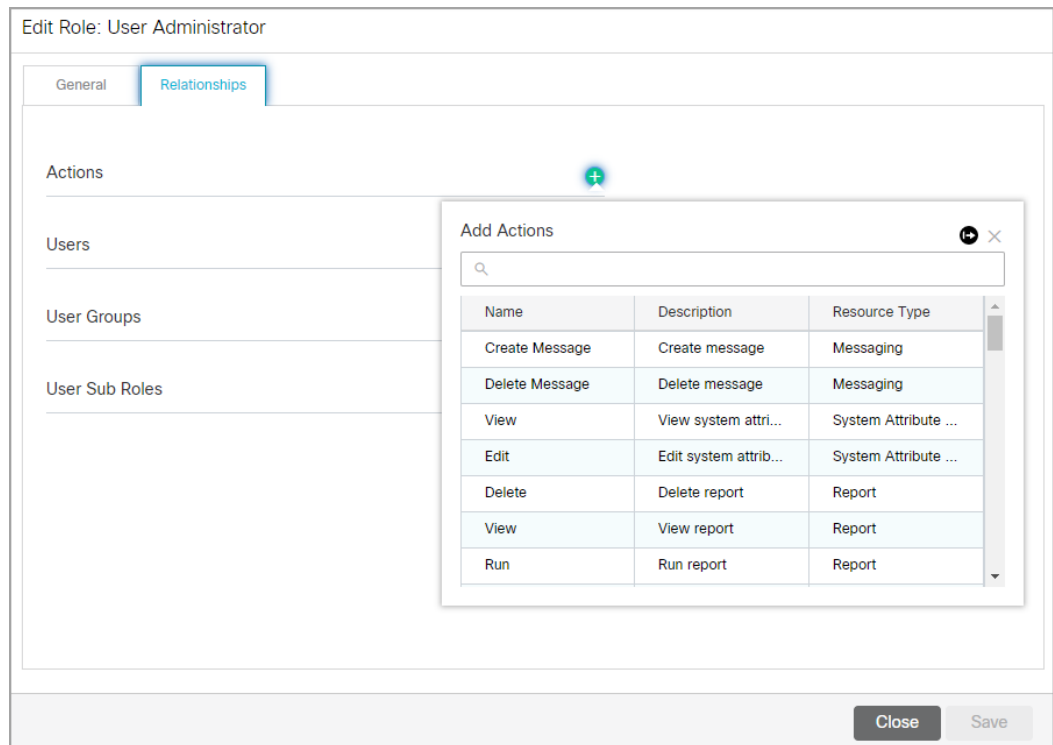
Custom Template ▼

Close

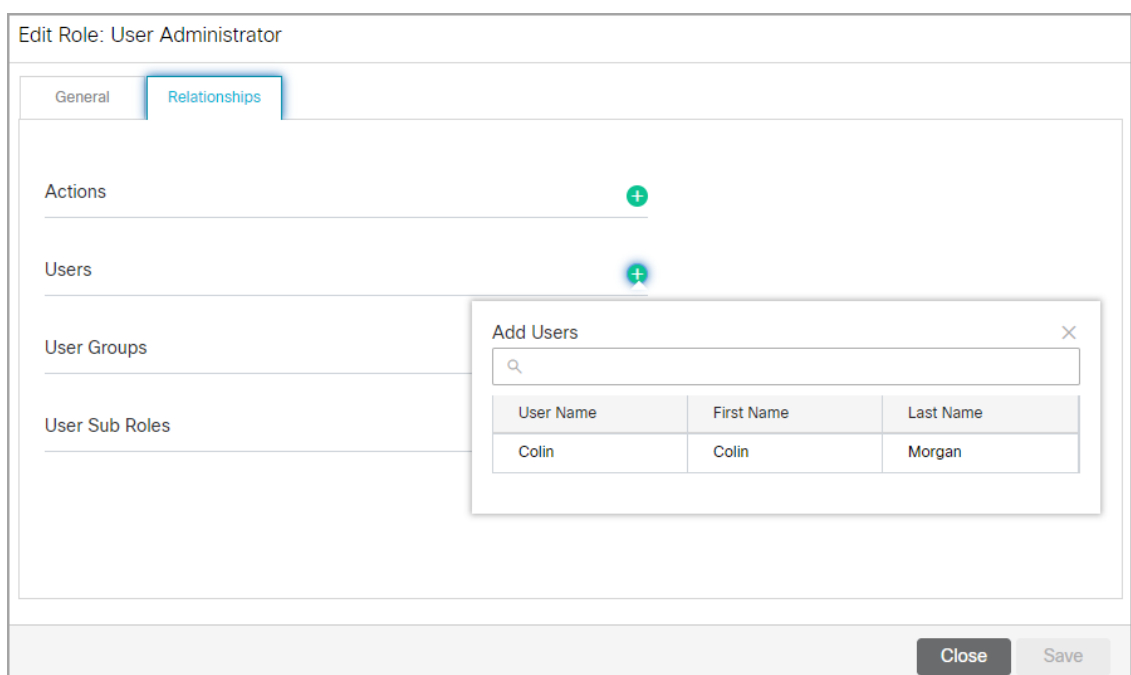
Save


- Click the **Save** button. This enables the Relationships tab.
- Next, go to the Relationships tab and do the following:
  - In the Actions section, click the **Search and Add**  button and select the actions to be included in the role.

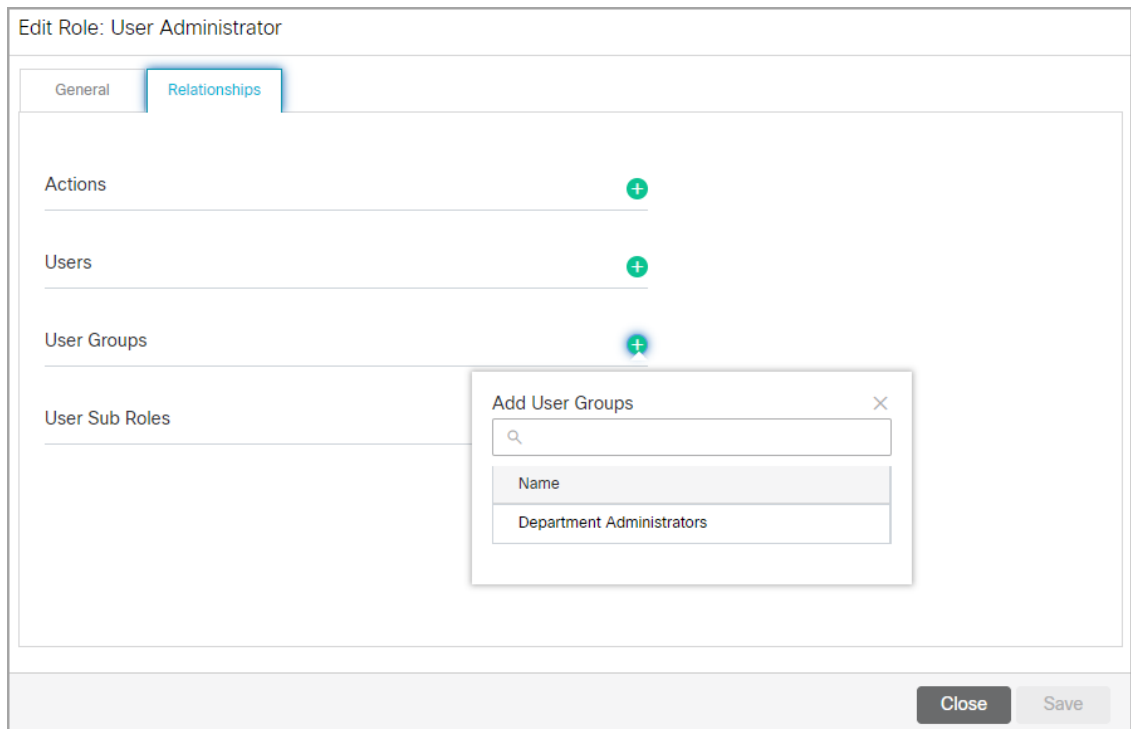
- When you start with a custom template, the role does not have any actions associated with it. While selecting the actions for the role, make sure you select all the actions that are required to do a task. For example, if you want a user with this role to be able to manage resolution codes, then make sure you assign all the four actions, Resolution - Create, View, Edit, and Delete, to the role.
- If you started with a pre-configured template, like the Agent Template, the Actions section will show the list of actions associated with the template. You can customize the role by adding or removing actions. If you feel you want to go back to the original list of actions, you can [restore the role](#) to its default state.




- b. Next in the Users section, click the **Search and Add**  button and assign the role to users.

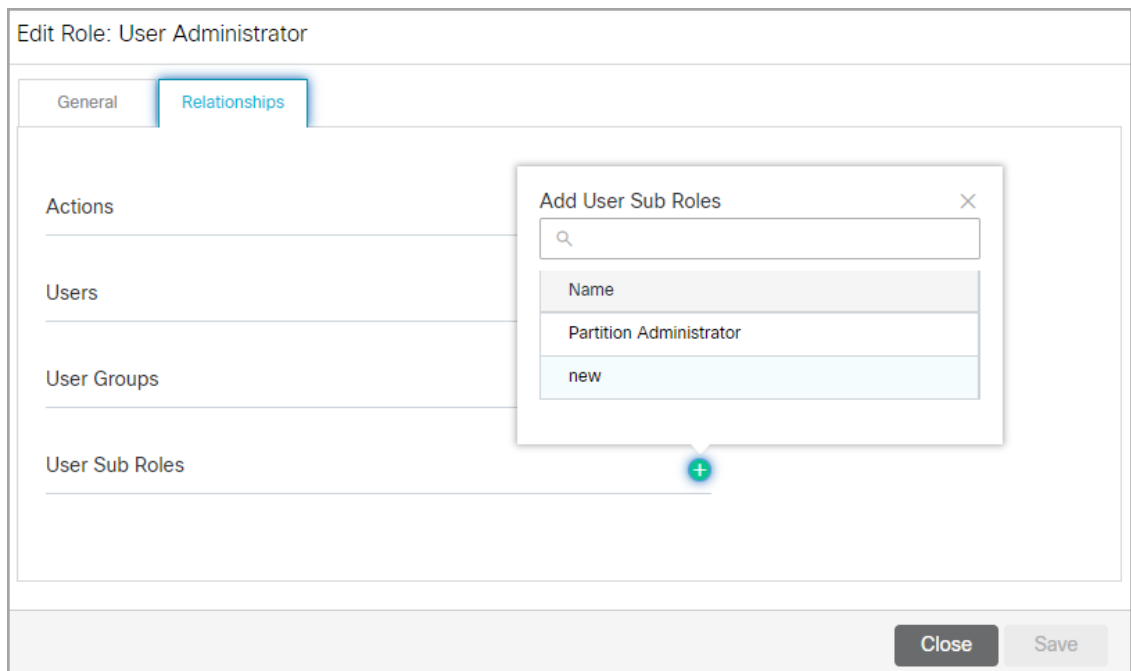


- c. In the User Groups section, click the **Search and Add**  button and assign the role to user groups. You can also choose to assign roles to users individually. However, it is recommended that you assign roles to user groups; it helps you manage your users better.



The screenshot shows the 'Edit Role: User Administrator' interface. The 'Relationships' tab is active. The 'User Groups' section has a plus icon. A modal window titled 'Add User Groups' is open, showing a search bar and a list of user groups. The list contains 'Department Administrators' which is highlighted. At the bottom right, there are 'Close' and 'Save' buttons.

- d. Now in the User Sub Roles section, click the **Search and Add**  button and select the roles you want to associate with this role as sub roles. You can even set default roles as sub roles. To know more about sub roles, see [Creating User Sub Roles](#).



The screenshot shows the 'Edit Role: User Administrator' interface. The 'Relationships' tab is active. The 'User Sub Roles' section has a plus icon. A modal window titled 'Add User Sub Roles' is open, showing a search bar and a list of user sub roles. The list contains 'Partition Administrator' and 'new', with 'new' highlighted. At the bottom right, there are 'Close' and 'Save' buttons.


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

## Copying 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. Based on where you want to create a user role, do one of the following:
  - If you are a partition administrator, from the partition-level Top menu, go to **User**.
  - If you are a department administrator, from the department-level Top menu, go to **User**.
2. From the Left menu, navigate to **Roles**.
3. From the Actions column, click the **Options**  button and select **Create Copy**.
4. In the **Enter Role Name** field, provide a name for the role.
5. Click the **OK** button.
6. A prompt is displayed to confirm the creation of the copy of the role. Select **Yes** to copy the role. The copied role retains the template of the original role.

## Restoring Roles

---

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

### To restore a role:

1. In the department-level Top Menu, click the **User** option.
2. In the Left menu, navigate to **Roles**.
3. Identify the user role you want to restore.
4. From the Actions column, click the **Options**  button and select **Edit**.
5. In the Edit Role workspace, click the **Restore Defaults** button.
6. 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. Click the **Restore** button.

### Restore Defaults

When you restore a role, the list of actions associated with the role is reset to its default state. All sub-roles associated with the role are also removed from the role.

Copy role before restoring


Enter Role Name\*

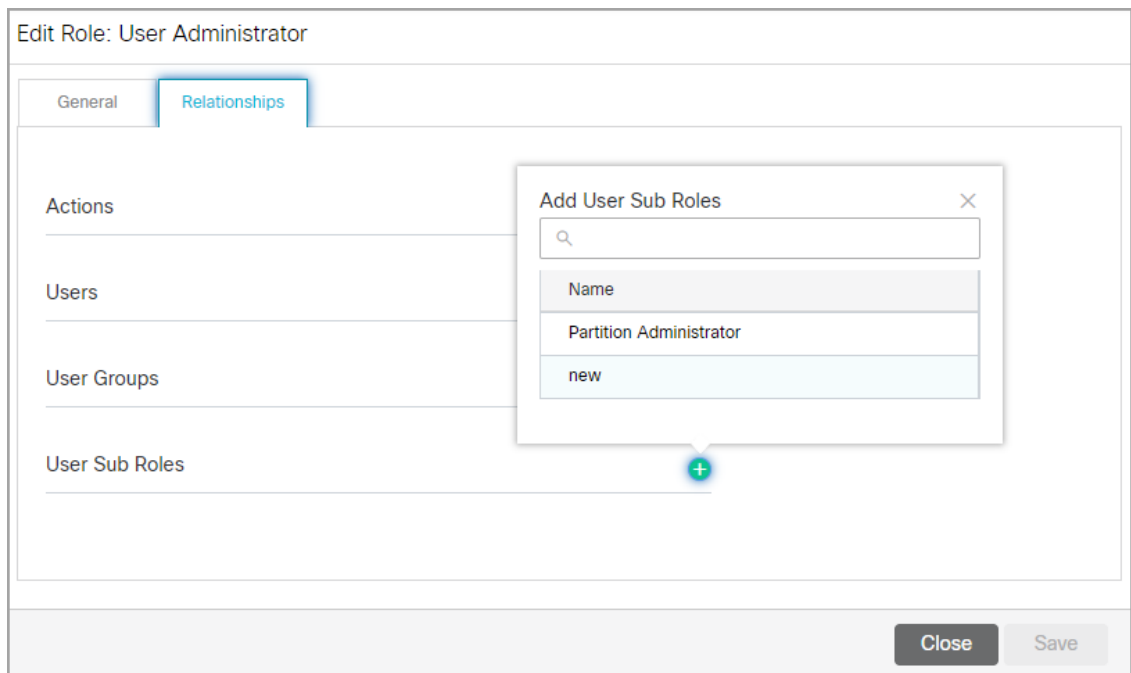
## Creating User Subroles

A subrole is a sub set 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 role.

### To create a subrole:

1. Based on where you want to add a user sub role, do one of the following:
  - If you are a partition administrator, from the partition-level Top menu, go to **User**.
  - If you are a department administrator, from the department-level Top menu, go to **User**.
2. In the Left menu, browse to **Roles**.
3. Identify the user role for which you want to create a subrole.
4. If you want to use an existing role as a sub role, do the following:
  - a. In the **Actions** column, click the **Options**  button.
  - b. Select **Edit** from the menu.
  - c. Go to Relationships tab and in the User Sub Roles section, select from the available roles.
  - d. Click the **Save** button.



5. To create a new subrole, follow the steps in [Creating users role](#) and assign it to the user role.

## About 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 created in the department is automatically included in this group. All users, standalone and Integrated users are 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.


Department level user groups are mapped to skill groups, which must be created and managed in Unified CCE. You cannot add users to this group from ECE. For information, see [Importing Data](#).

## Editing User Groups in Departments

---







The User Management tab allows you to edit user groups, assign actions to them, and set user group permissions.

### To edit user groups:

1. In the department-level Top Menu, select the **User** option.
2. In the Left menu, navigate to **User Groups**.
3. From the Actions column, click the **Options**  button and select **Edit**.
4. In the Edit Group workspace, under the General tab, the following information is provided and cannot be changed:
  - Name
  - Description



- Peripheral
- Skill Group
- Media Routing Domain

5. Under the Relationships tab, edit the following fields:


- **Actions:** Click the **Search and Add**  button and select an action to add it to the Actions list, applying the action to the user group. To remove an action from the list, hover your mouse over it and click the **Delete**  button.
- **Users:** Users that are assigned to the user group appear here.
- **Languages:** Click the **Search and Add**  button and select languages to apply to the user group. To remove a language from the list, hover your mouse over it and click the **Delete**  button.
- **User roles:** Click the **Search and Add**  button and select user roles to apply to the user group. To remove a role from the list, hover your mouse over it and click the **Delete**  button.

### Edit Group: All Users In Eight Bank

General
Relationships
Permissions

**Actions**  

Name	Description	Resource T...	Grant
View	View scree...	Screen Attri...	Explicit
Create	Create user...	User Attribu...	Explicit

**Languages** 


Name
English (US)

**Users**

---

**User Sub Groups**

---

**User Roles** 

---

Close
Save

- Under the Permissions tab, edit the permissions for the the user group.

Edit Group: All Users In Eight Bank

General Relationships **Permissions**

User Group	Name	<input type="checkbox"/> Own	<input type="checkbox"/> View	<input type="checkbox"/> Edit	<input type="checkbox"/> Delete	<input type="checkbox"/> Execute
User	Stock Rates	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Usage Links](#)

Close Save

- Click the **Save** button.

## Managing User Groups in the Business Partition

---

### Creating User Groups in the Business Partition

---

To create a group of partition administrators:

- In the partition-level Top Menu, select the **User** option.
- In the Left menu, navigate to **User Groups**.
- Click the **New** button.
- In the Create Group workspace, under the General tab, provide the following:
  - **Name**
  - **Description**

### Create Group







- General
- Relationships
- Permissions

Name*	Department Administrators
Description	Creating group for managing departments
Peripheral	
Skill Group	
Media Routing Domain	

Close Save


5. Click the **Save** button.

6. Under the Relationships tab, edit the following fields:


- **Actions:** Click the **Search and Add**  button and select an action to add it to the Actions list, applying the action to the user group. To remove an action from the list, hover your mouse over it and click the **Delete**  button.
- **Languages:** Click the **Search and Add**  button and select languages to apply to the user group. To remove a language from the list, hover your mouse over it and click the **Delete**  button.
- **Users:** Users that are assigned to the user group appear here.
- **User roles:** Click the **Search and Add**  button and select user roles to apply to the user group. To remove a role from the list, hover your mouse over it and click the **Delete**  button.

### Edit Group: Department Administrators

General Relationships Permissions

**Actions** 

Name	Description	Resource T...	Grant
Delete	Delete report	Report	Explicit
Edit	Edit system...	System Attri...	Explicit

**Languages** 


---

**Users**

---

**User Sub Groups**

---

**User Roles** 

Name
Partition Administrator

**Close** **Save**

- Under the Permissions tab, select the permissions that you want to assign to the user group.

### Edit Group: Department Administrators

General Relationships Permissions

Department	Name	<input type="checkbox"/> Own	<input type="checkbox"/> View	<input type="checkbox"/> Edit	<input type="checkbox"/> Administer
User Group	Eight Bank	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User	Eight Banks- Mana...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Eight Banks- Mark...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Eight Banks- Media	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Eight Banks- PE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>


**Close** **Save**

8. Click the **Save** button.

## Deleting User Groups in the Business Partition

---

To delete a group of partition administrators:

1. In the partition-level Top Menu, select the **User** option.
2. In the Left menu, navigate to **User Groups**.
3. From the Actions column, click the **Options**  button and select **Delete**.
4. A message appears asking to confirm the deletion. Click **Yes** to delete the user.

## About Users

---

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

A specific type of administrator is created during the installation. The first business user, created during installation, is a user called Partition Administrator. 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.

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 a Unified CCE user. Activities to this user are assigned from Unified CCE queues only. For more details on integrated queues, see [About Queues](#). Department users cannot be created in ECE and must be imported from their associated MRD. For more information, see [Importing Data](#).

The following table outlines the features and functionality for users:

User Feature and Functionality	Users
Configured in	Unified CCE
Associated with Skill Group or User Group in	Unified CCE
Status in Enterprise Chat and Email	Read only
Email routing is from	Unified CCE
Activity is reported by CUIC Reports	Yes

## Types of Department Users

---

The following table describes the licenses, roles, and explicit actions that need to be assigned to users:

Users	Licenses	Roles
Administrator	<ul style="list-style-type: none"><li>▪ ECE Platform</li></ul> and <ul style="list-style-type: none"><li>▪ ECE MailPlus: For managing emails</li><li>▪ ECE ChatPlus: For managing chat</li></ul>	Administrator
Agent	<ul style="list-style-type: none"><li>▪ ECE Platform</li></ul> and <ul style="list-style-type: none"><li>▪ ECE MailPlus: For working on email activities</li><li>▪ ECE ChatPlus: For working on chat activities</li></ul>	Agent Agent (Read Only)
Supervisor	<ul style="list-style-type: none"><li>▪ ECE Platform</li></ul> and <ul style="list-style-type: none"><li>▪ ECE MailPlus: For managing emails</li></ul>	Supervisor Supervisor (Read Only)

Users	Licenses	Roles
	<ul style="list-style-type: none"><li>▪ ECE ChatPlus: For managing chat</li></ul>	

All users in ECE cannot be created within ECE. They must be imported from the Cisco MRD. For more information on importing users, see [Importing Data](#).

## Creating Partition Administrators

---

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 administrator:

1. In the partition-level Top Menu, select the **User** option.
2. From the Left menu, navigate to **Users**.
3. From the users space, click the **New** button.
4. In the Edit User space, on the General tab, set the following properties for the user:
  - a. Provide the following details:
    - **Title:** From the dropdown list select a suitable Title. It is an optional field.
    - **First Name:** Type the first name of the user.
    - **Middle Name:** Type the middle name of the user. It is an optional field.
    - **Last Name:** Type the last name of the user.
    - **Suffix:** Provide the suffix. It is an optional field.
    - **Email Address:** Provide the email address of the user. It is an optional field.

### Create User

General Relationships Permissions

Title  
Mr

First Name\*  
Colin

Middle Name  
Merlin

Last Name\*  
Morgan

Suffix

Email Address  
mcolin@gmail.com

b. In the User Configurations 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.
- **User status:** Select the status of the user. By default the new user's status is **Enabled**. Once the user is saved, the following options are available: **Enabled** and **Disabled**.

### Edit User: Colin

General

Relationships

Permissions

#### User Configurations

---

**User Name\***

**Password\***

**User Status**

Enabled
▼

**Peripheral**

▼

**Unified CCE Agent Login Name**

▼

- c. In the Privileges section, click the checkbox to select either of the following:

On selecting either of the privileges, only the Language can be configured in the Relationships tab. Also, permissions cannot be assigned for the user after selecting either of the privileges.

- **Manage Partition Resource:** On selecting this, the user will be able to view and manage all partition resources including permissions.
- **View Partition Resource:** On selecting this, the user can only view the partition resources.

#### Privileges

---

**Manage Partition Resource**

**View Partition Resource**

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

- **Company**

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

Edit User: Colin

---

General

Relationships

Permissions

Business

---

Company	<input type="text" value="TCS"/>
Division	<input type="text"/>
Department	<input type="text" value="Support"/>
Job title	<input type="text" value="Department Manager"/>
Work phone	<input type="text" value="6501256781"/>
Extension	<input type="text"/>
Employment status	<input style="text-align: right; font-size: small; color: #0070c0; vertical-align: bottom; border: none; border-bottom: 1px solid #ccc; width: 100%;" type="text" value="Employee"/>

e. 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**

Edit User: Colin

General

Relationships




Permissions

Personal

---

Home address line 1	<input type="text" value="1839 Jackson Street"/>
Home address line 2	<input type="text"/>
Home city	<input type="text" value="Mountain View"/>
Home state	<input type="text" value="CA"/>
Home zip code	<input type="text" value="95632"/>
Mobile number 2	<input type="text"/>
Secondary email address	<input type="text"/>

5. Next, go to the Relationships tab, and set the following:

- In the Languages section, the KB language set as the default language in the **KB primary language** setting is automatically assigned to the user. If other languages are available, click the **Search and Add**  button to assign those languages to the user and you can change the default KB language of the user by clicking the toggle button next to the language.
- In the User Roles section, click the **Search and Add**  button to 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.
- In the Actions section, you can view the list of actions assigned to the user. Click the **Search and Add**  button to assign additional actions to the user.

It is highly recommended that you do not assign actions directly to user. You should always create a user role, with the actions, and assign the role to the user. This makes user management easier. For more details on creating user roles, see [Creating User Roles](#).

Edit User: Colin

General Relationships Permissions

User Groups

Languages +

Name	Default Language
English (US)	<input type="checkbox"/>

User Roles +

Actions +

6. Next go to the Permissions tab and select the permissions you want to assign to the user group.

Edit User: Colin

General Relationships Permissions

Name	Own	View	Edit	Administer
Sasha	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Close Save

7. Click the **Save** button.

## Editing User Details in Departments

You can edit the details of any users you have already created through the User option in the Top menu.

## To edit user details:






1. In the department-level Top Menu, select the **User** option.
2. From the Left menu, navigate to **Users**.
3. From the list, select the user you want to edit
4. In the Edit User space, under the General tab, the following options details are displayed:
  - **Username:** The username under which this user appears in the system. This is managed in Unified CCE and cannot be changed here.
  - **Screen name:** The name under which this user is visible in chats and communications.
  - **Title:** Select a title from the dropdown menu.
  - **First name:** The user's first name. This is managed in Unified CCE and cannot be changed here.
  - **Middle name:** The user's middle name.
  - **Last name:** The user's last name. This is managed in Unified CCE and cannot be changed here.
  - **Suffix:** The professional suffix for this user (for example, MD).
  - **Password:** The user's password. This is managed in Unified CCE and cannot be changed here.
  - **Authentication Type:** The method in which the user accesses the application. This is managed in Unified CCE and cannot be changed here.
  - **User Status:** The current status of the user.
  - **Peripheral:** The peripheral gateway to which the user is assigned. This is managed in Unified CCE and cannot be changed here.
  - **Unified CCE Agent Login Name:** The login name for the user in Unified CCE. This is managed in Unified CCE and cannot be changed here.
  - **Email Address:** An external email address for the user.

The screenshot shows the 'Edit User: Sash' interface. On the left is a navigation menu with 'Users' selected. The main area has three tabs: 'General', 'Relationships', and 'Permissions'. The 'General' tab is active and contains the following fields:

- Title: Ms (dropdown)
- First Name\*: Sash (text input)
- Middle Name: (text input)
- Last Name\*: Ch (text input)
- Suffix: (text input)
- Email Address: (text input)
- User Configurations section:
  - User Name\*: Sash (text input)
  - Password\*: \*\*\*\* (password input)
  - Screen Name\*: Sash (text input)
  - User Status: (dropdown)
  - Manager: (text input with a green '+' button)
  - Peripheral: AGENTPG\_1 (dropdown)
  - Unified CCE Agent Login Name: Sash (dropdown)

At the bottom left is a 'Sign Out' link, and at the bottom right are 'Close' and 'Save' buttons.

5. Under the Relationships tab, edit the following fields:

- **Actions:** Click the **Search and Add**  button and select an action to add it to the Actions list, applying the action to the user. To remove an action from the list, hover your mouse over it and click the **Delete** button. Actions applied to the user by the user group to which the user is assigned cannot be removed.
- **User Groups:** The user groups to which the user is assigned. This cannot be changed.
- **Licenses:** Click the **Search and Add**  button and assign licenses to the user. The licenses that are available are: **ECE Platform**, **ECE MailPlus**, and **ECE ChatPlus**.
- **Languages:** Click the **Search and Add**  button and select languages to apply to the user. To remove a language from the list, hover your mouse over it and click the **Delete** button.
- **User Roles:** Click the **Search and Add**  button and select user roles to apply to the user. To remove a role from the list, hover your mouse over it and click the **Delete** button. Roles applied to the user by the user group to which the user is assigned cannot be removed.
- **User Attribute Settings:** Click the **Search and Add**  button to select user attribute settings. This lets you control the level of access a user has in the system. For more details on user attribute settings, see [About User Attribute Settings](#).

Edit User: Sash

General Relationships Permissions

User Groups

Licenses +

Name
ECE ChatPlus

Languages +

Name	Default Language
English (US)	<input type="checkbox"/>

User Roles +

Name
Agent

Direct Reports +

User Attribute Settings +

Close Save

6. Under the Permissions tab, select the permissions you want to assign to the user group.

Edit User: Sash

General Relationships **Permissions**

Usage Links	Name	<input type="checkbox"/> Own	<input type="checkbox"/> View	<input type="checkbox"/> Edit	<input type="checkbox"/> Delete	<input type="checkbox"/> Execut
Link Groups	Stock Ra...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Close Save

7. Click the **Save** button.


## Specifying a User's Manager in Departments

A manager can monitor the activities and cases assigned to agents from the Agent Console. A manager has a My Team folder in his Inbox tree, in the Agent Console, in which all the users who report to the user are listed. The manager has a read only view of the activities and cases assigned to the users reporting to him.

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

You cannot assign managers of user groups.

To assign a manager of a user:

1. In the department-level Top Menu, select the **User** option.
2. From the Left menu, navigate to **Users**.
3. From the list, select a user.
4. If you are assigning the manager of the user, then in the General tab, navigate to the **Manager** field. Click the **Search and Add**  button and select a user. The user selected in the manager field becomes the manager of the user you are editing.

Edit User: Sash

General Relationships Permissions

Suffix

Email Address

User Configurations

User Name\*

Password\*

Screen Name\*

User Status

Manager


Peripheral

Unified CCE Agent Login Name

Select ×

User Name	First Name	Last Name
santosh6	santosh6	k
sumit1	sumit1	p
sumit2	sumit2	p
sumit3	sumit3	p
sumit4@egeng.info	sumit4	p
sumit5	sumit5	p

Close Save

- If you are editing the properties of the manager, then in the Edit User space, under the Relationship tab, navigate to the **Direct Reports** section. Click the **Search and Add**  button and select the users who report to the user you are editing. This makes the current user a supervisor for the selected users in this list.

Edit User: Saer

General Relationships Permissions

Direct Reports

User Attribute Settings

Departments

Name
Eight Bank

Actions

Name	Description	Resource T...
Print	Print activity	Activity
Print	Print case	Case
Create	Create a gl...	Saved Sea...

Add Direct Reports

Search

User Name	First Name	Last Name
santosh6	santosh6	k
sumit5	sumit5	p
sumit4@egeng.info	sumit4	p
sumit3	sumit3	p
sumit2	sumit2	p
sumit1	sumit1	p

Close Save


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. Based on where the user is, do one of the following:
  - If you are in the partition, from the partition-level Top menu , go to **User**.
  - If you are in a department, from the department-level Top menu, go to **User**.
2. From the Left menu, navigate to **Users**.
3. From the list, select the user you want to delete and click the **Delete**  button.
4. A message appears asking to confirm the deletion. If the user has created any supervision monitors, a message is displayed to inform that all the monitors created by the user will be deleted. Click **Yes** to delete the user.

# Access Restrictions

- [About Blocking Visitors](#)
- [Enabling Visitor Blocking](#)

# About Blocking Visitors

---

## Chat Block 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. Once enabled, agents and supervisors can block such customers from the Agent Console for a defined period of time.

## IP Based Customer Throttling

---

The **IP Based Customer Throttling** tracks the number of chat activities initiated from each IP address to inhibit the Denial-of-Service attacks. The IP address of customers or spambots, who are creating chats with an intent to flood the queue with irrelevant chat requests, are blocked once they reach the configured number of chats that can be created within 60 minutes. This prevents the delay of service to genuine customers who are trying to reach the agents.

When the IP based customer throttling setting is enabled, the administrator can configure the number of chats that can be initiated using the same IP address in an hour. For instance, if users enable this setting and allow four chats per hour, not more than four chats can be initiated from an IP address in an hour. If a customer with an IP address, say 222.111.22.11 tries to initiate the fifth chat within an hour, the IP address will be blocked for the remaining duration. However, as soon as the 60 minutes have elapsed, the customer with the IP address 222.111.22.11 can initiate a new chat session. However, if the customer with the same IP address exceeds the configured limit again, they are prevented from creating more chat sessions for 60 minutes once more. In this way, agents can dedicate their time on the requests of genuine customers, thereby enhancing their efficiency and improving customer satisfaction.

## Enabling Visitor Blocking

---

To enable visitor blocking:

1. In the partition-level Top menu, click the **Security** tab .
2. In the Left menu, select **Blocked Visitors**.
3. In the Blocked Visitors space, in the IP Based Customer Throttling section, set the following:
  - **Enable IP based throttling:** Click the **Toggle** button to enable throttling based on the customer's IP address.
  - **Number of chats per hour:** Provide the number of chats that can be initiated using the same IP address in an hour. The value can range from a minimum of 1 chat per hour to a maximum of 20 chats per hour.
4. In the Chat Block Visitors section, set the following:
  - **Enable blocking of visitors:** Click the **Toggle** button to enable the ability for agents to block customers.

- **Block criteria:** From the dropdown menu, select the method in which the user is identified for the ban. Select Browser cookie to use cookies to identify and ban the user. Select **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 them. The minimum value for this field is 1 hour. The maximum value for this field when the criteria is set to **Browser cookie** is 168 hours (7 days). The maximum value for this field when the criteria is set to **Visitor IP address** is 87,600 hours (3650 days).

### Blocked Visitors

---

#### IP Based Customer Throttling

---

Enable IP based throttling

Number of chats allowed per hour\*

---

#### Chat Block Visitors

---

Enable blocking of visitors

Block criteria

Block duration in hours\*

5. Click the **Save** button.

# Attachments

- [About File Attachments](#)
- [Blocking Attachment File Types](#)
- [Allowing Attachment File Types](#)
- [Enabling and Disabling Chat Attachments](#)
- [Enabling and Disabling Email Template Attachments](#)
- [Configuring File Attachment Settings](#)

## About File Attachments

---

As a partition administrator, you can specify the file types that can be attached to emails and chat messages. You can choose to allow or block specific file types by creating an allow list or deny 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 [About Queues](#).

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 [About Blocked File Extensions](#).

## Blocking Attachment File Types

---

To block file types for attachments:

1. In the partition-level Top Menu, click the **Security** option.
2. In the Left menu, select **Attachments**.
3. Select **Block file types listed below** from the dropdown list next to **Allow or Block File Type**.
4. In the **File Types** field, enter the file extension types that you wish to block.
  - Extensions require a period in front of their name (for example, ".txt") and must be separated by commas (for example, .txt, .exe, .xls,).
  - Before saving, you can also choose to enable or disable chat attachments for agents and customers. See [Enabling Chat Attachments](#) for more information.

### Attachments

Allow or block file types*	Block file types listed below ▾
File types*	.csv
Enable Chat Attachments for Agents and Customers	<input checked="" type="checkbox"/>
Maximum size for each chat attachment (MB)*	3 ▾
Maximum size for each knowledge base attachment (MB)*	3

5. Click the **Save** button.

## Allowing Attachment File Types

---

To allow file types for attachments:

1. In the global-level Top Menu, click the **Security** option.
2. In the Left menu, select **Attachments**.
3. Select either **Allow all file types** or **Allow file types listed below** from the dropdown list next to **Allow or Block File Type**.
4. If **Allow file types listed below** is selected, you must enter the file extensions that you wish to allow in the **File Types** field.
  - Extensions require a period in front of their name (for example, ".txt") and must be separated by commas (for example, .txt, .exe, .xls,).
  - Before saving, you can also choose to enable or disable chat attachments for agents and customers. See [Enabling Chat Attachments](#) for more information.
5. Click the **Save** button.

## Enabling and Disabling 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. Image attachments sent during chat interactions appear in line. This feature can also be disabled if you want to prevent customers and agents from sharing files during chat interactions.

To enable or disable chat attachments for agents and customers:

1. In the global-level Top Menu, click the **Security** tab.
2. In the Left menu, select **Attachments**.
3. Click the toggle button next to **Enable Chat Attachments for Agents and Customers** to disable this feature, or re-enable it if you previously turned it off. Note that chat attachments are enabled by default.
4. Use the dropdown field next to **Maximum Size for Each Chat Attachment (MB)** to set the desired maximum file size for chat attachments. File sizes are listed in megabytes (MB) and can range from 2MB to 10MB in size. By default, the value is set to 3 MB.
  - You can also choose to allow or block specific file attachment types before saving. See [Allowing Attachment File Types](#) and [Blocking Attachment File Types](#) for more information.
5. Click the **Save** button.

Chat attachments can be further configured at the queue level. For more information, see [Creating Queues](#).

## Enabling and Disabling Email Template Attachments

---

With attachments enabled at the partition level, authors can attach files to the articles that they create for emails like headers, greetings, and so on. To help control their use, limits can be placed on the maximum allowed size for article attachments for the partition.

To enable or disable email attachments for agents and customers:

1. In the global-level Top Menu, click the **Security** tab.
2. In the Left menu, select **Attachments**.
3. Use the dropdown field next to **Maximum Size for Each Knowledge Base Attachment (MB)** to set the maximum total size allowed for any one article attachment for the partition. If the combined file size of the attachments exceed this maximum, the email is rejected. Minimum allowed value is 1 MB and maximum allowed value is 25 MB. By default, the value is set to 3 MB.
  - You can also choose to allow or block specific file attachment types before saving. For more information, see [Allowing Attachment File Types](#) and [Blocking Attachment File Types](#).
4. Click the **Save** button.

## Configuring File Attachment Settings

---

To configure attachment settings for the partition:

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

- **Maximum Size For Knowledge Base Attachment (MB):** Set the maximum size for any one article attachment for the partition. Minimum allowed value is 1 MB and maximum allowed value is 25 MB. By default, the value is set to 3 MB.

4. Click the **Save** button.

# Audit Log

- [About Audit Log](#)
- [Viewing the Audit Log](#)

# About Audit Log

---

Audit logs allow administrators to monitor the actions performed by all the users in the Administration Console. The audit log reporting functionality enhances the accountability of actions. Administrators can find the root cause of any issue by identifying the resources on which the action was performed and who performed the action. Users can view, search, and filter audit data. The audit log contains data for up to four weeks at any point of time.

## Audit of Administration Objects

---

The Audit Log contains the list of all the actions performed by the various users in the Administration Console. The following fields are within the Audit log view:

- **Device IP:** The source IP address of the user who performed the action.
- **Audit Date:** The date and time when the action was performed.
- **Actor:** Name of the user who performed the action. For example, if an action was performed by a department administrator called John, then John would be mentioned under this field.
- **Department:** Name of the department where the action is performed. When the action is performed at the partition level, Partition is mentioned under this field.
- **Resource Type:** Resource type of the administration object. For example, Calendar, Users, Workflow, and so on.
- **Resource Identifier:** The resource on which the action was performed. For example, if the administrator creates a user, then User is the resource type whereas the name of the user, say Greg, is the resource identifier. For the Update action type, the updated value of the attribute of the object will be visible under the Resource Identifier field. For example, if the administrator changes the user's name from Greg to Gregson, then the latter is mentioned under this field.
- **Action Type:** The action that was performed on the object. It includes the following actions: Create, Update, or Delete.

For objects with multi-side relationships, the changes are logged against the object which was modified. For example, the event of adding a user to a group is captured in the audit log as an event for the user group and not for the user.

- **Details:** A Show More link is available in this field, which shows further details for the other audit data fields. This link is disabled for the Delete action type. The detailed data consists of:
  - **Department:** Name of the department where the action is performed.
  - **Resource Identifier:** The resource on which the action was performed.
  - **Audit Date:** The date and time when the action was performed
  - **Action Type:** The action that was performed on the object
  - **Attribute Name:** The name of the attributes on which the action was performed.
  - **Old Value:** Previous value of the attribute. This field appears for the Update action type.


- **New Value:** Current value of the attribute. This field is available for Create and Update action types.
- **Permissions Granted and Permissions Removed:** Permissions granted to or removed from the user on the following objects: user, user groups, usage links, usage link groups, routing queues, departments, or partition. These fields are available only when such an action has been performed. The Show More link lists the attribute name, the name assigned to that attribute and all the permissions granted or removed in a tabular format.

## Viewing the Audit Log

---

To view the audit log, you can select from one or more filter options which are enabled for all the columns. If there are two or more filters selected, then the filter functionality follows the “AND” condition. For instance, to view the audit log data for the user Paul Watson from the Payments department, select the desired values from the Actor and Department filter criteria.

### To view the audit log:

1. In the partition-level Top Menu, click the **Security** option.
2. In the Left menu, select **Audit Log**. You can view the audit log data for up to four weeks.
3. Select one or more options from the available filter criteria:
  - **Resource Type:** From the dropdown menu, select the Resource Type for which you wish to view the audit log.
  - **Select Department:** From the dropdown menu, select the Department.
  - **IP Address:** Provide the IP address for which you wish to filter the audit log.
  - **Time Range:** It filters the data based on what you select from the following options:
    - **Today:** Fetches the audit data for the current day.
    - **Last Week:** Fetches the data from last week.
    - **Custom Range:** In case of custom date range selection, you need to provide a Start date and End date. Note that the date range must be within 28 days from the selected date.
  - **Resource Identifier:** From the dropdown menu, select the Resource Identifier for the selected Resource Type. Note that this field is disabled if All Resources is selected in the Resource Type field or if All Departments is selected in the Select Department field.
  - **Actor:** Click the **Search and Add**  button and select the department to view the list of all the users present in that department. You can view the First name, Last name and User Name. Select the user for whom you wish to view the audit log.

To view the audit logs for users shared across different departments, you can select the other department to which the actor belongs. For instance, administrator Amy Greene in the Accounts department is shared with the Service department. She logs into the administration console and navigates into the Service department and edits some users. To view the audit log for the update action, from the Actor field, you can search for the Accounts department and select Amy Greene, and from the Select Department field you can select Service.

4. The audit log reloads after every filter selection and the relevant information is displayed on the screen. You can view the IP address from which the action was performed, the audit date, the actor, the department to which the actor belongs, the resource type and identifier, the type of action that was performed and some more details.
5. You can also perform the following actions on the Audit log page:
  - **Refresh:** Click the Refresh button to fetch the latest audit log data. If there are any filters and you choose to refresh the data, the audit data will be refreshed based on the filter selection.
  - **Reset Filter:** Clicking this button will reset all the filter selections and the audit log view will return to its original view.
  - **Edit Column:** You can select what columns are displayed in the Audit Log by enabling or disabling the columns in the list. Click the checkbox next to the column name to enable or disable the column.

The screenshot displays the Audit Log interface with the following components:

- Filters:**
  - Resource Type:** All Resource Types (dropdown)
  - Select Department:** Partition (dropdown)
  - IP Address:** (text input)
  - Time Range:** 02/24/2021 04:16:46 pm - 03/23/20...
  - Resource Identifier:** (dropdown)
  - Actor:** (text input) with a green plus icon to the right.
- Buttons:** Refresh, Reset Filter (highlighted with a blue border), and Edit Columns.
- Table:**

Device IP	Audit Date	Actor	Department	Resource Type	Resource Ide...	Action Type	Details
10.32.81.124	03/22/2021 0...	System Admi...		Licenses	ECE Platform	Create	<a href="#">Show More</a>
10.32.81.124	03/22/2021 0...	System Admi...		Licenses	ECE CIH Platf...	Create	<a href="#">Show More</a>

# Certificate Management

- [About Certificate Management](#)
- [Creating Certificates](#)
- [Deleting Certificates](#)

## About Certificate Management

---

Integration across components require valid SSL certificates to ensure that a secure communication with the third party happens seamlessly. With Certificate Management, authenticated administrators can import certificates in the Administration Console to serve the purpose. Currently, following certificates can be imported:

- **Cisco IDS** server certificate for the Cisco IDS Single-Sign On.
- **WXM Survey** certificate for the post-chat survey page.

After importing the certificates, administrators can view the following details in the Certificate Management space:

- **Name:** Name of the certificate provided by the administrator.
- **Component Type:** The component type provided by the administrator:
  - **Cisco IDS**
  - **WXM Survey**
- **Description:** The description for the certificate provided by the administrator.
- **Expire Date:** The date and time when the certificate will expire. This information is derived from the imported certificate.


Name	Component Type	Description	Expire Date
Cisco IDS certificate	Cisco IDS	for Cisco IDS Single sig...	2021-09-21 02:05:19
WxM Survey	WXM Survey	certificate	2021-09-21 02:05:19

## Creating Certificates

---



To create certificates:

1. In the partition-level Top Menu, click the **Security** option.
2. In the Left menu, select **Certificate Management**.
3. In the Certificate Management space, click the **New** button.
4. In the Create Certificate space, in the Details tab, provide the following details:
  - **Name:** Type a name for the certificate.

- **Description:** Add a description for the certificate.
- **Component Type:** You can select from either of the two options: **WXM Survey** or **CISCO IDS** depending on the type of certificate you wish to import.
- **Import Certificate:** To import the certificate, click the **Search and Add**  button. In the Import Certificate window that opens, provide the following details:
  - **Certificate file:** Click the **Browse** button and select the certificate you wish to import. The certificates can only be imported in the following formats: `.pem`, `.der` (BINARY), or `.cer` /`cert`.
  - **Alias Name:** Provide an alias for your certificate.

### Create Certificate

Details


<b>Name*</b>	<input type="text" value="Cisco IDS certificate"/>
Description	<input type="text" value="Certificate for CISCO IDS"/>
<b>Component Type*</b>	<input style="text-align: right; border-bottom: none; border-right: none; border-left: none; border-top: none; width: 100%;" type="text" value="CISCO IDS"/> 
Import Certificate	<input style="background-color: #f0f0f0; border: none; width: 100%;" type="text" value="ussuhvwm0497.egeng.info.cer"/> 

5. Click **Save**.

## Deleting Certificates

---

To delete certificates:

1. In the global-level Top Menu, click the **Security** option.
2. In the Left menu, select **Certificate Management**.
3. In the Certificate Management space, hover over the certificate you wish to remove and click the **Delete**  button.
4. Click the **Yes** button when the system prompts you to confirm the deletion.

# Cross-Origin Resource Sharing

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

## 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.

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:

CORS stands for Cross Origin Resource Sharing

1. In the partition-level Top menu, click the **Security** option.
2. In the Left menu, click **CORS**.
3. In the Cross Origin Resource Sharing space, set the following:
  - **Enable Cross Origin Resource Sharing:** Click the **Toggle** button to enable CORS. By default, CORS is enabled in the application.
  - **Select origins for CORS:** Select **Allow all origins for CORS** or select **Allow following origins for CORS** and provide the list of allowed websites for CORS.
  - **Allowed Website URL:** This field is enabled if **Allow following origins for CORS** is selected. Enter the domain or URL and click the **Done**. 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`. Allowed websites appear in the **Allowed Websites** field.

### Cross Origin Resource Sharing

Enable Cross Origin Resource Sharing

Select origins for CORS

Allow all origins for CORS

Allow following origins for CORS

Allowed Website URL


Access Control Allow Origins (Allowed Websites)	Actions
http://health.gov.com	...

4. Click the **Save** button.

## Deleting Cross-Origin Resource Sharing Websites

---

To delete cross-origin resource sharing websites:

1. In the partition-level Top menu, click the **Security** option.
2. In the Left menu, click **CORS**.
3. In the Cross Origin Resource Sharing space, under the list of allowed websites, in the **Actions** column, click the **Options**  button. Select **Delete** from the menu.
4. A message appears asking to confirm the decision. Click **Yes** to delete the website.

# Rich Text Content Policies

- [About Rich Text Content Policies](#)
- [Enabling and Disabling Rich Text Content Policies](#)
- [Configuring the Rich Text Content Policy File](#)
- [Exporting and Importing Rich Text Content Policies](#)
- [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 ECE users

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 the Using a Plain Text Policy section of [Configuring the Rich Text Content Policy File](#).

## Enabling and Disabling Rich Text Content Policies

---

To enable or disable rich text content policies:

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

2. In the Left menu, select **Rich Text Content Policy** to display the policy list. Both chat and email policies are shown. You can also see if a policy is enabled or disabled underneath the Status header.

The Email-inbound policy is enabled by default.

3. Select a policy from the list to open it. You can make direct edits to the selected policy or import an existing one to replace it.
4. Enter information for the following fields:
  - **Name:** the name you want to apply to the policy.
  - **Description:** information about the policy.
5. Click the **Enable** toggle button to turn the policy on or off. You can also select **Restore** to remove any changes you have made to the policy.
6. Click the **Save** button. Once you have saved the policy, you can then export it via the **Export Policy** option.

## 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>
```

## 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 rich text content policies:

1. In the partition-level Top Menu, click the **Security** option.
2. In the Left menu, select **Rich Text Content Policy** to display the policy list. Both chat and email policies are shown. You can also see if a policy is enabled or disabled underneath the Status header.
3. Select a policy from the list to open it. You can make direct edits to the selected policy or import an existing one to replace it.
4. Click the **Export Policy** button and save the XML file to a local directory.
5. 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](#).
6. Return to the Chat and Email Administration Console and select the **Import Policy** button.

7. Locate the updated XML file and import it.
8. Click the **Save** button.

You can also import an existing policy that you have already created.

#### To import an existing rich text content policy:

1. In the partition-level Top Menu, click the **Security** option.
2. In the Left menu, select **Rich Text Content Policy** to display the policy list. Both chat and email policies are shown. You can also see if a policy is enabled or disabled underneath the Status header.
3. Select a policy from the list to open it.
4. Click **Import Policy** to open the Import Policy space.
5. Click the **Browse** button to open up the file navigator. Navigate to the existing policy you wish to upload and click it.
6. Click **Upload**.

## Restoring Rich Text Content Policies

---

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

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

#### To restore rich text content policies:

1. In the partition-level Top Menu, click the **Security** option.
2. In the Left menu, select **Rich Text Content Policy** to display the policy list. Both chat and email policies are shown. You can also see if a policy is enabled or disabled underneath the Status header.
3. Select a policy from the list to open it.
4. Click the **Restore** button.
5. In the window that opens, click **Yes**.

# Customer Single Sign-On

- [About Customer Single Sign-On](#)
- [Creating Identity Providers](#)
- [Configuring Customer Single Sign-On](#)
- [Enabling Chat Entry Points for Customer SSO](#)
- [Configuring Your Website for Chat Customer SSO](#)
- [Troubleshooting Chat Customer SSO](#)

## About Customer Single Sign-On

---

Customer single sign-on 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.

- **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 as an add-on feature. For more information, 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, see *Enabling Auto-Login*. To learn how to configure entry points for Secure Chat, see *Enabling Customer Single Sign-On for Chat Templates*.

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 the system for customer single sign-on, there is 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. 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

---

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

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

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

- **Configure Single Logout for the Identity Provider:** This involves providing SLO endpoints exposed by the ECE application to the IdP. For more information, see "Planning Your Configuration," below.

- **Enable and Configure Customer SLO in the ECE Application:** This involves turning on single logout services for each provider configured in the ECE application, as well as providing additional details required by these services. For more information, see [Creating Identity Providers](#).

## Planning Your Configuration

---

Before configuring Chat Customer Single Sign-On, perform the following:

- Identify the entry points for which this feature should be enabled.
- Identify the attributes to transfer through SAML and configure the 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 configuring the system for Secure Chat, the chat templates must also be enabled to use customer single sign-on. For more information on configuring chat templates for Secure Chat with Aqua templates, see [Enabling Customer Single Sign-On for Chat Templates](#).
- If configuring SLO for Customer 360, provide ECE SLO endpoints to each Identity Provider for which SLO shall be enabled.
  - 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 the application.

## Creating Identity Providers

---

### Important things to note about SAML 2.0 Single Sign-On:

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 enabling encrypted SAML assertion, a Java Keystore (JKS) file is required for the decryption certificate.
- A Java Keystore (JKS) file is necessary if the service provider is enabled to authenticate users in SAML 2.0, as well. Contact your IT to obtain the Java Keystore file.
- SAML 2.0 provides a well-defined, interoperable metadata format that can be used to expedite the trust process between the Service Provider (SP) and the Identity Provider (IdP). Metadata ensures a secure transaction between an identity provider and a service provider. To enable SAML, a Circle of Trust (COT) between the service provider and identity provider must be established. Consult your IT department about obtaining IdP and SP metadata. Note: SP metadata for customer portals, chat, agent portals, and the agent desktop should be provided separately.

- SAML is a time sensitive protocol and the IdP determines the time-based validity of a SAML assertion. If the identity provider and the service provider clocks are not synchronized, the assertion becomes invalid and stops the SAML SSO feature. For SAML SSO to operate, you must install the correct Network Time Protocol (NTP) setup and ensure the time for the IdP and SP applications is completely synchronized. Consult your IT department about synchronizing the IdP clock with the SP clock.

### To create identity providers:

1. In the partition-level Top menu, click the **Security** option.
2. In the Left menu, navigate to **Single Sign-On > Providers**.
3. Click the **New** button.



A maximum of 25 identity providers can be created in a partition.


4. In the Create SSO Providers space, 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 the toggle switch to make this provider the default identity provider for customer single sign-on configurations. Otherwise leave the toggle switch unselected .
  - **Start Page (Absolute URL):** Provide the URL for the page on which web-based customers should land when successfully logging in with single sign-on.
  - **RelayState URLs:** 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 allow any RelayState URLs used by the service provider ( ECE application). Provide the following:
    - **Allow all RelayState URLs:** Allow all RelayState URLs of the service provider.
    - **Allow RelayState(s) that start with the following URL(s):** Provide the URL domain names in the field below the option and press **Enter**.

The screenshot shows a configuration window with two tabs: 'General' and 'Configuration'. The 'General' tab is selected. The form contains the following fields and controls:

- Name\***: Text input field containing 'SSO Provider'.
- Description**: Empty text input field.
- ID**: Greyed-out text input field.
- Default**: Toggle switch, currently turned off.
- Start Page (Absolute URL)**: Text input field containing 'https://startpage.com'.
- RelayState URLs**: Section header.
- Select option for RelayState URLs**: Two radio buttons. The first, 'Allow All RelayState URLs', is selected. The second is 'Allow RelayStates that start with the following URLs'.

At the bottom right, there are two buttons: 'Close' (grey) and 'Save' (blue).

5. Click the **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 External URL of the Application is correctly configured. For more information, see [General Partition Settings](#).
  - 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. Click the **Search and Add**  button and provide the certificate in the field. The certificate must start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----"
    - **Enable encrypted assertion:** Click the Toggle button to enable assertion encryption. The default state sets it to **disabled**.
    - **Assertion decryption certificate:** If **Enable Encrypted Assertion** is enabled, click the **Search and Add**  button and provide the following in the Assertion Decryption Certificate window:
      - **Java keystore file:** Provide the file path of your Java Keystore File, for example: C:\keystore\ *version\_number* \SSO\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 application 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.

- Under the Service Provider option, provide the following:
  - **Enable identity provider initiated logout service:** Enable the Toggle button to allow the ECE 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 ECE application, which then terminates the user's session in the application. Only requested user sessions are logged out.
  - **Enable service provider initiated logout service:** Enable the Toggle button to allow the IdP to accept logout requests from the ECE application. With this setting enabled, when the user logs out of a channel in the ECE application, a logout request is sent from the ECE 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. **Note:** In default ECE templates, the logout request is sent to the default provider configured in ECE. 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 ECE 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 **Enabled**.
  - **Request signing certificate:** Click the **Search and Add**  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, for example: C:\keystore\*version\_number*\SSO\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 application 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:** Click the Toggle button to enable. Setting this field to **Enabled** then enables the **Identity provider login URL** field.
  - **Identity provider login URL:** The URL for SAML authentication.
  - **Entity ID:** Entity ID or the service provider.

Create SSO Provider

General

Configuration

Identity Provider

SAML Version SAML 2.0

Entity ID\* 1005

Identity Provider Certificate\* \*\*\*\*\* +

Enable Encrypted Assertion

Assertion Decryption Certificate\* javakeystore.js +

Clock skew (in seconds)\* 0

Service Provider

Enable Identity Provider Initiated Logout Service

Enable Service Provider Initiated Logout Service

Close

Save


6. Click the **Save** button.

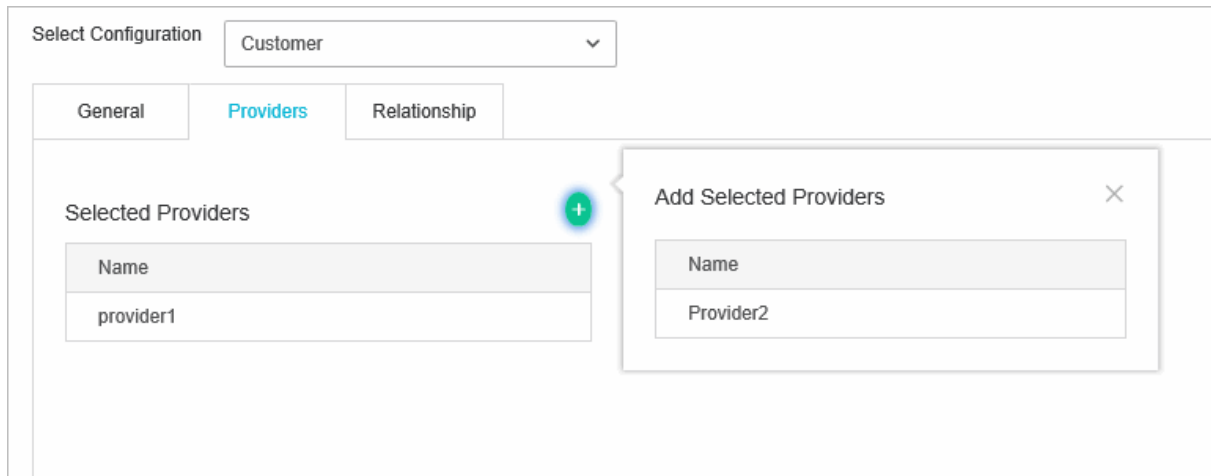
## Configuring Customer Single Sign-On

To configure settings for customer single sign-on:

1. In the partition-level Top menu, click the **Security** option.
2. In the Left menu, navigate to **Single Sign-On > Configurations**.
3. In the Select Configuration dropdown, select **Customer**.
4. 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 is 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. Under the Providers tab, click the **Search and Add**  button and 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](#).



6. 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 [Enabling chat Entry Points for Customer SSO](#).
7. Click the **Save** button.

## Enabling Chat Entry Points for Customer SSO

Before enabling chat entry points to use Chat Customer Single Sign-On, you must [configure the settings for secure chat](#).

To enable chat entry points for chat customer single sign-on:

1. In the department-level Top Menu, click the **Apps** option.
2. In the Left menu, navigate to **Chat & Messaging > Entry Points**.
3. Select an entry point you wish to modify.
4. Under the General tab, set the **Apply customer chat single sign-on** toggle to **On**.
5. Click the **Save** button. If at any point you need to see which entry points use chat customer SSO, they appear in the Relationship tab of the Customer SSO configuration.

Once you enable the Apply Customer Chat SSO setting for an entry point, the chat creation request must contain a SAML assertion. If the SAML assertion is missing, or is not valid for the entry point, chat requests are denied for that entry point.

## Configuring Your Website for Chat Customer SSO

Chat templates should also be configured for chat customer single sign-on. For more information on configuring chat templates for Secure Chat with templates, see [Enabling Customer Single Sign-On for Chat Templates](#).

## To configure your website for chat customer single sign-on:

1. Generate the HTML code for chat entry point. For more information about chat entry points, see [About Entry Points](#).
2. Edit the `egainDockChat.postChatAttributes` parameter in the HTML code. Set the value of this parameter to **True**.

If using an undocked template, edit `egainChat` properties in place of `egainDockChat` parameters.

3. Add the following code immediately after the `</script>` tag in the generated HTML code:

```
<script language=javascript>

    // Customer information passed to ECE as name-value pairs. Base64
    encoded SAML token is passed with the name "SAMLResponse"

    egainDockChat.storeChatParameters('SAMLResponse', '<Base64 encoded SAML
    assertion>'); // You MUST pass the SAML assertion with the name
    'SAMLResponse' in this function

</script>
```

You need to add an additional code to get the Base64 encoded SAML assertion for the user that is logged on to your website.

4. If you want to transfer any additional attributes outside the SAML assertion, you can pass them as name-value pairs using the `egainDockChat.storeChatParameters` function as follows:

```
<script language=javascript>

    // Customer information passed to ECE as name-value pairs. Base64
    encoded SAML token is passed with the name "SAMLResponse"

    egainDockChat.storeChatParameters('SAMLResponse', '<Base64 encoded SAML
    assertion>');

    egainDockChat.storeChatParameters('fieldname_2', '977-213-4444'); //
    SSN of the customer

    egainDockChat.storeChatParameters('fieldname_3', '4AZZXX7895463'); //
    account number of the customer

    //fieldname_2 and fieldname_3 are the second and third field
    respectively in the loginParameters array configured in the
    eGainLiveConfig.js file of the chat template

</script>
```

The attributes transferred as name-value pairs outside the SAML assertion must not be the same as the attributes transferred in the SAML assertion. This will result in chat request being denied.

5. Save your changes.

## Troubleshooting Chat Customer SSO

---

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 the administrators 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.
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'.

# Agent Single Sign-On

- [About Agent Single Sign-On \(SSO\)](#)
- [Preparing to Configure Single Sign-On](#)
- [Configuring Single Sign-On for Agents](#)
- [Configuring Single Sign-On for Partition Administrators](#)
- [Signing In with Single Sign-On](#)

## About Agent Single Sign-On (SSO)

---

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

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

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

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

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

- The process of configuring a system for single sign-on must be performed to the Security node at the partition level by a partition user with the following necessary actions: **View Application Security** and **Manage Application Security**.
- For supervisors and administrators to log into the consoles other than the Agent Console, once SSO is enabled, you must provide a valid External URL of the Application in the partition settings. See [General Partition Settings](#) for more information.
- A Java Keystore (JKS) certificate is needed to configure SSO to allow users with administrator or supervisor roles to sign in to partition 1 of ECE outside of Finesse using their SSO login credentials. Consult your IT department to receive the JKS certificate.
- A Secure Sockets Layer (SSL) certificate of Cisco IDS must be imported to all application servers in an installation. To obtain the necessary SSL certificate file, contact your IT department or Cisco IDS support.
- 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.

## Preparing to Configure Single Sign-On

---

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

## Integrating with Unified CCE or Packaged CCE

---

The application must already be properly integrated with Unified CCE or Packaged CCE. For more information about integrating with Unified CCE or Packaged CCE, see [About CCE Integration](#).

## Configuring an Identity Provider

---

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

If you wish configure SSO to allow users with administrator or supervisor roles to sign in to the partition 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, see *Enterprise Chat and Email Administrator's Guide to the Administration Console*.

To configure public key certificate in the relying party trust:

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

## Creating and Importing Certificates

---

Before configuring SSO to use Cisco IDS for [Single Sign-On for Agents](#), the Cisco IDS certificate must be imported into the application. For more details, see [About Certificate Management](#).

## Configuring Agent Single Sign-On

---

To configure SSO for agents:

1. In the partition-level Top Menu, click the **Security** option.
2. In the Left menu, navigate to **Single Sign-On > Configurations**.
3. In the Select Configuration dropdown, select **Agent**.
4. In the General tab, set the following:
  - **Enable Single Sign-On:** Click the Toggle button to enable SSO.
  - **Single Sign-On Type:** Select **Cisco IDS**.
  - **Create or update user account on login:** This toggle is used for user auto-provisioning. This is not available for ECE.
5. Click the **SSO Configuration** tab. Contact your Unified CCE administrator to acquire the necessary details for the following sections. Provide the following:

- **Primary User Info Endpoint URL:** The User Info Endpoint URL of the primary Cisco IDS server. This URL validates the user token/User Info API. This value can be provided by the Cisco IDS server management team. It is in format: `https://cisco-ids-1:8553/ids/v1/oauth/userinfo` where *cisco-ids-1* indicates the Fully Qualified Domain Name (FQDN) of the Primary Cisco IDS server.
- **User Identity Claim Name:** The name of the claim returned by the User Info Endpoint URL, which identifies the username in Unified or Packaged CCE. The claim name and the username in Unified or Packaged CCE should match. This is one of the claims obtained in response to the Bearer token validation. This value can be provided by the Cisco IDS server management team.
  - If the username of agents in Unified or Packaged CCE matches the User Principal Name, provide "upn" as the value for User Identity Claim name field.
  - If username of agents in Unified or Packaged CCE matches with the SAM Account Name, provide "sub" as the value for User Identity Claim name field.
- **Secondary User Info Endpoint URL:** The secondary user Info Endpoint URL of the Cisco IDS server. This value can be provided by the Cisco IDS server management team. It is in format: `https://cisco-ids-2:8553/ids/v1/oauth/userinfo` where *cisco-ids-2* indicates the Fully Qualified Domain Name (FQDN) of the Secondary Cisco IDS server.
- **User Info Endpoint URL Method:** The HTTP method used by ECE for making Bearer token validation calls to the User Info Endpoint URL. Select one of the following options. The option selected here should match the IDS server's method.
  - 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.
- **Access Token Cache Duration (Seconds):** The duration, in seconds, for which a Bearer token should be cached in ECE. Bearer tokens for which validation calls are successful are only stored in caches. (Minimum value: 1; maximum value 30)
- **Allow SSO Login Outside Finesse:** Click this Toggle button if you wish to allow users with administrator or supervisor roles to sign in to the partition of ECE outside of Finesse using their SSO login credentials. If enabled, information under the Identity Provider and Service Provider sections must be provided. This requires that your IdP configuration allows for a shared IdP server.

### Configurations

Select Configuration Agent

General
SSO Configuration

OpenId Connect Provider

---

Primary User Info Endpoint URL\* https://v288891.cic.na:/ids/v1/oauth ...

User Identity Claim Name\* sub

Secondary User Info Endpoint URL https://v288891.cic.na:/ids/v1/oauth ...

User Info Endpoint URL Method\* GET

Access Token Cache Duration (Seconds)\* 30

Allow SSO Login Outside Finesse

Identity Provider

---

Entity ID\* :adfs01.edgemo.info/adfs/services/trust

Identity Provider Certificate\* \*\*\*\*\* +


Cancel
Save

6. If **Allow SSO Login Outside of Finesse** is set to **Enabled**, provide the following details in the Identity Provider section:

- **Entity ID:** Entity ID of the IDp server. For example, the FQDN of the IDp server.
- **Identity Provider Certificate:** The public key certificate. 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 encrypted assertion with the Identity Provider for console login, click the Toggle button set the value to **Enabled**. If not, set the value to **Disabled**.
- **Assertion Decryption Certificate:** If Enable encrypted assertion is set to **Enabled**, click the **Search and Add**  button and confirm your choice to change the certificate. 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.

7. If **Allow SSO Login Outside of Finesse** is set to **Yes**, provide the following in the Service Provider section:

- **Service Provider Initiated Authentication:** Set the toggle button to **Enabled**.
- **Pass Subject Attribute to SAML Request:** If the Identity Provider (IdP) supports the Subject attribute in the SAML authentication request, set the toggle button to **Enabled**.
- **Entity ID:** Provide the External URL of the ECE application.
- **Request Signing Certificate:** A Java Keystore (JKS) certificate is needed to provide the necessary information. Consult your IT department to receive the JKS certificate. Click the **Search and Add**  button and provide the following information.
  - **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.

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 [Preparing to Configure Single Sign-On](#).

- **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`.

- **Identity Provider 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.
8. Click the **Save** button.
  9. In the partition-level Top Menu, click the **Apps** option.
  10. In the Left menu, navigate to **General Settings**.
  11. In the General Settings space, go to the **External URL of the ECE application** setting and provide the external-facing URL. For more information, see [General Partition Settings](#).
  12. Click the **Save** button.

## Configuring SSO for Partition Administrators

---

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

- This process is to configure single sign-on for partition administrators that are auto-provisioned in ECE when they access the ECE gadget in the CCE Admin Web interface. This process is not applicable for configuring SSO for partition administrators created locally in ECE.
- This is for the ECE gadget accessed within CCE Admin WEB interface. For example, `https://IP_Address/cceadmin`.
- 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 server can access this LDAP server URL to avoid connectivity issues.

### To configure SSO for partition administrators:

1. In the partition-level Top Menu, click the **Security** option.
2. In the Left menu, navigate to **Single Sign-On > Configurations**.
3. In the Select Configuration dropdown, select **Partition Administrator**.
4. In 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.

Partition can be added automatically to the system when ECE is accessed via the CCE Administration Console if ECE is configured with LDAP lookup. However, in Active Directory deployments with multiple domains in a single forest or where Alternate UPNs are configured, the Domain Controller URL with the standard LDAP ports of 389 and 636 should not be used. The LDAP integration should be configured to use the Global Catalog URL with ports 3268 and 3269.

- **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`.
- **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.

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.

### Configurations

Select Configuration Partition Administrator

SSO Configuration

LDAP URL *	<input style="width: 90%;" type="text" value="ldap://rmlab-adddc.ciscolab.com:444"/>
DN attribute *	<input style="width: 90%;" type="text" value="userPrincipalName"/>
Base	<input style="width: 90%;" type="text" value="CN=Users,DC=ciscolab,DC=com"/>
DN for LDAP search	<input style="width: 90%;" type="text" value="strator,CN=Users,DC=ciscolab,DC=com"/>
Password	<input style="width: 90%;" type="password" value="....."/>

Cancel
Save

5. Click the **Save** button.

## Signing In with Single Sign-On

- 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 Enabled and, in this example, ADFS is used as the Identity Provider:
  - Users can login with Identity Provider initiated SSO to the partition using the following URL:
 

```
https://ADFS server FQDN/adfs/ls/idpinitiatedsignon.aspx?
loginToRP=Relying PartyTrust Identifier in URL encoded format
```
  - Users can login with Service Provider initiated (SSO / Non-SSO) to the Reports Console by using the following URL:
 

```
http(s)://external_url_of_application/context_root/web/apps/consoles URI
```
- 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://external\\_url\\_of\\_application/desktop](https://external_url_of_application/desktop).

For more information about configuring users, see Editing User Details in Departments.

# Data Adapters

- [About Data Adapters](#)
- [About Data Adapter Authentication](#)
- [Configuring Basic Authentication](#)
- [Configuring OAuth 2.0 Authentication](#)
- [Deleting Authentication Configurations](#)
- [About Access Links](#)
- [Creating Web Service - RESTful Links](#)
- [Testing Access Links](#)
- [Deleting Access Links](#)
- [About Data Usage Links](#)
- [Creating Usage Links](#)
- [Configuring the Display of Results](#)
- [Assigning Permissions on Usage Links](#)
- [Testing Usage Links](#)
- [Deleting Usage Links](#)
- [About Usage Link Groups](#)
- [Creating Usage Link Groups](#)
- [Configuring the Display of Results](#)
- [Assigning Permissions on Usage Link Groups](#)
- [Deleting Usage Link Groups](#)
- [Example One – Get Weather Information for a City](#)
- [Example Two – Extract Stock Information From a Website](#)
- [Example Three – Shorten URLs Using Google API](#)

# About Data Adapters

---

The Data Adapter module provides you with a quick and easy method to integrate with external sources of information residing within your enterprise, or on the web. It is a flexible integration tool for accessing data from external sources such as local and remote databases, HTTP or HTTPS services, XML files, and so on. The data is then available through XML APIs for automated processing and display.

External information is accessed and processed through two-way connections called data links. Data links can be used to display and process external information in the application, as well as to extract and present information in external applications.

## Do You Need Data Links?

---

The benefits of using the Data Adapter is manifold, but consider the following factors to evaluate the need to set up data links.

- Who owns the data?

If an external system controls the reading and writing of data or if important data is in an external database, you are likely to need data links.

- How do you access the data?

If access to external data is through defined APIs, URLs, or web services, or if the protocol for information transfer is not open, you are likely to need data links.

- What is the nature of the data required in customer interactions?

You are likely to need data links if interactions with customers require information that:

- Is very customer-specific and not "global."
- Ages quickly, so that agents have to access data in real time.
- Is used frequently, so agents have to access the information for each customer interaction.

## How Do Data Adapters Work?

---

Data links are of two types:

1. Access links, which connect to the external source and fetch data. Access links are discussed in detail in [About Access Links](#).
2. Usage links, which use the fetched data either in displays within the application, or as input criteria for making decisions about processing information within the application. Usage links are explained in [About Usage Links](#).

A working data-link connection typically involves:

- Creating a data access link to fetch data from the external source.

- Creating data usage links, which are made available to users to process the data extracted from the external source. Multiple usage links can be grouped to create a single display. Usage link grouping is discussed in detail in [About Usage Link Groups](#).

## Where and How Can You Use Data Links?

---

Once data links are created, they can be used in the following modules:

### Workflows

- Data retrieved from usage links can be used in "IF" conditions to make routing decisions or to update attributes of business objects.

### The Agent Console

- Usage links that can be executed by the agent are displayed in the Links section in the Information pane of the agent desktop. Agents can add the output of usage links to responses by clicking the **Add to Reply** button.

## About Data Adapter Authentication

---

While some web services have publicly available APIs and links that data adapters can use, there are plenty of services out there that require security clearance. Thus, it may be necessary to configure data adapters to use provide these services with the required authentication details. There are two options for the type of authentication configurations: **Basic** and **OAuth 2.0**. You can create a maximum of 25 authentication configurations. It is recommended you create your authentication configurations before configuring the access links. For more information, see [About Access Links](#).

## Configuring Basic Authentication

---

Basic authentication uses standard fields in the HTTP header, obviating the need for handshakes.

Data-adapter authenticates to "basic authentication" enabled web services with a username and password combination, the client's username and password are concatenated, and passed in the Authorization HTTP header.

To create a basic data adapter authentication configuration:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Authentication**.
3. Click the **New** button.
4. In the Create Authentication workspace, on the General tab, provide the following details:
  - **Name:** The name for the configuration.
  - **Description:** A brief description of the configuration.
  - **Authentication Type:** Select **Basic**.

**Create Authentication**

General Configuration

Name\* Basic Authentication

Description

Authentication Type\* Basic

5. Under the Configuration tab, provide the following details:
- **User name:** The user name for the account the data adapter will use for authentication.
  - **Password:** The password for the account the data adapter will use for authentication.

**Create Authentication**

General Configuration

User Name\* adapter\_user

Password\* .....

6. Click the **Save** button to save your configuration. This configuration can now be used when creating data links. For more information, see [About Access Links](#).

## Configuring OAuth 2.0 Authentication

---

OAuth2.0 configuration is required for web-services that need user's authorization to allow its resources access to the third-party client. OAuth generated/provided Access Token is passed in the Web services Authorization HTTP header.

To create an OAuth 2.0 data adapter authentication configuration:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Authentication**.

3. Click the **New** button.
4. In the Create Authentication workspace, on the General tab, provide the following details:
  - **Name:** The name for the configuration.
  - **Description:** A brief description of the configuration.
  - **Authentication Type:** Select **OAuth 2.0**.

The screenshot shows a web form titled "Create Authentication". It has two tabs: "General" (which is active and highlighted with a blue border) and "Configuration". Under the "General" tab, there are three input fields:

- Name\***: A text input field containing the text "OAuth2.0 authentication".
- Description**: An empty text input field.
- Authentication Type\***: A dropdown menu with "OAuth2.0" selected and a downward arrow on the right.

5. Under the Configuration tab, provide the following details:
  - **OAuth2 ClientId:** The unique string representing the registration information provided by the service provider.
  - **OAuth2 ClientSecret:** The unique string provided by the service provider that acts as a means of authorizing a client, that requested an access token.
  - **Refresh Token:** The credential used to obtain new access tokens when the current access token expires.
  - **Token Request URL:** The access token request URL and click **OK** to close the window. This field is required.
  - **Method:** Select the method in which the access token is retrieved. Select either **Post** or **Get**. The method selected depends on what the client authentication server supports.

If Method is specified as **GET**, then the **Content-Type** and **Token Request Body** fields are disabled as these field values are not used in the actual token request.
  - **Content-Type:** Select the format of the content type. The options are : **application/json**, **application/xml**, or **application/x-www-form-urlencoded**.
  - **Token Request Body:** The parameters for the token request body. Format the parameters string property with variables and values to ensure that correct information in the request is sent. i.e.

```
client_id=<client_id>&client_secret=<client_secret>&refresh_token=
<refresh_token>&grant_type=refresh_token
```

- **Access Token JSON Path:** The JSON query path of an attribute in the return JSON response. For example: `$.access_token`
- **Access Token:** If you wish to provide a current access token, enter the string in the field. Leave this field blank if you do not have an Access Token, new token will be requested by application using the provided details.
- **Headers:** Any necessary additional values to include in the response header by entering a Name and Value for the fields. When you have entered the necessary header values, click the **Add** button to add the values to the header. Do this as many times as necessary. Note that you cannot add content-type header name and value for either **GET** or **POST** methods.

The screenshot shows the 'Create Authentication' configuration window with the 'Configuration' tab selected. The form contains the following fields and values:

- OAuth2 ClientId:** 234454232350-3ixytzcyj6878977t557...
- OAuth2 ClientSecret:** [Redacted]
- Refresh Token:** 1/V8kjDpK8H4jijGH67hKlknjikosHijik7...
- Token Request URL\*:** https://googleapis.com/auth2/v4/token
- Method\*:** POST
- Content-Type\*:** application/x-www-form-urlencoded...
- Token Request Body\*:** <client\_secret>&refresh\_token=<refresh\_token>&grant\_type=refresh\_token
- Access Token JSON Path\*:** \$.access\_token
- Access Token:** [Redacted]

At the bottom, there is a 'Headers' section with two input fields: 'Header Name' and 'Header Value'.


6. Click the **Save** button to save your configuration. This configuration can now be used when creating data links. For more information, see [About Access Links](#).

Keep the OAuth2.0 configuration up-to-date in the application as it changes based on the web-services provider access and authorization policies.

## Deleting Authentication Configurations

An authentication configuration cannot be deleted if it is used in a data access link.

To delete an authentication configuration:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Authentication**.
3. In the Authentication workspace, hover your mouse over the authentication you wish to remove and click the **Delete**  button.
4. Click the **Yes** button when the system prompts you to confirm the deletion.

## About Access Links

---

Access links connect to the external source and fetch data.

The following access link types can be created:

- **Web service - RESTful link:** A web service link provides the mechanism to connect to a web service using representation state transfer (REST) operations. With these type of data access links, the web service APIs of third-party applications can be used to perform necessary functions, instead of developing custom applications to perform the same actions. To configure a RESTful link, you need the API request URL (HTTP/HTTPS) with the desired method (Get, Post, Put, Delete), along with any necessary authentication details. If necessary, a header and body can be provided as well.

Working on access links involves:

- **Configuring authentication details:** If the data links you are creating require authentication, you can configure the authentication format and details. For more information, see [Configuring Data Adapter Authentication Information](#).
- **Creating access links:** Creating access links is the first step in creating data adapters. Access links extract the data from the source.
- **Testing access links:** After creating the access links you can test them to ensure that they are working properly.

## Creating Web Service - RESTful Links

---

To create a web service link:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Access Links**.
3. Click the **New** button.

You can create a maximum of 75 access links in a department.

4. In the Create Access workspace, under the General tab, provide the following details.
  - **Name:** Type the name for the web service link.
  - **Type:** This is set to Web Service - RESTful and cannot be changed.


**Method:** Provide the API input method by selecting one of the following options from the dropdown list.

- **Get**
  - **Post**
  - **Put**
  - **Delete**
- **Description:** Type a brief description.

The screenshot shows a web form titled "Create Access Link". It has three tabs: "General", "Input", and "Output". The "General" tab is active. The form contains the following fields:

- Name\***: A text input field containing "Stock Rates".
- Type\***: A dropdown menu with "Web Services - RESTful" selected.
- Method\***: A dropdown menu with "GET" selected.
- Description**: An empty text input field.

5. Under the Input tab, provide the following details.

- **URL:** Provide the request URL.
- **Authentication:** If you have created an authentication configuration for this data link, select the appropriate configuration from the dropdown list. For more information, see [Configuring Data Adapter Authentication Information](#). If authentication is not required, select **None**.
- **Accept:** Select the format you wish the output of the data link to use: **application/json** or **application/xml**.
- **Content-type:** Select the format you wish the content that web services link expect as an input. Select either **application/json**, **application/xml**, or **application/x-www-form-urlencoded**.
- **Body:** Provide the body for the response.
- **Header:** Provide Any necessary additional values to include in the response header by entering a Name and Value for the fields. When you have entered the necessary header values, click the **Add**  button to add the values to the header. Do this as many times as necessary.

URL, Body, and Header values accept the input variables in the format `<%variable_name%>`. These variables can be mapped to business object macros for pass contextual data to the web-services call.

### Create Access Link

General
Input
Output

URL\*

Authentication\*

Accept\*

Content-Type\*

Body

Headers

Header Name	<input style="width: 95%;" type="text"/>	Header Value	<input style="width: 95%;" type="text"/>	+
-------------	------------------------------------------	--------------	------------------------------------------	---

Header Name	Header Value
No items to display in list.	

6. Under the Output tab, click the **New** button.

7. In the Create Output Format window, provide the output path information:

- **Extract Or Filter:** Select one of the options from the dropdown. Select **Extract** to fetch the attribute or an object from the original web-services response. Select **Filter** to filter an attribute/object from the above extracted object. Extraction and filters work based on the XPATH and JSON query.
- **PATH:** Provide the path for the response. Enter XPATH query when expected output is in XML format. OR enter JSON query when expected output is in JSON format. An example of JSON output:  

```
{ "firstName": "John", "lastName" : "Bell", "age"      : 26, "address"
  : { "streetAddress": " 1252 Borregas Avenue ", "city"      : "
Sunnyvale ", "postalCode"  : " 94089 " } } JSON Query to fetch
Fist name from the above output Extract or Filter : Extact PATH :
$.firstName
```
- **Internal Field Name:** Provide the response field name.
- **Field Order:** Provide the response field order.
- **Decoding:** Provide the decoding format if necessary. The data extracted can be decoded to map the output values to user defined strings. For example, if the values returned are 1 and 0, then they can be mapped to Yes and No respectively by entering the following string:  
0=No,1=Yes.

Create Output Format

Extract Or Filter\* Extract

Path\* \$.identifier

Internal Field Name\* Stock Symbol

Decoding

Cancel Done

8. Click the **Done** button to set the output and close the window. In the Output JSON Format space, the **Field Order** field is automatically updated as more and more output formats are created.
9. Click the **Save** button.

## Testing Access Links

---

After creating the links, you can test them to see if they are created properly.

To test an access link:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Access Links**.
3. In the Access Links space, select the link you want to test.
4. In the Edit Access space, click the **Test** button.
5. The Test Data Access Link window appears, where you can enter the values for the input parameters of the link and click the **OK** button.

The Test Data Access Link window appears only if any input parameter needs to be provided.


The Result window appears. Here, you can view the results of the test. If the access link is not configured properly, an error message is displayed.

## Deleting Access Links

---

If the access link is being used in a usage link it will not get deleted. To be able to delete it, first remove it from the usage link.

To delete an access link:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Access Links**.
3. In the Access Links workspace, hover your mouse over the link you wish to remove and click the **Delete**  button.
4. Click the **Yes** button when the system prompts you to confirm the deletion.

The Delete button is enabled only if you have the delete permission on the access link.

## About Data Usage Links

---

After you have created access links, you can define the display format of the data that is fetched by the access link. This is done using usage links. Different types of access links can be used in a single usage link. Usage links support macros, making them simple to use in workflows and by agents.

## Creating Usage Links

---

To create a usage link:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Usage Links**.
3. Click the **New** button.

You can create a maximum of 75 usage links in a department.

4. In the **Create Usage Link** space, under the General tab, provide the following details.
  - **Name:** Type the name of the usage link.
  - **Description:** Type a brief description.

Set the following fields if you want to configure macros for the usage link. Macros can be configured only for usage links that do not require any input parameters.

- **Macro Name:** Type a name for the macro. A macro name cannot contain spaces, or any of the following characters: < ` , . ? ; ; & " ' !
- **Default Value:** Type the default value of the macro. When the macro is expanded, and the macro does not have any content, the default value of the macro is used. The default content should be adequate enough to represent the original content.

### Create Usage Link

- General
- Data Access Links
- Input
- Output
- Formatting
- Permissions

Name\*

Description

---


Macro Details

Macro Name

Description


Default Value


Exception Article  +

- Under the Data Access Links tab, click the **Search and Add**  button. In the Add Selected Data Access Links pop-up, select the data access links.

### Create Usage Link

- General
- Data Access Links
- Input
- Output
- Formatting
- Permissions

Data Access Links 

Name
Stock Advanced 

- The Input tab shows all the input parameters configured for the data access links selected in the Data Access Links tab. Here, you can pre-determine values for some or all available parameters. You can

create different usage links from the same access link, and just change the value of the input parameters here, to get different answers.

The screenshot shows the 'Create Usage Link' dialog box with the 'Input' tab selected. It contains a table with the following data:

Data Access Link	Parameter Name	Parameter Type	Parameter Value
Stock Advanced	ticker_sym	String	IBM

- Under the Output tab, click the **New** button.
- In the Create Output Format window, provide the following details:
  - **Data Access Link:** From the dropdown list, select the data access link.
  - **Field Name:** From the dropdown list, select the field name.
  - **Display Name:** Type the display name for the field in which the data is to be extracted.
  - **Field Width:** Specify the width of the field.
  - **Hyperlink:** Set the hyperlink.

The screenshot shows the 'Create Output Format' dialog box with the following fields:

- Data Access Link\*: Stock Advanced
- Field Name\*: Stock Symbol
- Display Name\*: Stock Symbol
- Field Width: 4
- Hyperlink: (empty dropdown)

Buttons: Cancel, Done

- Click the **Done** button.
- Click the **Save** button.

After creating the usage links, create macros for the usage links, configure the display of results for the Agent Console, assign permissions to users so that they can access the usage links, and test the usage links.

## Configuring the Display of Results

---

After you have created the usage link, you can configure how the results should appear in the Agent Console.

To configure the display of results:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Usage Links**.
3. Select the link you wish to edit.
4. In the Edit Usage Link space, on the Formatting tab, provide the following details.
  - **Header:** Specify a header for the results.
  - **Footer:** Specify a footer for the results.
  - **Include column headers in response:** With this option, you can specify that when the agents adds the results of a usage link to the Reply pane, the header and footer of the result will be added to the response or not. By default it is disabled. Select **Yes** to enable it.

The screenshot shows the 'Create Usage Link' dialog box with the 'Formatting' tab selected. The dialog has a title bar 'Create Usage Link' and a tabbed interface with tabs for 'General', 'Data Access Links', 'Input', 'Output', 'Formatting', and 'Permissions'. The 'Formatting' tab is active and contains three fields: 'Header' with the value 'Stock Rates', 'Footer' which is empty, and 'Include Column Headers In Response' which is a toggle switch currently turned on.

5. Click the **Save** button.

## Assigning Permissions on Usage Links

---

After creating the data usage links, the next most important step is to give permissions to the users to access the data usage links. The user who creates the data usage link does not get the execute and delete permissions automatically. You have to assign these permissions to yourself to be able to execute or delete the data usage link. To add usage links as macros to other usage links, you must have execute permissions.

To assign permissions:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Usage Links**.
3. Select the link you wish to edit.

4. In the Edit Usage Link space, on the Permissions tab, assign the following permissions to users and user groups:
  - Own
  - View
  - Edit
  - Delete
  - Execute: Users with execute permissions are the only ones who can use the usage links. You must give this permission to all the users who should have access to the usage links.
5. Click the **Save** button.

## Testing Usage Links

---

After creating the usage links you can test them to see if they are created properly. It is highly recommended that you test your links after creating them.

### To test the usage link:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Usage Links**.
3. Select the link you wish to edit.
4. In the Edit Usage Link space, click the **Test** button.

The Test Data Usage Link window appears, where you enter the values for the input parameters of the link. The Result pane is enabled and here you can view the results.


The Test Data Usage Link window appears only if any input parameter needs to be provided.

## Deleting Usage Links

---

If the usage link is used in a usage link group, it cannot be deleted. To be able to delete it, first remove it from the usage link group.

### To delete a usage link:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Usage Links**.
3. In the Usage Links workspace, hover your mouse over the link you wish to remove and click the **Delete**  button.

The **Delete** button is enabled only if you have the delete permission on the usage link group.

4. Click the **Yes** button when the system prompts you to confirm the deletion.

# About Usage Link Groups

---

A data usage link group is a combination of two or more data usage links. To be able to create usage link groups, you need to first create the usage links.

## Creating Usage Link Groups

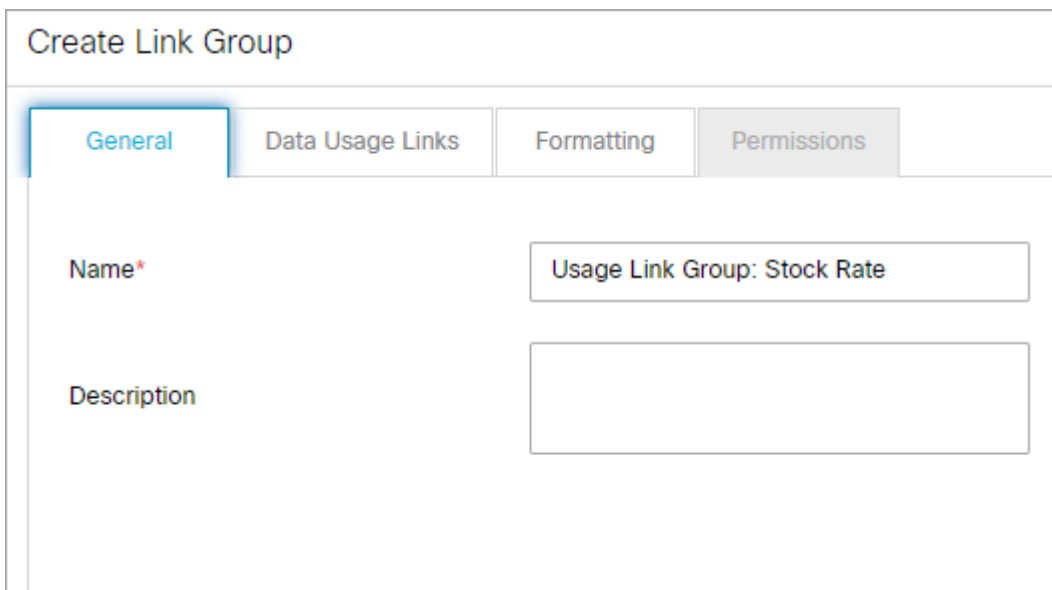
---

To create a link group:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Link Groups**.
3. Click the **New** button.

You can create a maximum of 75 link groups in a department.

4. In the Create Link Group space, under the General tab, provide the following details.
  - **Name:** Type the name of the usage link group.
  - **Description:** Type a brief description.



The screenshot shows a web interface titled "Create Link Group". It has four tabs: "General", "Data Usage Links", "Formatting", and "Permissions". The "General" tab is active. Below the tabs, there are two input fields. The first is labeled "Name\*" and contains the text "Usage Link Group: Stock Rate". The second is labeled "Description" and is currently empty.

5. Under the Data Usage Links tab, click the **Search and Add**  button. In the Add Selected Data Usage Links pop-up, select the data access links.

The screenshot shows a 'Create Link Group' window with four tabs: 'General', 'Data Usage Links', 'Formatting', and 'Permissions'. The 'Data Usage Links' tab is selected. Below the tabs, there is a section titled 'Data Usage Links' with a green plus icon in the top right corner. A table is displayed with the following content:

Name
Stock Rates

6. Click the **Save** button.

After creating the usage link groups, configure the display of results for the agent desktop and assign permissions to users so that they can access the usage link group.

## Configuring the Display of Results

---

After you have created the usage link group, you can configure how the results should appear in the Agent Console.

To configure the display of results:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Link Groups**.
3. Select the link group you wish to edit.
4. In the Edit Link Group space, on the Formatting tab, provide the following details.
  - **Number of rows:** Specify the number of rows you want in the results page when you run the link.
  - **Number of columns:** Specify the number of columns you want in the results page when you run the link.
  - **Orientation:** From the dropdown list, select the orientation. The options available are:
    - **Fill rows and then fill columns**
    - **Fill columns and then fill row**
  - **Header:** Specify a header for the results.
  - **Footer:** Specify a footer for the results.

### Create Link Group

General

Data Usage Links

Formatting

Permissions

Number of Rows*	<input style="width: 90%;" type="text" value="1"/>
Number of Columns*	<input style="width: 90%;" type="text" value="1"/>
Orientation*	<input style="border-bottom: 1px solid #ccc;" type="text" value="Fill Columns and Then Fill Rows"/> <span style="font-size: 0.8em;">▼</span>
Header	<input style="width: 90%;" type="text" value="Stock Rates"/>
Footer	<input style="width: 90%;" type="text"/>

5. Click the **Save** button.

## Assigning Permissions on Usage Link Groups

After creating the data usage link groups, the next most important step is to give permissions to users to access the data usage link group. All users (that includes administrators, authors, and agents) who need to use the data usage link groups must be given the Execute permission on the link. The user who creates the data usage link group does not get the execute and delete permissions automatically.

### To assign permissions:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Link Groups**.
3. Select the link group you wish to edit.
4. Select the Permissions tab.
5. In the Types box, choose the permission type you wish to set. Options include:
  - **User:** Sets permissions at the individual user level.
  - **Group:** Sets permissions at the user group level.
6. Once you have selected a permission type, assign the following permissions to users and user groups:
  - Own
  - View
  - Edit

- Delete
- Execute: The users with execute permissions are the only ones who can use the usage link groups. You must give this permission to all the users who should have access to the usage link groups.


7. Click the **Save** button.

## Deleting Usage Link Groups

---

To be able to delete the usage link group, you need to have delete permissions on it. The user who creates the usage link does not get this permission automatically. You have to give delete permissions to yourself, to be able to delete the usage link group. For information on how to give permissions, see [Assigning permissions on usage link groups](#).

To delete a usage link group:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Link Groups**.
3. In the Link Groups workspace, hover your mouse over the group you wish to remove and click the **Delete**  button.

The **Delete** button is enabled only if you have delete permission on the usage link group.

4. A message appears asking to confirm the deletion. Click **Yes** to delete the usage link group.

## Example One – Get Weather Information for a City

---

In this example, we describe how to create Web Services- RESTful link to look up weather using the weather report API available from [www.openweathermap.com](http://www.openweathermap.com). This example does not use any authentication.

These examples follow the process outlined in “Creating Web Service - RESTful Links” on page 16. Please refer to this section for more information about creating access links.

To create a link:

1. Before creating the link, sign-up at <http://www.openweathermap.com> and get the API key to be used for the data adapter.
2. In the department-level Top Menu, click the **Data Adapters** option.
3. In the Left menu, navigate to **Access Links**.
4. Click the **New** button.
5. In the Create Access space, under the General tab, provide the following details.
  - **Name:** Type a name.
  - **Type:** Type is set to **Web Services - RESTful** and cannot be changed.
  - **Method:** Set the method as **Post**.

6. Select the Input tab and provide the following details.

- **URL:** Type the URL

`http://api.openweathermap.org/data/2.5/weather?  
q=<%city%>&APPID=c854f43c700fa17b1729367c9e0648e9`

The `<%city%>` sets up the dynamic variable that needs a value every time this access link is executed.

Replace the value of APPID in the URL with the API key value generated at <http://www.openweathermap.com>.

- **Authentication:** Set as **None**.
- **Accept:** Set as **application/json**.
- **Content-type:** Set as **application/x-www-form-urlencoded**.

### Create Access Link

General **Input** Output

URL\*

Authentication\*

Accept\*

Content-Type\*

Body

Headers

Header Name	Header Value
<input type="text"/>	<input type="text"/>

+

7. Select the Output tab and click the **New** button. Provide the following details:

- **Extract Or Filter:** Select **Extract**.
- **PATH:** Set as **\$. weather[0]['description']**.
- **Internal Field Name:** Provide the name as **Weather**.

8. Click the **Save** button.
9. In the Output JSON Format space, the value of the **Field Order** field is automatically updated as **1**.
10. Select the access link you just created from the list.
11. Click the **Test** button. The Test Data Access Link window appears.
12. In the Test Data Access Link window, type the city name as Sunnyvale.
13. The Results tab then displays the weather information for Sunnyvale.

## Example Two – Extract Stock Information From a Website

---

In this example, we describe how to create a data access link to look up asking price for stocks using the API from <https://intrinio.com>. This example uses basic authentication.

### Configure Basic Authentication

---

To create authentication:

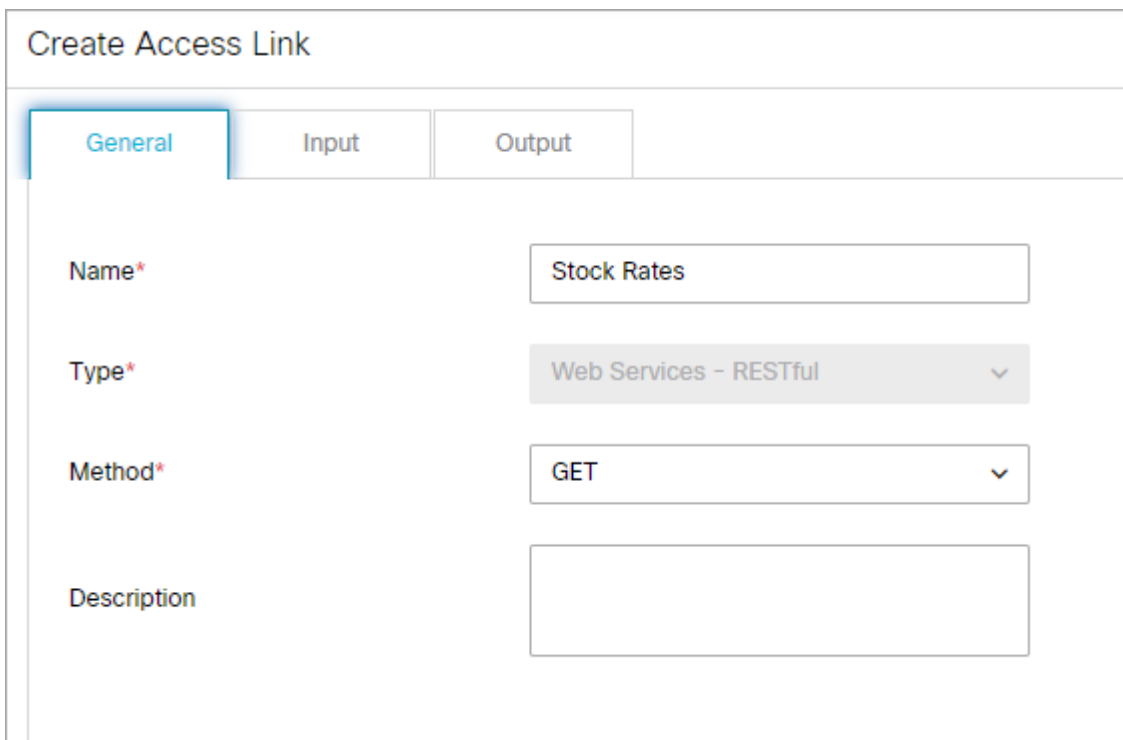
1. Sign-up at <https://intrinio.com> and get the API username and password to be used for the data adapter.
2. In the department-level Top Menu, click the **Data Adapters** option.
3. In the Left menu, navigate to **Authentication**.
4. Click the **New** button and follow the instructions outlined in [Configuring Basic Authentication](#) to configure authentication using the username and password generated from <https://intrinio.com>. Name this example authentication "Intrinio Basic Auth".

## Create the Access Link

---

To create a link:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Access Links**.
3. Click the **New** button.
4. Select the General tab, provide the following details.
  - **Name:** Type the name as *Stock rates*.
  - **Type:** Type is set to **Web Services - RESTful** and cannot be changed.
  - **Method:** Set the method as **Get**.



The screenshot shows a web form titled "Create Access Link". It has three tabs: "General", "Input", and "Output". The "General" tab is selected. The form contains the following fields:

- Name\***: A text input field containing "Stock Rates".
- Type\***: A dropdown menu with "Web Services - RESTful" selected.
- Method\***: A dropdown menu with "GET" selected.
- Description**: An empty text area.

5. Select the **Input** tab and provide the following details.
  - **URL:** Type the URL  

```
https://api.intrinio.com/data_point?
identifier=<%ticker_sym%>&item=ask_price.
```

The `<%ticker_sym%>` sets up the dynamic variable that needs a value every time this access link is executed.
  - **Authentication:** Select the example "Intrinio Basic Auth" example you just created for `https://intrinio.com`.
  - **Accept:** Set as **application/json**.
  - **Content-type:** Set as **application/x-www-form-urlencoded**.

### Create Access Link

General
Input
Output

URL\*

Authentication\*

Accept\*

Content-Type\*

Body

Headers

Header Name	<input style="width: 95%;" type="text"/>	Header Value	<input style="width: 95%;" type="text"/>	<input data-bbox="1380 763 1422 804" style="width: 20px; height: 20px;" type="button" value="+"/>
-------------	------------------------------------------	--------------	------------------------------------------	---------------------------------------------------------------------------------------------------

Header Name	Header Value
No items to display in list.	

6. Select the Output tab, click the **New** button, and provide the following details.

- **Extract Or Filter:** Select **Extract**.
- **PATH:** Set as **\$.identifier**.
- **Internal Field Name:** Provide the name as **Stock Symbol**.

Click the **Done** button to return to the Output Format page. In the Output JSON Format space, the value of the **Field Order** field is automatically updated as **1**. Then click the **New** button.

- **Extract Or Filter:** Select **Extract**.
- **PATH:** Set as **\$.value**.
- **Internal Field Name:** Provide the name as **Ask Price**.

Click the **Done** button. In the Output Format JSON space, the value of the **Field Order** field is automatically updated as **2**.

### Create Access Link

General
Input
Output

Output Format JSON

New

Extract Or Filter	Path	Internal Field Name	Field Order	Decoding
Extract	\$.value	Ask Price	<input style="width: 50px; text-align: center;" type="text" value="1"/>	
Extract	\$.identifier	Stock Symbol	<input style="width: 50px; text-align: center;" type="text" value="2"/>	

7. Click the **Save** button.
8. Once you have returned to the Access Links list, select the Stock Rates link you just created.
9. Click the **Test** button. The Test Data Access Link window appears.
10. In the Test Data Access Link window, type the `ticker_sym` as *IBM*.
11. The Result tab then displays the stock price extracted from the website.

## Example Three – Shorten URLs Using Google API

---

In this example, we describe how to create a data access link to create short URLs using the Google API. This example uses OAuth authentication.

### Configure OAuth 2.0 Authentication

---

To configure authentication:

1. Sign-up and enable OAuth2.0 for URL Shortener API at <https://developers.google.com/apis-explorer/#p/>
  - From the Google API Manager, note down the client ID, client secret, and refresh token to be used for the data adapter.
2. In the department-level Top Menu, click the **Data Adapters** option.
3. In the Left menu, navigate to **Authentication**.
4. Click the **New** button.
5. [Configure OAuth 2.0 Authentication](#) using the client ID, Secret, and refresh token generated from <https://developers.google.com>. For the rest of the fields, provide following details:
  - **Token Request URL:** Set as `https://www.googleapis.com/oauth2/v4/token`.
  - **Method:** Set as **Post**.

If Method is specified as **GET**, then the **Content-Type** and **Token Request Body** fields are disabled as these field values are not used in the actual token request.

- **Headers:** Set as Content-Type, application/x-www-form-urlencoded.
- **Token Request Body:** Set as  
client\_id=<client\_id>&client\_secret=<client\_secret>&refresh\_token=<refresh\_token>&grant\_type=refresh\_token.
- **Access Token JSON Path:** Set as \$.access\_token.
- **Access Token:** Leave this field blank.

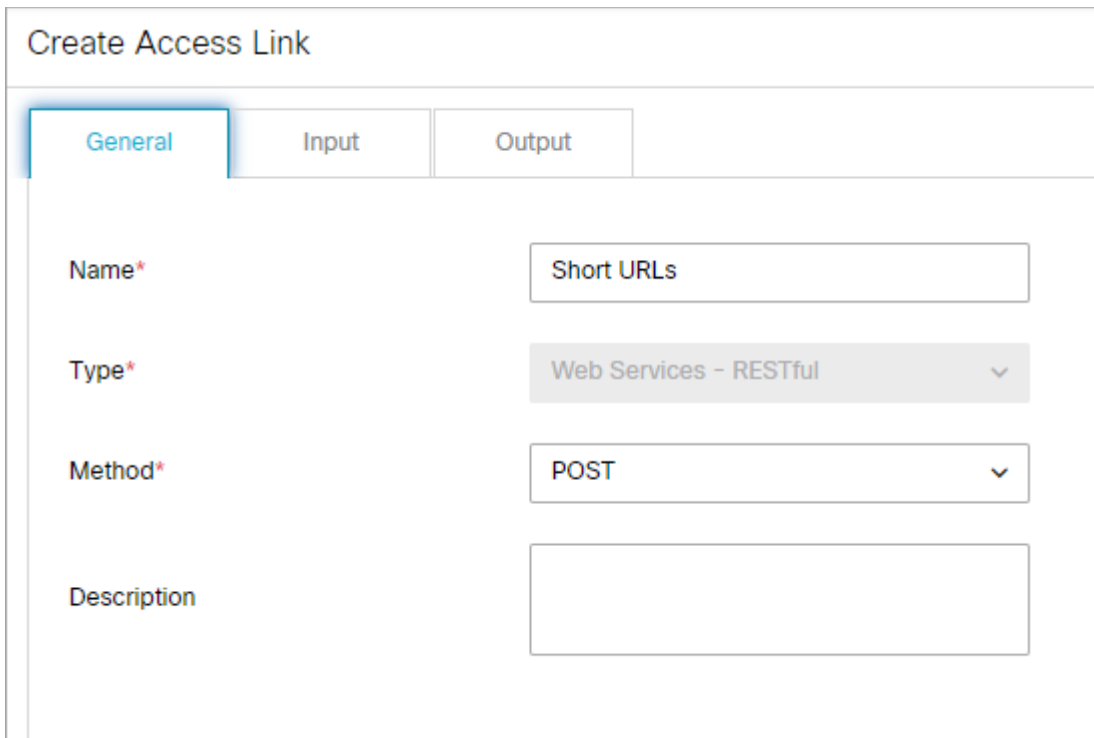
6. Click the **Save** button.

## Create the Access Link

---

To create a link:

1. In the department-level Top Menu, click the **Data Adapters** option.
2. In the Left menu, navigate to **Access Links**.
3. Click the **New** button
4. Select the General tab and provide the following details.
  - **Name:** Type the name as *Short URLs*.
  - **Type:** Type is set to **Web Services - RESTful** and cannot be changed.
  - **Method:** Set the method as **Post**.



The screenshot shows a form titled "Create Access Link" with three tabs: "General", "Input", and "Output". The "General" tab is selected and contains the following fields:

Name*	Short URLs
Type*	Web Services - RESTful
Method*	POST
Description	

5. Select the Input tab and provide the following details.

- **URL:** Type the URL `https://www.googleapis.com/urlshortener/v1/url`.
- **Authentication:** Select the OAuth authentication created for Short URL API.
- **Accept:** Set as **application/json**.
- **Content-type:** Set as **application/json**.
- **Body:** Set the body as `{"longUrl": "<%URL%>"}`  
The `<% URL%>` sets up the dynamic variable that needs a value every time this access link is executed.

Create Access Link

General

Input

Output

URL\*

Authentication\*

Accept\*

Content-Type\*

Body

Headers

Header Name		Header Value	
			+

Header Name	Header Value
No items to display in list.	

6. Select the Output tab, click the **New** button, and provide the following details.

- **Extract Or Filter:** Select **Extract**.
- **PATH:** Set as **\$.id**.
- **Internal Field Name:** Provide the name as **Short URL**.

Click the **Done** button to return to the Output Format page. In the Output Format JSON space, the value of the **Field Order** field is automatically updated as **1**.

Create Access Link

General Input **Output**

Output Format JSON

**New**

Extract Or Filter	Path	Internal Field Name	Field Order	Decoding
Extract	\$.id.	Short URL	<input type="text" value="1"/>	

7. Click the **Save** button.
8. Click the **Test** button. The Test Data Access Link window appears.
9. In the Test Data Access Link window, type any URL.
10. The Results tab then displays the shortened URL returned by the Google API.

# Calendars

- [About Business Calendars](#)
- [Managing Shift Labels](#)
- [Managing Day Labels](#)
- [Managing Business Calendars](#)
- [Deleting Business Calendars](#)

# 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.
- Reports: Calendars are used in reports. For example, reports like Email volume by queue, Email age by queue, and Email volume by alias.

It is not mandatory to set calendars. If not set, the system considers the agent's work time as 24\*7\*365.

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 and cases, and trigger alarms to alert supervisors. To create your business calendar, it is essential that you first create shifts and day labels.

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.

## Shift labels

---

A shift label describes the type of shift, and whether agents work in that shift or not. For example, you can create shift labels like:

- Morning shift and Evening shift, when agents work.
- Lunch break, Holidays, and Weekends, when agents do not work.

## Day labels

---

Day labels define the work time for each shift. Shift labels are used for creating day labels. For example, you can create day labels like:

- Weekday
  - 8 am to 12 pm: Morning shift
  - 12 pm to 1 pm: Lunch break
  - 1 pm to 5 pm: Evening shift
- Holiday
  - 12 am to 11.59 pm: Holiday

Use day labels to create calendars.

# Managing Shift Labels

---

## Creating Shift Labels

---

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

To create a shift label:

1. In the department-level Top Menu, click the **Business Rules** option.
2. In the Left menu, click **Business Calendars > Shifts**.
3. In the Shifts space, click the **New** button.

A maximum of 75 shift labels can be created in a department.

4. In the Create Shift space, provide the following details.

- **Name:** Type a name for the shift label.

Do not use comma (,) in the name of the shift label.

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

### Create Shift

Name*	<input type="text" value="Night Shift"/>
Description	<input type="text"/>
Agents work this shift	<input checked="" type="checkbox"/>

- **Agents work this shift:** Click the Toggle button if agents work in this shift or not. By default **Enabled** is selected. Select **No** if agents do not work in this shift.

5. Click the **Save** button.

## Deleting Shift Labels

---

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

### To delete a shift label:

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

## Managing Day Labels

---

Before you create day labels, ensure that you have first created the shift 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.

Before creating day labels, first create the shift labels.

### To create a day label:

1. In the department-level Top Menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Business Calendars > Days**.
3. In the Days space, click the **New** button.

A maximum of 75 day labels can be created in a department.

4. In the Create Day space, in the General tab, provide the following details.
  - **Name:** Type a name for the day label.

Do not use comma (,) in the name of the day label.

- **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.

Create Day

General Time

Name\* Weekday

Description Monday to Friday

Time Zone (GMT-05:00) Eastern Standard Time (...)

5. Go to the Time 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.

Create Day

General Time

Add Time

Start Time	End Time	Shift Label	Actions
08:30 am	01:30 pm	Morning Shift	...
01:31 pm	02:30 pm	Break	...
02:31 pm	06:30 pm	Morning Shift	...

Likewise, specify the start time, end time, and shift labels for the whole day. Click the **Add Time** button.

6. Click the **Save** button.

## Deleting Day Labels

---

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

To delete a day label:

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

## Managing Business Calendars

---

### Setting the Time Zone

---

Before you create a calendar, determine the time zone when your agents work. Make sure that you select the appropriate time zone in the department setting, 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).

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

To change the time zone setting:

1. In the department-level Top Menu, click the **Apps** option.
2. In the Left menu, navigate to **Settings**.
3. Select the Business calendar timezone setting. From the available time zones, select the time zone for your department.
4. 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.

You need to create day labels before creating calendars.

To create a calendar:

1. In the department-level Top Menu, click the **Business Rules** option.
2. In the left menu, navigate to **Business Calendars > Calendars**.

3. In the Calendars space, click the **New** button.

A maximum of 75 calendars can be created in a department.

4. In the Create Calendar space, in the General tab, provide the following details:

- **Name:** Type a name for the calendar.
- **Effective start date:** Select the date on which the calendar becomes active. Two calendars in a department cannot have overlapping dates. Also, the start date should be greater than the current date.
- **Effective end date:** Select the date on which the calendar becomes inactive. Two calendars in a department cannot have overlapping dates. Also, the end date should be greater than the start date. On the set end date, the calendar becomes inactive. Once a calendar becomes inactive, the system considers the agents work time as 24\*7\*365, unless some other calendar becomes active automatically.
- **Time Zone:** It shows the time zone selected for the department. This field is disabled. If you want to change the time zone for your department, you can do it by changing the Business calendar timezone setting.
- **Description:** Type a brief description.

### Create Calendar

- General
- Normal Week
- Exception Day

Name\*

Effective Start Date\*

Effective End Date\*

Time Zone

Description

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

### Create Calendar

General
Normal Week
Exception Day

Sunday*	Weekend <span style="float: right;">▼</span>
Monday*	Weekday <span style="float: right;">▼</span>
Tuesday*	Weekday <span style="float: right;">▼</span>
Wednesday*	Weekday <span style="float: right;">▼</span>
Thursday*	Weekday <span style="float: right;">▼</span>
Friday*	Weekday <span style="float: right;">▼</span>
Saturday*	Weekend <span style="float: right;">▼</span>

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

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

### Create Calendar

General
Normal Week
Exception Day

Add Exception Day


Date <span style="float: right;">⇅</span>	Day label <span style="float: right;">⇅</span>	Actions <span style="float: right;">⇅</span>
04/14/2021	Holiday	...
01/01/2022	Holiday	...

7. Click the **Save** button.

## Deleting Business Calendars

---

To delete a calendar:

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

# Codes & Classifications

- [About Classifications](#)
- [Creating Categories](#)
- [Deleting Categories](#)
- [Creating Resolution Codes](#)
- [Deleting Resolution Codes](#)
- [Creating Not Ready Reason Codes](#)
- [Enabling and Enforcing Not Ready Reason Codes](#)
- [Deleting Not Ready Reason Codes](#)
- [Creating Transfer Codes](#)
- [Deleting Transfer Codes](#)

# 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:

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

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

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

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

## 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.

## 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.

## 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 Categories

---

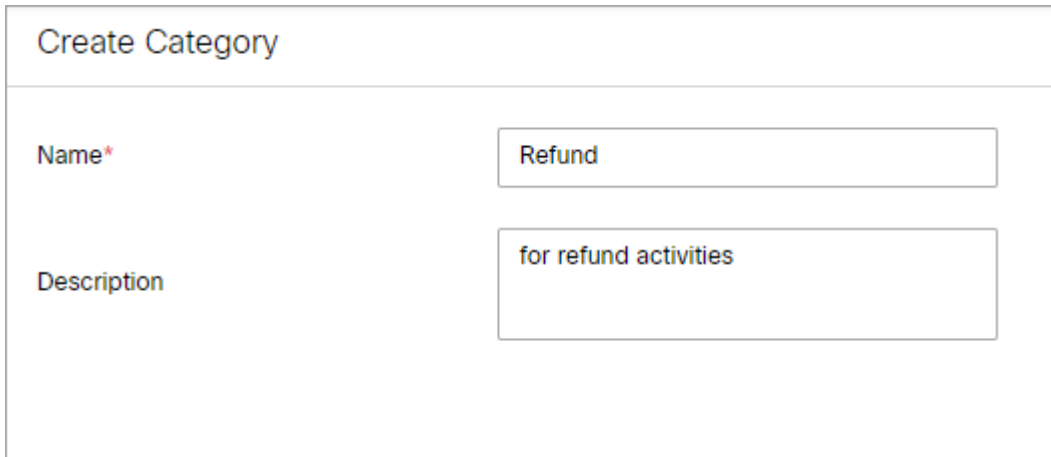
Categories and resolution codes can only be nested 3 levels deep.

To create a category:


1. In the department-level Top Menu, click the **Business Rules** option.

2. In the Left menu, navigate to **Codes and Classification > Categories**.
3. In the Categories space, click the **New** button.
4. In the Create Category space, provide the following details.

- **Name:** Type the name of the category.
- **Description:** Provide a brief description.




The screenshot shows a 'Create Category' form. The title 'Create Category' is at the top. Below it, there are two input fields. The first field is labeled 'Name\*' and contains the text 'Refund'. The second field is labeled 'Description' and contains the text 'for refund activities'.

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

## Deleting Categories

---

To delete a category:

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

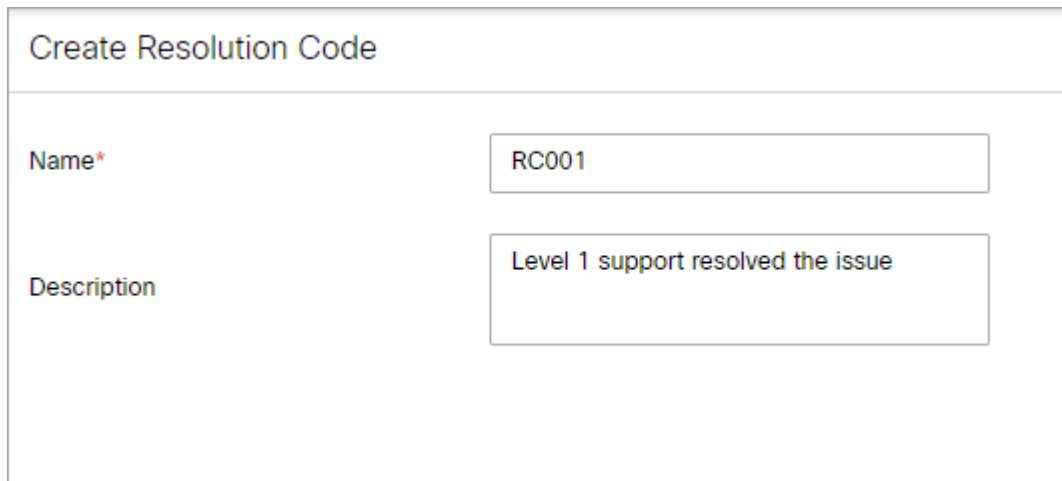
## Creating Resolution Codes

---


Resolution codes can only be nested 3 levels deep.

### To create a resolution code:

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




The screenshot shows a form titled "Create Resolution Code". It contains two input fields. The first field, labeled "Name\*", has the value "RC001". The second field, labeled "Description", has the value "Level 1 support resolved the issue".

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

## Deleting Resolution Codes

---

### To delete a resolution code:

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

## Creating Not Ready Reason Codes

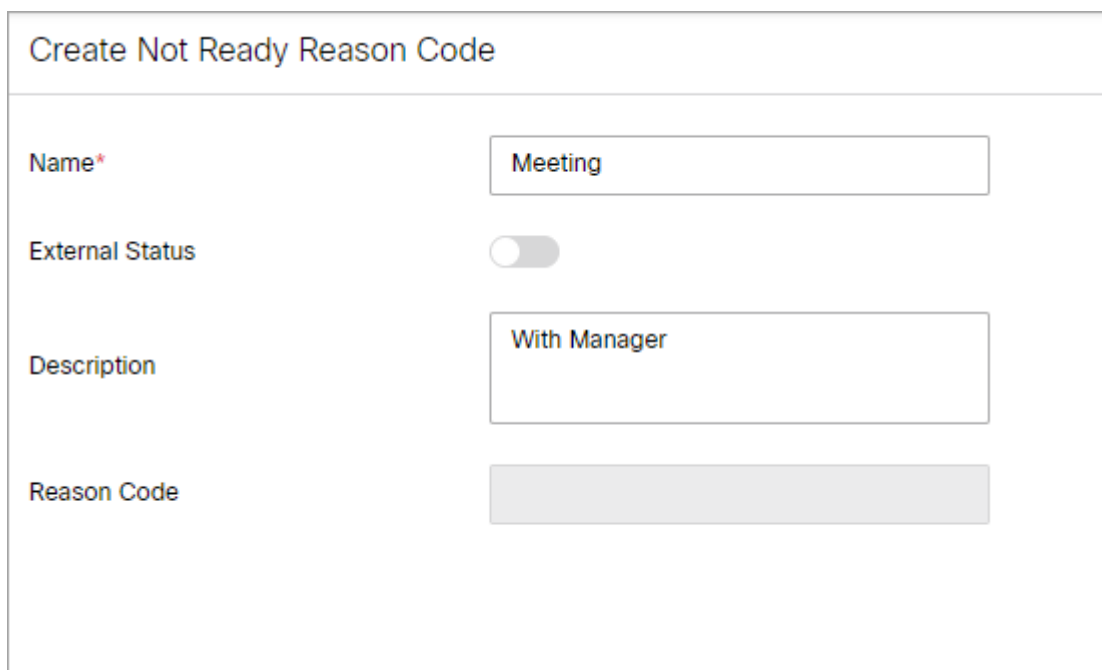
---

To create a not ready reason code:

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

A maximum of 75 not ready reason codes can be created in a department.

4. In the Create Not Ready Reason Code space, provide the following details:
  - **Name:** Type the name of the Not Ready Code.
  - **Description:** Provide a brief description.
  - **External Status:** Click the Toggle button if the code you are creating is external to the Unified CCE system. Do not click it otherwise.
  - **Reason Code:** Provide an external ID for the reason code to send to the Unified CCE system if it is an external code. The code must be an integer between 1 and 65535.



The screenshot shows a form titled "Create Not Ready Reason Code". It contains the following fields and values:

- Name\***: Meeting
- External Status**: A toggle switch is currently turned off.
- Description**: With Manager
- Reason Code**: (Empty field)

5. Click the **Save** button.

## Enabling and Enforcing Not Ready Reason Codes

---

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

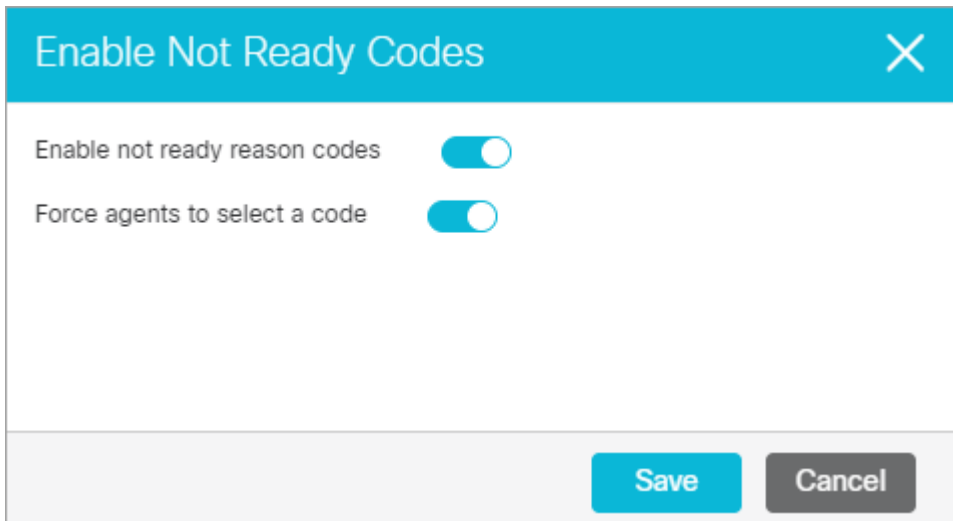
To enable not ready reason codes:

1. In the department-level Top Menu, click the **Business Rules** option.

2. In the Left menu, navigate to **Codes and Classification > Not Ready Reason Codes**.
3. In the Not Ready Codes space, click the **Enable Not Ready Codes** button.
4. In the Enable Not Ready Codes space, click the **Enable not ready reason codes** toggle button.
5. Click the **Save** button.

To enforce not ready reason codes:


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



## Deleting Not Ready Reason Codes

---

To delete a not ready reason code:

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

## Creating Transfer Codes

---

To create transfer codes:

1. In the department-level Top Menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Codes and Classification > Transfer Codes**.

3. In the Transfer Codes space, click the **New** button.

A maximum of 75 transfer codes can be created in a department.

4. In the Create Transfer Code space, provide the following:

- **Name:** The name of the transfer code.
- **Description:** A brief description of the transfer code.

Create Transfer Code

Name\*


Description

5. Click the **Save** button.

## Deleting Transfer Codes

---

To delete transfer codes:

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

# Macros

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

## About Macros

---

Macros are commands that fetch stored content. They are easy to use and display their contents, 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:

- **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.
- **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 department-level Top Menu, click the **Business Rules** option.
2. In the Left menu, navigate to **Macros > Business Object**.
3. In the Business Object Macro space, click the dropdown menu to select the type of macro.
4. Click the **New** button.
5. In the Create Business Object space, provide the following details.
  - **Name:** Type a name for the macro.
  - **Definition:** Click the dropdown menu and select the attribute that defines this macro. Please note that for any date attributes (for example, case creation date) are displayed in the GMT timezone.
  - **Description:** Provide a brief description.
  - **Default Value:** Provide the default value for the macro.

### Create Business Object


Name*	<input type="text" value="contact_person_id"/>
Definition*	<input type="text" value="contact_person_id"/> ▼
Description	<input type="text" value="Unique ID for the contact person"/>
Default Value	<input type="text"/>
Exception Article	<input type="text"/> 

6. Click the **Save** button.

## Creating Combination Macros

---

To create a combination macro:

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

### Create Combination

**Name\***

**Description**

**Default Value**

**Exception Article**  +

**Definition\***

Name
user_salutation
user_first_name
user_last_name
user_middle_name


5. Click the **Save** button.

## Deleting Macros

---

Macros used in workflows cannot be deleted.

To delete a macro:

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

# Dictionaries

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

# Setting Language Options for the User Interface

---

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

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

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

## To set the language for the user interface:

1. In the partition-level Top Menu, click the **Language Tools** option.
2. In the Left menu, click **Login Page**.
3. In the Login Page space, click the checkbox next to the language you want to enable on the login page. If you want the users to be able to view the UI in multiple languages, then select the language packs to be made available to the users. When more than one language pack is selected, then a new **Language** option shows on the login page. At the time of login, the user can select the language in which he wants to see the UI.
4. If you wish to set the language to the primary language that the application shows on the login page, click the **Set Primary** link in the Actions column for the language.

The screenshot shows the 'Language Tools' configuration page in the Cisco Enterprise Chat and Email interface. The page is titled 'Enterprise Chat and Email' and shows the user 'Partition Administrator'. The 'Language Tools' tab is active, and the 'Language Pack' section is expanded. The table below lists the available language packs, with 'English' selected and marked as the primary language.

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

5. Click the **Save** button.

## About Dictionaries

Dictionaries refer to a list of words stored in the system for reference. Agents use dictionaries to check spellings in outgoing emails.

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

Each department comes with predefined dictionaries and one of them is configured as the default dictionary. A department can have only one default dictionary and it can be changed according to the business requirements.

The dictionaries available in the system are:

1. Brazilian Portuguese Dictionary
2. Danish Dictionary
3. Dutch Dictionary
4. English (UK) Dictionary
5. English (US) Dictionary
6. Finnish Dictionary
7. French Dictionary

8. German Dictionary
9. Italian Dictionary
10. Norwegian (Bokmaal) Dictionary
11. Portuguese Dictionary
12. Spanish Dictionary
13. Swedish Dictionary

## Creating Dictionaries

---

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

To create a new dictionary:

1. In the department-level Top Menu, click the **Language Tools** option.
2. In the Left menu, click **Dictionaries**.
3. In the Dictionaries space, click the **New** button.

A maximum of 25 dictionaries can be created in a department.

4. In the Create Dictionary space, on the General tab, provide the following details.
  - **Name:** Provide the name of the dictionary.
  - **Language:** From the drop down list, select a language for the dictionary.
  - **Description:** Provide a brief description.
  - **Default Language:** Click the Toggle button to make this dictionary as the default dictionary of the department.

### Create Dictionary

- General
- Suggested
- Approved
- Blocked

Name\*

Language\*

Description

Default Language

5. Click the **Save** button.

## Choosing a Default Dictionary

---

To choose a default dictionary:


1. In the department-level Top Menu, click the **Language Tools** option.
2. In the Left menu, click **Dictionaries**.
3. In the Dictionaries space, click the **Set as Default** option in the actions column corresponding to the desired dictionary to set it as the default dictionary for the department.

## Deleting Dictionaries

---

The 13 predefined dictionaries provided in the system cannot be deleted.

To delete a dictionary:

1. In the department-level Top Menu, click the **Language Tools** option.
2. In the Left menu, navigate to **Dictionaries**.
3. In the Dictionaries workspace, hover your mouse over the dictionary you wish to remove and click the **Delete**  button.
4. Click the **Yes** button when the system prompts you to confirm the deletion.

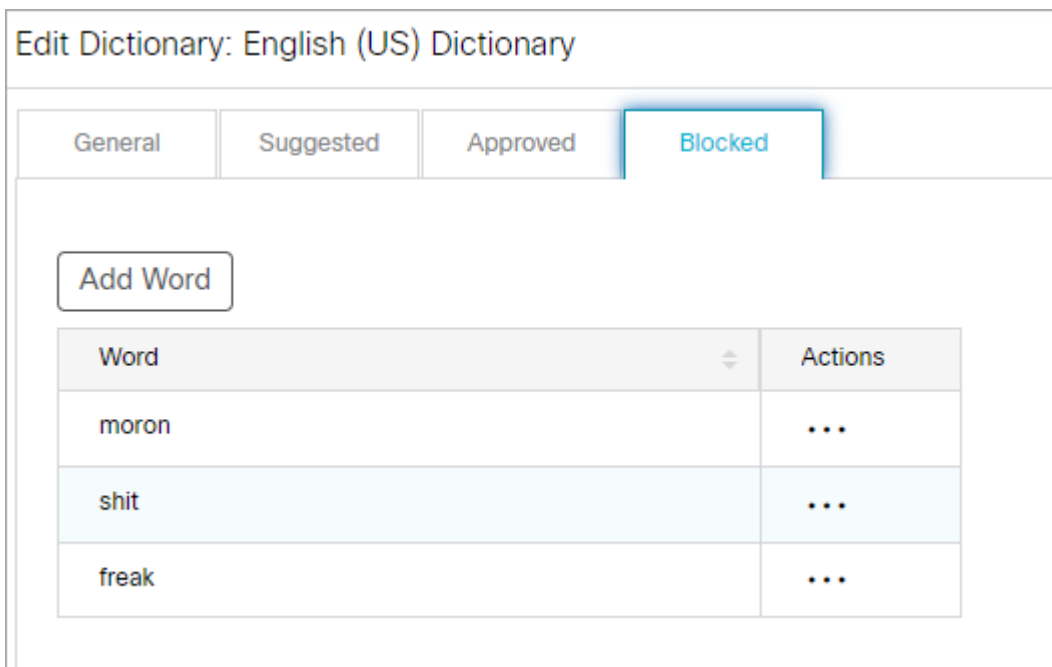
## Viewing and Adding Blocked Words


---

You can create a list of blocked words that users should not be allowed to use in emails, chats, and so on. Any word that is included in this list is blocked, 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 department-level Top Menu, click the **Language Tools** option.
2. In the Left menu, click **Dictionaries**.
3. In the Dictionaries space, select a dictionary to edit.
4. In the Edit Dictionary space, on the Blocked tab, view the list of blocked words. To add new words to the list of blocked words, click the **Add Word** button, and type the word into the Add Word field. Click **Done**.



5. If you want to delete a blocked word, under the **Actions** column, click the **Options**  button. Select **Delete** from the menu.
6. A message appears asking to confirm the decision. Click **Yes** to delete the blocked word.
7. Click the **Save** button.

## Approving and Rejecting Suggested Words

---

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

### To approve suggested words:

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

The screenshot shows the 'Edit Dictionary: English (US) Dictionary' interface. It has four tabs: 'General', 'Suggested', 'Approved', and 'Blocked'. The 'Suggested' tab is active. In the top right corner, there are two buttons: 'Reject' (red) and 'Approve' (green). Below these is a table with two columns: 'Words' and 'Suggested By'. The table contains three rows of data:

<input type="checkbox"/> Words	Suggested By
<input type="checkbox"/> moro	santosh7
<input checked="" type="checkbox"/> pdf	santosh7
<input checked="" type="checkbox"/> eightbank	santosh7

5. Click the **Save** button.

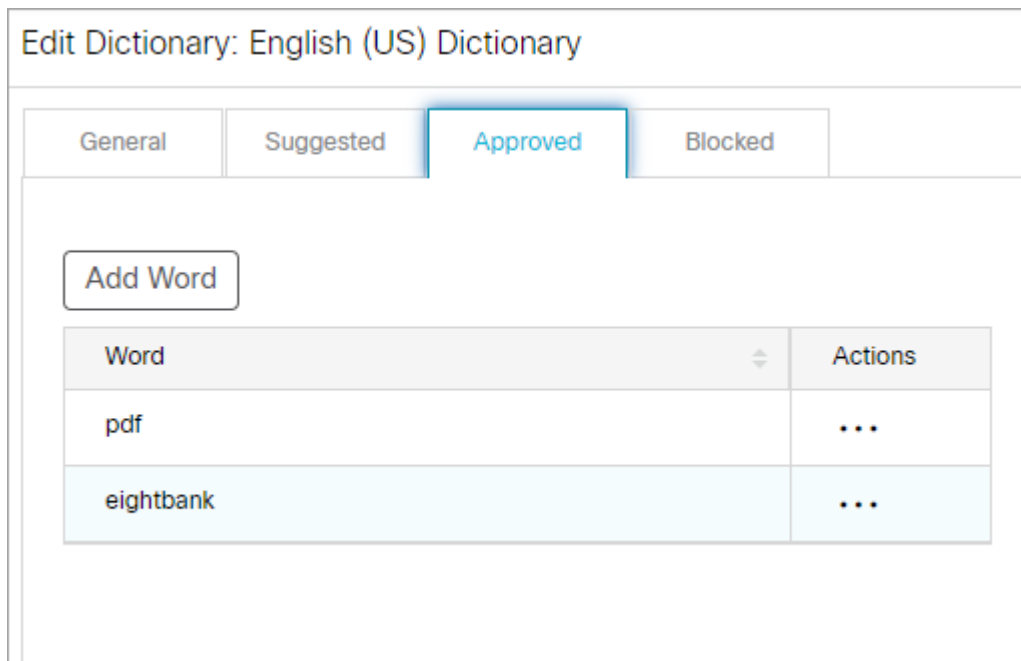
## Viewing and Adding Approved Words


---

You can create a list of approved words that users should be allowed to use in emails and chats without being flagged by the spell checker or any auto-corrected search tools.

### To add approved words:

1. In the department-level Top Menu, click the **Language Tools** option.
2. In the Left menu, click **Dictionaries**.
3. In the Dictionaries space, select a dictionary to edit.
4. In the Edit Dictionary space, on the Approved tab, view the list of approved words.



5. To manually add Approved words to a dictionary, click the **Add Word** button, and type the word into the Add Word field. Click **Done**.
6. If you want to delete a blocked word, under the **Actions** column, click the **Options**  button. Select **Delete** from the menu.
7. Click the **Save** button.

## Choosing a Default Dictionary

---

To choose a default dictionary:

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

Enterprise Chat and Email Partition Administrator

Service Apps Business Rules Data Adapters Language Tools Tools User

New

Dictionaries	Name	Language	Actions
Settings	Brazilian Portuguese Dictionary	Portuguese (Brazilian)	<a href="#">Set as Default</a>
	Danish Dictionary	Danish	<a href="#">Set as Default</a>
	Dutch Dictionary	Dutch	<a href="#">Set as Default</a>
	English (UK) Dictionary	English (UK)	<a href="#">Set as Default</a>
	English (US) Dictionary	English (US)	<b>Default</b>
	Finnish Dictionary	Finnish	<a href="#">Set as Default</a>
	French Dictionary	French	<a href="#">Set as Default</a>
	German Dictionary	German	<a href="#">Set as Default</a>
	Italian Dictionary	Italian	<a href="#">Set as Default</a>
	Norwegian (Bokmaal) Dictionary	Norwegian (Bokmal)	<a href="#">Set as Default</a>
	Portuguese Dictionary	Portuguese	<a href="#">Set as Default</a>
	Spanish Dictionary	Spanish	<a href="#">Set as Default</a>
	Swedish Dictionary	Swedish	<a href="#">Set as Default</a>

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

# Supervision Monitors

- [About Supervision Monitors](#)
- [Queue Attributes](#)
- [User Group Attributes](#)
- [User Attributes](#)
- [Creating Supervision Monitors](#)
- [Starting Monitors](#)
- [Deleting Supervision Monitors](#)

## About Supervision Monitors

---

A monitor provides various perspectives on the information it tracks by presenting it in the form of tables, as well as pie and bar charts. For each business object, (users, user groups, and queues) users can select a number of attributes for monitoring. Monitors display real-time information, which is automatically refreshed every 30 seconds. Monitors created from the Administration Console can also be viewed from the Agent Console as a supervisor.

The monitors enable users to observe the functioning of three types of business objects in the system:

- Queues
- User groups
- Users

While setting up a monitor users can:

- Configure it to run automatically, manually, or automatically whenever you are logged in to the system.
- Select the objects and their attributes that you want monitored.
- Create messages and alerts that are sent to specified recipients when certain conditions are met.

### Settings to View Bar Charts

---

Users can view information in the form of bar charts. Bar charts for queues, user groups and users are only available when certain attributes are selected for monitoring while [creating a monitor](#). The following table shows which attribute needs to be selected for each business object to view information in the form of bar charts.

Attribute	Attribute Definition
Queues	<ul style="list-style-type: none"><li>▪ Queue name</li><li>▪ Users - Number logged in</li><li>▪ Email - Service level</li><li>▪ Email - Oldest not started</li></ul>
User Groups	<ul style="list-style-type: none"><li>▪ Email - Number of users available</li></ul>
Users	<ul style="list-style-type: none"><li>▪ User name</li><li>▪ Email - Available to handle</li><li>▪ Email - Number in progress</li><li>▪ Email - Number not started</li></ul>

# Queue Attributes

---

## General Attributes

---

- **Queue ID:** The unique ID assigned to the queue, usually a number.
- **Queue name:** Name of the queue.
- **Queue status:** Status of the queue. The status of the queue can be Active or Inactive.
- **Users - Number logged in:** Number of agents who are currently logged into the application and can be assigned activities from the queue. These are the agents who have pull permission on the queue and agents to whom email activities can be assigned or transferred from the queue.

## Chat Activity Attributes

---

- **Chat - Current service level (%):** Number of serviced sessions currently in progress, which were picked up before the threshold setting configured for the department / Total number of serviced sessions currently in progress \* 100.
- **Chat - Daily service level (%):** Chats answered before service level setting / sample set of chats completed on the day, till that point of time \* 100.
- **Chat - Number in progress:** Number of chat activities assigned to agents and are being worked on (Status: Assigned- In Progress).
- **Chat - Number not started:** Number of chat activities assigned to agents, but on which work has not yet started (Status: Assigned - New).
- **Chat - Number of agents available:** Number of agents who are logged in and 'Available', who can either be assigned chat activities from the queue or can pull activities from the queue, and whose Chat - User max load setting is not exceeded.
- **Chat - Number unassigned:** Number of unassigned chat activities in the queue (Status: Assignment - Ready for Internal assignment).
- **Chat - Oldest in progress:** Age of the oldest chat activity in the queue - where the activity has been assigned and been worked upon (activity status 'Assigned-In Progress'). If your calendar is set in business hours it does not affect this column.
- **Chat - Oldest unassigned:** Age of the oldest chat activity in the queue, where the activity has not been assigned (activity status 'Assignment-Ready for Internal assignment') If your calendar is set in business hours it does not affect this column.
- **Chat - Oldest not started:** Age of the oldest chat activity in the queue, where the activity has been assigned but has not been worked on (Status: 'Assigned-New'). If your calendar is set in business hours it does not affect this column.
- **Chat - Queue Priority:** The priority level of a queue. Activities that come in from high-level customers can be assigned to high-priority queues. The priority levels range from 1 to 9, with 1 being the most urgent level of priority, and 9 being the lowest level of priority.

## Email Activity Attributes

---

- **Email - Number in progress:** Number of email activities assigned to agents and being worked on (Status: Assigned- In Progress).
- **Email - Number in wrapup:** Number of email activities assigned to agents and being wrapped up (Status: Assigned- Wrap Up).
- **Email - Number not started:** Number of email activities assigned to agents, but on which work has not yet started (Status: Assigned - New).
- **Email - Number unassigned:** Number of unassigned email activities in the queue. (Status: Assigned - Ready for Internal assignment)
- **Email - Oldest not started [hh:mm]:** Age of the oldest email activity in the queue, where the activity has been assigned but has not been worked on (Status: Assigned - New). Age = Current date - created on date.

Age is not calculated in business hours.

- **Email - Service Level:** This is calculated by using two configured items: sample size and response time limit. It indicates the percentage of emails for which response was sent before the time limit elapsed. (This does not include auto-acknowledgments).

## User Group Attributes

---

### General Attributes

---

- **User group name:** Name of the user group.
- **User group ID:** The unique ID assigned to the user group, usually a number.

### Chat Activity Attributes

---

- **Chat - Assigned and in progress:** Number of chat activities assigned to the agents of the group and which are being worked on (Status: Assigned - In progress).
- **Chat - Assigned but not started:** Number of chat activities assigned to the agents of the group, but on which work has not yet started (Status: Assigned - New).
- **Chat - Available agents:** Number of agents logged in and available to handle chats.

## Email Activity Attributes

---

- **Email - Assigned and in progress:** Number of email activities assigned to the agents in the group and being worked on (status as assigned; substatus as in progress).
- **Email - Assigned but not started:** Number of email activities assigned to the agents in the group, but on which work has not yet started (status as assigned; substatus as not started).

- **Email - Assigned but pending:** Number of email activities assigned to the group, but on which work is pending (status as assigned; substatus as pending).
- **Email - Number of users available:** Number of group members logged in and available to handle emails.

## User Attributes

---

### General Attributes:

---

- **User name:** Name of the user.
- **User ID:** The unique ID assigned to the user, usually a number.
- **User status:** Status of the user, whether the user is logged in or not.
- **First Name:** First name of the user to be monitored.
- **Last Name:** Last name of the user to be monitored.
- **Screen Name:** Screen name of the user to be monitored.

### Chat Activity Attributes

---

- **Chat - Available to handle:** Is the agent available to handle chats: Yes or No. If the value is No, the Not Ready code the agent selected for the reason why he is unavailable is displayed.
- **Chat - Number in progress:** Number of chat activities assigned to agent and being worked on (Status: 'Assigned - In Progress').
- **Chat - Number not started:** Number of chat activities assigned to agents, but on which work has not yet started (Status: 'Assigned - New').
- **Chat - Oldest in progress:** Age of the oldest open chat activity assigned to the agent and been worked upon (activity status 'Assigned-In Progress') If your calendar is set in business hours it does not affect this column.
- **Chat - Oldest not started:** Age of the oldest open chat activity assigned to the agent but has not been worked on. (Status: 'Assigned-New') If your calendar is set in business hours it does not affect this column.
- **Unavailable chat reason:** Reason for why the agent is unavailable for chat activities.

### Email Activity Attributes

---

- **Email - Available to handle:** Is the agent available to handle emails: Yes or No. If the value is No, the Not Ready code the agent selected for the reason why he is unavailable is displayed.
- **Email - Number in progress:** Number of email activities assigned to this agent, which the agent is working on (Status: 'Assigned-In Progress').

- **Email - Number not started:** Number of email activities assigned to this agent, on which the agent has not yet started work (status: Assigned - New).
- **Email - Oldest in progress:** Age of the oldest email on which the agent is working (Status: Assigned-In Progress).
- **Email - Oldest not started:** Age of the oldest email on which the agent has not yet started work (Status: Assigned-New).
- **Unavailable email reason:** Reason for why the agent is unavailable for email activities.

## Creating Supervision Monitors

---

Supervision monitors can be created from different areas of the Administration Console depending on the type of monitor that is being created.

To create a monitor:

1. In the department-level Top Menu, click on one of the following:
  - **User**
  - **Business Rules**
2. From the Left menu, depending upon the previous selection, navigate to the **Users, User Groups** or **Queues**.
3. Click the **Monitor** button, corresponding to the space you have selected. The My Monitors window opens in a new tab.

For User Groups, Users and Queues the button changes to **Monitor User Groups, Monitor Users** and **Monitor Queues** respectively.

4. In the My Monitors window, click the **New** button. The window refreshes to the Create Monitor page.

A maximum of 100 monitors can be created in a department.

5. On the Create Monitor page, provide the following details.
  - **Name:** Type a name for the monitor. This is required information.
  - **Description:** Provide a brief description.
  - **Start type:** From the drop down list, select a start type for the monitor from the following options:
    - **Automatic:** The monitor runs automatically and if notification conditions are met, it sends alerts automatically at a fixed time interval, irrespective of whether the user who created the monitor is logged in or not.
    - **Manual:** The monitor has to be started manually by the user who created the monitor.
    - **On login:** The monitor starts automatically, once the user who created the monitor logs in. And if the notification conditions configured for the monitor are met, the alerts are sent automatically.

- **Object Selection section:** Select objects to be monitored. Select from users, user groups, and queues. Click the checkbox to make the selection. Once you are done selecting, click the **Next** button.

The **Next** button is enabled only after you provide the name for the monitor and select the objects to be monitored.

**Create Monitor** [Close]

Name\* Sample Monitor

Description

Start Type Manual

**Object Selection**

Queues  User Groups  Users

Filter Text:

Name

Default exception queue

Chat queue

**Email queue**

Call queue

**Selected**

**Queues**  
Email queue

Cancel Next Save

6. On the next page, in the Select Attributes section, select the attributes of the Users, User Groups and Queues to be monitored. For more details, see [Queue Attributes](#), [User Group Attributes](#), or [User Attributes](#). Click the **Next** button.

Some attributes are selected by default. They can be removed from the list if required.

Create Monitor
✕

### Select Attributes

▼ Type

- ▼  Queue
  - Chat - Current service level (%)
  - Chat - Daily service level (%)
  - Chat - Number in progress**
  - Chat - Number not started**
  - Chat - Number of agents available**
  - Chat - Number unassigned**
  - Chat - Oldest in progress [hhh:mm]
  - Chat - Oldest unassigned [hhh:mm]**
  - Chat - Oldest not started [hhh:mm]**
  - Chat - Queue priority
  - Email - Number in progress
  - Email - Number in wrapup
  - Email - Number not started
  - Email - Number unassigned
  - Email - Oldest not started [hhh:mm]

Move Up
Move Down

Type	Attribute Name
Queue	Queue Name
Queue	Chat - Number of agents available
Queue	Chat - Number in progress
Queue	Chat - Number not started
Queue	Chat - Oldest not started [hhh:mm]
Queue	Chat - Number unassigned
Queue	Chat - Oldest unassigned [hhh:mm]

Cancel
Back
Next
Save

7. On the next page, perform the following:

- In the Notification section, set the following:
  - **Enable Notification:** Click the checkbox to enable notifications
  - **Notification Frequency (Minutes):** Specify the time interval at which notifications should be sent when a condition specified in the monitor is met. The default value is set to 30 minutes.
- In the Conditions section, set the conditions for sending notifications.
  - Click the **Add New Criteria** button.
  - In the **Add New Criteria** window, specify conditions for raising alerts and sending notifications. Only objects and attributes that you have selected are displayed in the Type and Attribute field. Once you specify the condition, the Notification Type section is enabled.
- In the Notification Type section, perform the following:
  - Select the **Display toast notification** checkbox to configure the alert to be presented as a pop-up box on the monitor when an alert condition is met.
  - Set up internal messages or emails to be sent when an alert condition is met. Specify to whom you want to send the notifications, subject of the message and content of the message. You can send notifications to internal users and to external email addresses.

It is always a good practice to enable notification for monitors. However, you can create and save a monitor without setting it up.

Create Monitor
✕

### Notification

Enable notification

Notification Frequency (Minutes)\*

#### Conditions

+ Add New Criteria

Type	Attribute	Operator	Value	AND/OR	
Email queue	Chat - Number in ...	<	5	AND	✎ -

#### Notification Type

Display toast notification

Send message

To:

Subject:

Cancel
Back
Save

8. Click the **Save** button.

## Starting Monitors

You can configure the monitor to keep running automatically all the time, or you can configure them to run automatically every time you log in to the application. If you do not want to run the monitors automatically, start them manually whenever you need them.

To start a monitor:

1. In the department-level Top Menu, click on one of the following:
  - **User**
  - **Business Rules**
2. From the Left menu, depending upon the previous selection, navigate to the **Users, User Groups** or **Queues**.
3. Click the **Monitor** button, corresponding to the space you have selected. The **My Monitors** window opens in a new tab.

For User Groups, Users and Queues the button changes to **Monitor User Groups**, **Monitor Users** and **Monitor Queues** respectively.

4. In the My Monitors window, select the monitor you want to start.
5. Click the **Start** button. The window refreshes. The monitor appears in a new window. View the information in table or chart format or both. The display is refreshed after every 30 seconds.

# Deleting Supervision Monitors

---

To delete a monitor:

1. In the department-level Top Menu, click on one of the following:
  - **User**
  - **Business Rules**
2. From the Left menu, depending upon the previous selection, navigate to the **Users, User Groups** or **Queues**.
3. Click the **Monitor** button, corresponding to the space you have selected. The My Monitors window opens in a new tab.
4. In the **My Monitors** window, select the monitor you want to delete.
5. Click the **Delete** button.

# Storage

- [About Storage](#)
- [View Data Storage](#)
- [About Purge Jobs](#)
- [Planning Schedule of Purge Jobs](#)
- [Creating Purge Jobs](#)
- [Viewing Purge Job History](#)
- [Deleting Purge Jobs](#)

## About Storage

---

The Storage feature is used to see how much space is allocated for the data, current data usage, and to purge data of certain objects from the systems to free up the space. For more information on how to purge data, see [Creating Purge Jobs](#).

You can purge the data and view the data storage for the following objects:

- Email Attachments
- Email Content and Attachments
- Chat Attachments
- Chat Transcripts and Attachments
- Activity & Classification Events
- User Events

## Who Can Manage Storage?

---

Only partition users with the **Manage Data Storage** action can manage purge jobs. This action is part of the default partition administrator role.

## View Data Storage

---

Partition administrators can view total data store size in use and the amount of space used by objects from the Data Storage node under Storage.

To view data storage:

1. In the partition-level Top menu, click the **Storage** option.
2. In the Left menu, navigate to **Data Storage**.
3. From the list on the Data Storage space, you can view the following details:
  - **Current Usage:** Current data usage of an object.
  - **Usage on:** Data used on the date mentioned on the screen.
  - **Total Data Store Size:** Total size of the allocated space.

## About Purge Jobs

---

A purge job is a process that runs automatically at a scheduled time, and deletes the data of the selected object based on the specified criteria (such as, Email attachments for activities older than 90 days) from the database. The purge job deletes all the object's data that meet the criteria defined for the job. User can create multiple purge jobs, but two jobs cannot have overlapping schedules. A job runs only when it is in active state.

After creating a job, it runs automatically on the scheduled date and time. It cannot be started or stopped manually.

Purge job will permanently delete the data for the selected objects and it cannot be recovered.

## What Can You Purge?

---

- **Email Attachments:** All types of email attachment. This includes inline attachments.
- **Email Content and Attachments:** Email attachment and content of emails. Activity and case details associated with the email are not purged.
- **Chat Attachments:** All chat attachments.
- **Chat Transcripts and Attachments:** Chat attachment and transcript of chat. Activity and case details associated with the chat are not purged.
- **Activity & Classification Events:** Audit details of activities, cases, categories, and resolution codes. For categories and resolution codes, it only includes events for creating, modifying, deleting, and usage.
- **User Events:** Events for user login, logout, availability changes. This includes license consumption and license release events triggered at the time of login and logout.
- **Audit Data:** This includes all related audit events data related to administrator actions, activity and case audit actions (not including activity and case history), and auditable actions related to workflows. This also includes actions that involves creating, deleting, or changing or merging of customer data (customer data, contact data).
- **All:** All categories of data is purged.

## Planning 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 the following:

- 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 center 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 6 PM, 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 6 PM, and another from 6 PM to 8 PM on the same day.

# Creating Purge Jobs

To create a purge job:

1. In the partition-level Top menu, click the **Storage** option.
2. In the Left menu, navigate to **Purge Jobs**.
3. On the Purge Jobs space, click the **New** button.

A maximum of 25 purge jobs can be created in a partition.

4. In the Create Purge Jobs space, go to General tab and provide the following details:
  - **Name:** Type a name for the job.
  - **Description:** Provide a description for the job.
  - **Status:** Click the Toggle button. An alert message appears, read and click **Yes** to make the job active.

The screenshot shows the 'Create Purge Jobs' form with the 'General' tab selected. The form contains the following fields and controls:

- Name\*:** A text input field containing 'Chat transcripts and attachments.'
- Description:** A text input field containing 'Purge job for chat transcripts and attachments.'
- Status\*:** A toggle switch that is currently turned on (blue).

At the bottom right of the form, there are two buttons: 'Close' and 'Save'.

5. Go to the Options tab and provide the following details:
  - **Data to purge:** Set the value for data to purge.
    - a. Click the **Add** button.
    - b. From the Select Purge Objects window, select the data to purge from these available options: **Email Attachments, Email Content and Attachments, Chat Attachments, Chat Transcripts and Attachments, Activity & Classification Events, User Events, All**. For details, see [What Can You Purge?](#)
    - c. Click **Done**.

If a purge job is already created for an object, you cannot create another one for it. If create a purge job for **All** objects, you can not create a purge job for any other object.

- **Abort purge job if open activities match criteria:** Set this to **Yes** if you want the purge job to abort if any open email 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:** From the dropdown menu, either select **Number of days** or select **Specific Date**. Depending on what you select, the following fields are visible:
  - **Number of days:** Specify a number between 180 to 4000.
  - **Date:** Select a date. It must be at least 180 days before the current date.

Create Purge Jobs

General
Options
Schedule
History

Data to purge\*  +

Abort purge job if open activities match criteria\*  ▼

Data older than\*  ▼

Number of days\*

Close
Save

6. Go to the Schedule tab and give the following details:

- **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.

7. In the Set a duration for this schedule section, provide the following:

- **Start date:** Select a start date for the job schedule.
- **End date:** Select an end date for the job schedule.

8. Click the **Save** button.

Once a purge job is created, you cannot change the **Data to purge** option.

The history tab is enabled once a purge job is saved., but you cannot see any data in it until the job is completed. To know more about the History tab, see [Viewing Purge Job History](#).

## Viewing Purge Job History

Once a purge job is completed, you can view the history of jobs run from the History tab. It shows the following details:

- When the purge job started and ended.
- The amount of data purged and the number of attachments purged by the job.

When a job is running to purge all data, you can see the **Information** button in **Data Purged** column. When you click the **Information** button, you can see how many records are purged for each type of data.

- 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 when a job fails or gets aborted. It reflects the reason for a job failure and 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.

An email notification is also sent when a job is aborted.

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.

### To view purge job history:

1. In the partition-level Top menu, click the **Storage** option.
2. In the Left menu, navigate to **Purge Jobs**.
3. On the Purge Jobs space, select a job from the list.
4. Go to the History tab to view history for the selected purge job.

Edit Purge Jobs: Activity & Classification Events

General Options Schedule **History**

Task Start	Task End	Data Purged	Status	Additional Information
02/26/2021 6:26:27 ...	02/26/2021 6:26:28 ...	14 records have been delet...	Success	

Close Save

## Deleting Purge Jobs

### To delete a purge job:

1. In the partition-level Top menu, click the **Storage** option.
2. In the Left menu, navigate to **Purge Jobs**.
3. On the Purge Jobs space, hover your mouse over the job you want to delete and click the **Delete** button.
4. A message appears asking to confirm deletion. Click **Yes** to delete the purge job.

# System Resources

- [About Process Logs](#)
- [Processes Available in the System](#)
- [Managing Logging for Processes](#)

## About Process Logs

---

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

A list of these processes, along with the log file names, is displayed under **System Resources > Process Logs**. The level of logging can be changed and log messages can be filtered for a particular user. Also, a group of processes can be created and the messages all logged in a single log file to get a comprehensive view of a single functionality - for example, such as a single log file for email, which includes log messages for retriever, dispatcher, and workflow processes.

Messages are logged at eight trace levels and they are:

- **1 - Fatal:** The Fatal log level indicates critical failures that cause severe problems, often rendering the system or a major component inoperative. A fatal error signals the need for immediate action to restore functionality. This level is reserved for the most serious issues, such as:
  - Inability to connect to the database.
  - Major configuration failures (e.g., missing critical files preventing system initialization).
  - Unrecoverable errors in core system components.
  
- **2 - Error:** This level indicates a significant problem that is preventing certain functions or requests from completing successfully. Although the system can still operate, the issue recorded at this level represents a serious failure that may impact user experience or data integrity. Common causes for errors include:
  - Failed API requests.
  - Incomplete transactions.
  - Unhandled exceptions in the code.
  - File input/output errors.
  
- **3 - Warn:** The Warn level logs situations that do not prevent operations but suggest that something unusual or problematic may occur that might need attention. These warnings could evolve into errors or performance issues if, left unresolved. This level is used for:
  - Repetitive transient issues (e.g., connection retries).
  - API response times exceeding thresholds, without outright failure.
  
- **4 - Info:** This level logs informational messages that reflect the normal functioning of the system. It records significant system events, interactions with external services, and user actions that do not indicate any issues but are important for maintaining operational visibility. This level is used to:
  - Log successful operations (e.g., service start/stop events).
  - Track user logins and actions.

- Report interactions with external systems (e.g., messages sent/received from CTI, MR servers).
- **5 - Perf:** This level logs performance-related data, capturing key metrics such as the system's responsiveness, throughput, and resource utilization. These logs are essential for monitoring and optimizing system performance, especially under heavy load. This level helps to:
  - Capture response times for critical transactions
  - Measure the execution time of specific methods or module
- **6 - Dbquery:** This level logs operations related to the database, including executed queries and their parameters. These logs are useful for tracking database performance and debugging slow queries, as well as understanding how data is being accessed and manipulated. This level is particularly helpful for:
  - Logging executed SQL queries along with their parameters
  - Tracking query execution times
  - Monitoring database load and identifying performance bottlenecks
  - Detecting inefficient or failed queries.
- **7 - Debug:** The Debug level logs detailed information that helps understand the flow of code execution. Debug logs provide insight into system internals and are often used to diagnose issues, particularly those that are hard to reproduce. Debugging logs are beneficial for:
  - Tracking the flow through different methods or services.
  - Capturing variable values and state changes at various points in code execution.
  - Diagnosing complex issues like race conditions, where detailed timing and sequencing data are crucial.
  - Understanding complex logic or multi-step processes.
- **8 - Trace:** The Trace level logs the most detailed information about system execution, tracking every method and function call across the entire codebase. This level provides highly granular data and is typically enabled only during detailed performance analysis or when debugging complex issues. Trace logs are useful for:
  - Analyzing performance bottlenecks in detail, including the time spent in each method.
  - Tracing the precise flow of execution throughout the system.
  - Debugging complex performance or execution issues, particularly those spanning multiple modules or services.
  - Monitoring application hops (e.g., from the front-end to the back-end, or external services).

## Processes Available in the System

---

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

Note that if the system is associated with multiple servers, then each server will have its own set of process logs shown below:

#Component	Process Name	Log File Name
Component Status	<i>Server_Name</i> : component-status	eg_log_ <i>Server_Name</i> _component-status.log
Distributed Services Manager (DSM)	<i>Services_Server_Name</i> : DSMController	eg_log_ <i>Services_Server_Name</i> _DSMController.log
Distributed Services Manager (DSM)	<i>Services_Server_Name</i> : dsm-registry	eg_log_ <i>Services_Server_Name</i> _dsm-registry.log
Distributed Services Manager (DSM)	<i>Services_Server_Name</i> : DSMControllerLaunchHelper	eg_log_ <i>Services_Server_Name</i> _DSMControllerLaunchHelper
Monitor Process	<i>Services_Server_Name</i> : monitor-process	eg_log_ <i>Services_Server_Name</i> _monitor-process.log
Application Server	<i>Application_Server_Name</i> : Application Server	eg_log_ <i>Application_Server_Name</i> _ApplicationServer.log
Purge Process	<i>Services_Server_Name</i> : purge-process	eg_log_ <i>Services_Server_Name</i> _purge-process.log
Alarm Service Process	<i>Services_Server_Name</i> : alarm-rules-process	eg_log_ <i>Services_Server_Name</i> _alarm-rules-process.log
Activity Pushback Service Process	<i>Services_Server_Name</i> : auto-pushback-process	eg_log_ <i>Services_Server_Name</i> _auto-pushback-process.log
Dispatcher Service Process	<i>Services_Server_Name</i> : dx-process	eg_log_ <i>Services_Server_Name</i> _dx-process.log
Report Service Process	<i>Services_Server_Name</i> : report-process	eg_log_ <i>Services_Server_Name</i> _report-process.log
Workflow Cache Service Process	<i>Services_Server_Name</i> : rules-cache-process	eg_log_ <i>Services_Server_Name</i> _rules-cache-process.log
Workflow Engine Service Process	<i>Services_Server_Name</i> : rules-process	eg_log_ <i>Services_Server_Name</i> _rules-process.log
Retriever Service Process	<i>Services_Server_Name</i> : rx-process	eg_log_ <i>Services_Server_Name</i> _rx-process.log
Process Launcher	<i>Server_Name</i> : ProcessLauncher	eg_log_ <i>Server_Name</i> _ProcessLauncher.log
Messaging Server	<i>Messaging_Server_Name</i> : MessagingServer	eg_log_ <i>Messaging_Server_Name</i> _MessagingServer.log

#Component	Process Name	Log File Name
Scheduler Process	<i>Services_Server_Name</i> : scheduler-process	eg_log_ <i>Services_Server_Name</i> _scheduler-process.log
Webhook Process	<i>Services_Server_Name</i> : webhook-process	eg_log_ <i>Services_Server_Name</i> _webhook-process.log
Database Monitoring	<i>Services_Server_Name</i> : DatabaseMonitoring	eg_log_ <i>Services_Server_Name</i> _DatabaseMonitoring.log
EAAS Process	<i>Services_Server_Name</i> : EAAS-process	eg_log_ <i>Services_Server_Name</i> _EAAS-process.log
EAMS Process	<i>Services_Server_Name</i> : EAMS-process	eg_log_ <i>Services_Server_Name</i> _EAMS-process.log

## Managing Logging for Processes

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

The system changes to be made to the log trace levels for these processes and to create filters to enable logging for specific users. New process logs cannot be created and existing ones cannot be deleted.

All of the changes described in this section take effect immediately. No restart is necessary.

### Viewing Logging Details for Processes

Process Logs can either be viewed by the Partition Administrator or the System Administrator.

To view the properties of a process logger:

1. In the partition-level Top menu, click the **System Resources** option.
2. In the Left menu, navigate to **Process Logs**.
3. In the workspace, select a process log to view.
4. In the Edit Process Log space, on the General tab, the following details can be viewed for the selected process log:
  - **Name:** The name of the process log.
  - **Description:** The description of the process log.
  - **Maximum trace level:** The maximum level of logging done by the process log.
  - **Log file name:** The name of the log file in which the log messages are recorded.
  - **Maximum File Size:** The maximum size of the log file. The value is set to 5 MB.

### Edit Process Log: Ussuhvin0705:alarm-rules-process

- General
- Advanced Logging

Name	Ussuhvin0705:alarm-rules-process
Description	Ussuhvin0705:alarm-rules-process
Maximum Trace Level	2 - Error
Log File Name	eg_log_Ussuhvin0705_alarm-rules-p...
Maximum File Size	5MB
Extensive Logging Duration	
Extensive Logging End Time	

## Changing the Logging for Processes

You can use the Maximum Backups for Log Files setting to determine the maximum number of log file zips to be generated.

To change the logging for a process:

1. In the partition-level Top menu, click the **System Resources** option.
2. In the Left menu, navigate to **Process Logs**.
3. In the workspace, select a process log to view.
4. In the Edit Process Log space, on the General tab, set the value for the **Maximum Trace Level** field. For more information about what these fields mean, see [About Process Logs](#).

If Maximum trace level is set to 5-Perf, the messages with the following trace levels are logged:

- 1 - Fatal
- 2 - Error
- 3 - Warn

- 4 - Info
  - 5 - Perf
5. If 8-Debug or 7-Trace are selected, it is necessary to determine a time at which the logging should end at these levels. Once the logging ends, the maximum trace level is reset to the trace level that was set prior to the Debug or Trace level. In the Extensive logging duration field, select one of the following:
- 10 minutes
  - 30 minutes
  - 1 hour
  - 2 hours
  - 4 hours
  - 1 day
  - 2 days
  - 1 week
6. In the Edit Process Log space, on the Advanced Logging tab, click the **Toggle** button to enable advanced logging for a particular type. Advanced logging can be enabled for the following:
- **User**
  - **User Session**
  - **Package**
  - **Class**

Edit Process Log: Ussuhvin0705:alarm-rules-process

General **Advanced Logging**

---

User

Enable Advanced Logging

User IDs (comma separated)\*

Maximum Trace Level

Log File Name

Maximum Log File Size (KB)

Extensive Logging Duration

Extensive Logging End Time

---

User Session

Enable Advanced Logging

User Session IDs (comma separated)\*

Maximum Trace Level

Log File Name

7. Once advanced logging has been enabled for the desired type, set the following fields:
  - **User Session IDs:** This is required information
  - **Maximum trace level**
  - **Extensive logging duration:** If 8-Debug or 7-Trace are selected.
8. Click the **Save** button.

# Services

- [About Services](#)
- [About Service Processes](#)
- [Creating Service Processes](#)
- [Deleting Service Processes](#)
- [Starting Service Processes](#)
- [Stopping Service Processes](#)
- [Increasing the Number of Instances](#)
- [About Service Instances](#)
- [Creating Service Instances](#)
- [Starting Service Instances](#)
- [Stopping Service Instances](#)
- [Deleting Service Instances](#)
- [Adding Aliases to Retriever Instances](#)
- [Configuring EAAS Service Instance](#)
- [Configuring EAMS Service Instance](#)

## About Services

---

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

### Unified CCE

---

- **EAAS:** The external agent assignment service (EAAS) routes email, chat, callback, and delayed callback activities requests to Unified CCE. EAAS sends a request to Unified CCE for every activity that arrives into an external assignment queue, for the identification of an agent who is available to handle the given activity. If the EAAS service is not running, customers cannot start the chat, callback, and delayed callback sessions and the off hours page is displayed to them. This service can have only one process and instance and neither can be deleted.
- **EAMS:** The external agent message service (EAMS) initiates and maintains a reliable channel of communication with the Agent Peripheral Gateway (PG)/ARM interface of Unified CCE. Each instance of this service is dedicated to communicating with an Agent PG, and reports the current state of integrated agents and tasks to the appropriate Agent PG (i.e. the Agent PG to which the relevant agent belongs). These events are then used by Unified CCE for reporting purposes.

### Email Services

---

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

### General Services

---

- **Archive (Enterprise) service:** The application uses a partitioning feature provided by the databases to manage growth of high volume objects in the active databases. Partitions for each object are added regularly at different intervals and ensures that there are always additional partitions available. It is important that this service should be set to automatic start and it is running after the application restarts. This service is also responsible for calculating data storage usage at regular intervals. A notification email about the success or failure to add a new partition is sent to the email address specified in the partition level setting "To: address for notifications from services". In case of failure, the service attempts to resume at next interval until it succeeds.
- **Purge service:** This service is responsible for the data purge functions in the application and handling of data. This service checks for upcoming schedules of configured purge tasks as defined in the application at regular intervals and execute them within available time window. A notification about the failure of the purge task is sent to the email address specified in the partition level setting "To: address for notifications from services". Purge service reattempts the incomplete or failed task on next

schedule.

This service checks for upcoming schedules of configured purge tasks as defined in the application at regular intervals and executes them within available time window.

- **Reports service:** This service generates the reports, which are scheduled to run automatically or are run manually, and sends notifications to users, if they are configured. Notifications are sent for both scheduled and manually run reports. For running the scheduled reports, the Scheduler service should also be running. The reports service also needs to be running for using the print feature available in the various console.
- **Scheduler service:** This service schedules the messaging and reminder system.

## Workflow Services

---

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

## About Service Processes

---

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

For each service, a service process is provided in the system. In addition to these, new service processes can be created.

New service processes must be started before they can be used.

## Creating Service Processes

---

Before creating a service process, estimate your system requirements well. Depending on your needs, you can create the number and type of service processes you require. New service processes can be created for the following services:

- Email services: Dispatcher and Receiver
- Workflow services: Workflow Cache and Workflow Engine
- EAMS

## To create a service process:

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

A maximum of 100 service processes can be created in a partition.

5. In the Create Process space, under the General tab, provide the following details:
  - **Name:** Type a name for the process. This is required information.
  - **Maximum Number of Instances:** Type the maximum number of instances this service process can have. This option is available only for those services that can have more than one instance.
  - **Description:** Provide a brief description.
  - **Start type:** From the dropdown list, select a start type for the service process. The following options are available:
    - **Manual:** The service process has to be started manually by the system administrator.
    - **Automatic:** The service process is started automatically by the system when the application is started.

The image shows a 'Create Process' dialog box with the following fields and values:

- Name\***: Dispatcher2
- Maximum Number of Instances\***: 5
- Description**: (empty text box)
- Start Type\***: Automatic (dropdown menu)

Buttons: Close, Save

6. Click the **Save** button.

## Deleting Service Processes


---

Certain service processes that are not required in the system can be deleted. Before a service process can be deleted, its status must be set to **Stopped**. Additionally, not all service processes in the system can be deleted.

To delete a service process:

1. In the partition-level Top Menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to delete a process.
3. In the workspace dropdown, select the **Processes** option.

If the instance is running, stop the service process before deleting it


4. From the Actions column, click the **Options**  button and select the **Delete** option.
5. In the deletion prompt that appears, select **Yes**.

## Starting Service Processes

---

Unless a service process is configured to start automatically when a system is running, it must be manually started to use it. Instances for service processes whose Start Type is set to **Manual** need to be manually started each time they are used.

### To start a service process:

1. In the partition-level Top Menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to start a process.
3. In the workspace dropdown, select the **Processes** option.
4. From the Actions column, click the **Options**  button.
5. Select the **Start** option.


The service process state in the State column changes to **Running**.

## Stopping Service Processes

---

A service process can be stopped if it is not needed. This frees up system resources. Additionally, changing the properties for a particular service process, such as changing the maximum number of service instances, may require that the service process be stopped and then started again before the changes take effect.

### To stop a service process:

1. In the partition-level Top Menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to stop a process.
3. In the workspace dropdown, select the **Processes** option.
4. From the Actions column, click the **Options**  button.
5. Select the **Stop** option.

The process stops running.

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

## Increasing the Number of Instances

---

To help increase system performance, certain service processes are allowed to create more than one service instance. The following services can have more than one instance:

- Email services: Retriever and Dispatcher
- Workflow service: Workflow Engine
- EAMS

The maximum number of service instances that can be created for each of the above service processes can be changed as well.

#### To increase the number of instances for a service process:

1. In the partition-level Top Menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to increase the number of service instances.
3. In the workspace dropdown, select the **Processes** option.
4. In the Edit Process space, under the General tab go to the **Maximum number of instances** field.
5. Type the maximum number of instances this service process can have.
6. Click the **Save** button. An instruction prompt to restart the service process appears. Click **OK**.

Any changes made to the properties for a service process requires that the service process first be stopped and restarted before the changes take effect.

7. Return to the workspace and select the previously edited service process.
8. From the Actions column, click the **Options**  button and select the **Stop** option.  
The service process state in the State column changes to **Stopped**.
9. Once the service process has stopped, click the **Options**  button again and select the **Start** option.

The service process state in the State column changes to **Running**.

## About Service Instances

---

Service instances are derivatives of service processes. Configure service instances within the business partition to accomplish specific functions, such as reducing system load by allowing service processes to run at different times. Service instances can be set to start automatically, or can be started manually by the partition administrator or the system administrator.

For example, in an installation that is used to manage five different email aliases you could configure two service instances of the retriever service process and assign three aliases to one instance and two aliases to the other.

## Creating Service Instances

---

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

- Email services: Retriever and Dispatcher
- Workflow service: Workflow Cache and Workflow Engine
- EAMS

### To create a service instance:

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

A maximum of 25 service instances can be created in a partition.

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

Creating a new service instance requires an active service process to be selected in the Use Process field. Either the default service process can be used or a new one can be created.

### Create Instance

General


**Name\***

**Description**

**Start Type\***

**Use Process\***

Close
Save

6. For retriever service instances, there is an additional Input tab. Under the Input tab, click the **Search and Add**  button to select an available email alias and add it to the retriever instance. For details, see [Adding Aliases to Retriever Instances](#).
7. For the EAAS, there is an additional MR Connection port field. For details, see [Configuring EAAS Service Instance](#).
8. For the EAMS, the Agent PG field has to be configured. For details, see [Configuring EAMS Service Instance](#).
9. Click the **Save** button.

The number of instances for a given service should tally with the maximum number of instances defined for the service process in Shared Resources. For more details, refer to [Increasing the number of instances](#).

## Starting Service Instances

---


Unless a service instance is configured to start automatically, it must be manually started each time that particular service instance is used. Every time a service process is started, any manual instances associated with that service must be started as well.

### Important things to note:

- The retriever service instance can be started only after adding an alias to the instance. For details, see [Adding Aliases to Retriever Instances](#).
- When creating additional service instances for a particular service process, check to make sure that the service process allows for more than one service instance to be associated with it. For more details, see [Increasing the Number of Service Instances](#).

### To start a service instance:

More than one service instances can be started for Retriever, Dispatcher, Workflow Cache, Workflow Engine ad EAMS services.

1. In the partition-level Top Menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to start an instance.
3. In the workspace dropdown, select the **Instances** option.
4. From the Actions column, click the **Options**  button.
5. Select the **Start** option.


The instance starts running.

## Stopping Service Instances

---

Stop the service instance if it is not needed. This frees up the system resources. Sometimes you need to stop and start a service instance after making some changes in its properties. For example, when you add an alias to a retriever instance, you need to stop and start the retriever instance and all the dispatcher instances for that partition.

### To stop a service instance:

1. In the partition-level Top Menu, click the **Services** option.
2. In the Left menu, browse to the service for which you want to stop an instance.
3. In the workspace dropdown, select the **Instances** option.
4. From the Actions column, click the **Options**  button.
5. Select the **Stop** option.

The instance stops running.

## Deleting Service Instances

---


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

### To delete a service instance:

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

2. In the Left menu, browse to the service for which you want to delete an instance.
3. In the workspace dropdown, select the **Instances** option.

If the instance is running, select the service process and stop the service instance before deleting it.


4. From the Actions column, click the **Options**  button and select the **Delete** option.
5. In the deletion prompt that appears, select **Yes**.

## Adding Aliases to Retriever Instances

---

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

To add aliases to a retriever instance:

1. In the partition-level Top Menu, click the **Services** option.
2. In the Left menu, navigate to **Email > Retriever**.
3. In the workspace dropdown, select the **Instances** option.
4. Either create a [new instance](#) or select the Retriever instance you want to use and click the **Input** tab.
5. Under the Input tab, click the **Search and Add**  button to select an available email alias and add it to the retriever instance.
6. Click the **Save** button.

Stop and start the retriever instance. The retriever picks emails from the alias only after you restart the retriever instance.

## Configuring EAAS Service Instance

---

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

### Configuring the MR Connection Port for an EAAS Service Instance

---

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

The port number entered here should match the corresponding value that is entered at the time of setting up the Media Routing Peripheral Interface Manager (MR PIM) in Unified CCE. As a best practice, we recommend that you use a port number greater than 2000. This value should be set after starting ECE, and before starting the EAAS process and instance.

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

## Configuring Security Settings for an EAAS Service Instance

---

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

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

- **Generate a security certificate for the Media Routing servers** that will be used by the instance. A certificate for the primary media routing (MR) server is mandatory and a certificate for the secondary MR server is optional. These certificates are generated and can be obtained in the Cisco Unified CCE environment. For more information, consult your Cisco Unified CCE documentation.
- **Generate a private key in the ECE environment.** To generate a private key:
  - In the ECE environment, open command prompt (cmd.exe)
  - Go to the file location:  
`application_server\ECE_installation_directory\Java\jdk\jdk_version\bin`
  - You can generate either a RSA certificate or an ECDSA certificate. To generate a RSA certificate, execute the following command: `keytool -genkey -keyalg RSA -alias ecesaml -keystore ecesaml.jks`. To generate a ECDSA certificate, execute the following command: `keytool -genkeypair -alias alias_name -keyalg EC -keysize 256 -sigalg SHA256withECDSA -validity 365 -storetype JKS -keystore jks_name.jks`
  - Provide the necessary details for the security certificate.

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

If you are using a domain-signed certificate instead of a self-signed one, you must convert it to a .jks file.

To configure security settings for an EAAS service instance:

1. In the global-level Top Menu, click the **Services** option.
2. In the Left menu, navigate to **Unified CCE > EAAS**.
3. Select **Instances** from the dropdown and select the EAAS instance you wish to edit.
4. In the Edit space, under the General tab, provide the following
  - **Name:** Type a name for the instance. This is required information.
  - **Description:** Provide a brief description.
  - **Start type:** From the dropdown list, select a start type for the instance. The following two options are available.
    - **Manual:** The service instance has to be started manually by the system administrator.
    - **Automatic:** The service instance is started automatically by the system when the application is started.

- **MR Connection Port:** Provide the port number for the Media Routing Peripheral Gateway.
- **Allowed MR Servers:** With ECE 12.6 ES 8, users can specify the MR servers that can connect with the MR port. Only the servers listed here can establish a connection with the port. The values for this field can either be the hostname, FQDN, or IP address that can be resolved from the services server. The preferred values are the MR PIM servers for side A and side B.

If multiple values are provided for this field, they should be separated by commas. If this field is left empty, then there are no restrictions on MR servers connecting to the port.

For the updates to the Allowed MR Servers setting to take effect, [stop](#) and then [start](#) the EAAS instance.

- **Use Process:** Select the process to which the service instance is applied from the dropdown. This is automatically selected and cannot be changed.

The screenshot shows a configuration window with two tabs: 'General' and 'Security'. The 'Security' tab is active. The form contains the following fields:

- Name\***: EAAS-instance
- Description**: This instance connects to Unified CCE Media Routing PIM to make routing decisions for activities.
- Start Type\***: Automatic
- MR Connection Port**: 38005
- Allowed MR Servers**: pimA.egain.com, 10.32.85.112
- Use Process\***: EAAS-process

5. Click the **Security** tab and provide the following:

- **Enable Security:** Click the **Toggle** button to enable or disable the security configuration.
- **MR Certificate:** Provide the security certificate of the primary Media Routing server.
- **Secondary MR Certificate:** Provide the security certificate of the secondary Media Routing server.
- **Private Key:** Provide the following details from the private key file that was generated in the ECE environment:

- **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 application needs to access files secured by the instance.
- **Alias name:** The unique identifier for the decryption key.
- **Keystore password:** The password required for accessing the Java Keystore File.
- **Key password:** The password required for accessing the Alias' decryption key.
- **Public Key:** Provide the details to Private Key field generates a public key here. This certificate must be installed on the Unified CCE environment. For more information about installing the public key on the Unified CCE environment, consult your Cisco Unified CCE documentation.
- **Supported Cipher Suites:** Click the Search and Add button and select one or more strings of the desired cipher suit names, separated by colons. The suite names must be in TLS format. For more information about which cipher suite names are accepted, consult your Cisco Unified CCE documentation.

6. Click the **Save** button.

## Configuring EAMS Service Instance

---

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

### Configuring Peripheral Gateway and CTI Server Details

---

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

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

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

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

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

## Configuring Security Settings for an EAMS Service Instance

---

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

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

- **Generate a security certificate for the CTI servers** that will be used by the instance. A certificate for the primary CTI server is mandatory and a certificate for the secondary CTI server is optional. These certificates are generated and can be obtained in the Cisco Unified CCE environment. For more information, consult your Cisco Unified CCE documentation.
- **Generate a private key in the ECE environment.** To generate a private key:
  - In the ECE environment, open command prompt (cmd.exe)
  - Go to the file location:  
`application_server\ECE_installation_directory\Java\jdk\jdk_version\bin`
  - You can generate either a RSA certificate or an ECDSA certificate. To generate a RSA certificate, execute the following command: `keytool -genkey -keyalg RSA -alias ecesaml -keystore ecesaml.jks`. To generate a ECDSA certificate, execute the following command: `keytool -genkeypair -alias alias_name -keyalg EC -keysize 256 -sigalg SHA256withECDSA -validity 365 -storetype JKS -keystore jks_name.jks`
  - Provide the necessary details for the security certificate.

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

If you are using a domain-signed certificate instead of a self-signed one, you must convert it to a .jks file.

To configure security settings for an EAMS service instance:

1. In the global-level Top Menu, click the **Services** option.
2. In the Left menu, navigate to **Unified CCE > EAMS**.
3. Select Instances from the dropdown and select the EAMS instance you wish to edit.
4. In the Edit space, under the General tab, provide the necessary information from [Configuring EAMS Service Instance](#).
5. Click the **Security** tab and provide the following:
  - **Enable Security:** Click the Toggle button to enable or disable the security configuration.
  - **MR Certificate:** Provide the security certificate of the primary Media Routing server.
  - **Secondary MR Certificate:** Provide the security certificate of the secondary Media Routing server.
  - **Private Key:** Provide the following details from the private key file that was generated in the ECE environment:

- **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 application needs to access files secured by the instance.
  - **Alias name:** The unique identifier for the decryption key.
  - **Keystore password:** The password required for accessing the Java Keystore File.
  - **Key password:** The password required for accessing the Alias' decryption key.
  - **Public Key:** Provide the details to Private Key field generates a public key here. This certificate must be installed on the Unified CCE environment. For more information about installing the public key on the Unified CCE environment, consult your Cisco Unified CCE documentation.
  - **Supported Cipher Suites:** Click the Search and Add button and select one or more strings of the desired cipher suit names, separated by colons. The suite names must be in TLS format. For more information about which cipher suite names are accepted, consult your Cisco Unified CCE documentation.
6. After you have configured the required values and saved your changes, you can click the **Test** button to verify your settings are valid and secure.
  7. Click the **Save** button. You must restart the service process and instances after saving your changes.

# Partition Tools

- [About System Attributes](#)
- [Creating Custom Attributes](#)
- [Modifying System Attribute Settings](#)
- [Enabling Custom Attributes for Analytics](#)
- [About Utilities](#)
- [List User Sessions](#)
- [Terminate Sessions](#)

## About System Attributes

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

System Attributes	
Name	Description
Customer Data	Customer Data
Contact Person Data	Contact Person Data
Contact Person Custom Attributes	Contact Person Custom Attributes
Individual Customer Data	Individual Customer Data
Activity Data	Activity Data
Customer Search Data	Customer Search Data
Activity Search Data	Activity Search Data
Contact Person Search Data	Contact Person Search Data
Activity calltracking reply pane data	Activity calltracking reply pane data
Customer calltracking reply pane data	Customer calltracking reply pane data
Contact person calltracking reply pane data	Contact person calltracking reply pane data

## Creating Custom Attributes

Attributes can be added to the following business objects.

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

To create a custom attribute:

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

1. In the partition-level Top menu, click the **Tools** option.
2. In the Left menu, navigate to **System Attributes**.
3. In the System Attributes space, select an attribute.
4. In the Edit Attributes space, under the Custom Attribute tab, click the **New** button.
5. In the Create Attribute window, on the Basics page, provide the following:
  - **Name:** Type a name for the custom attribute. The following characters are not allowed in the name: ~ ! @ # \$ % ^ & \* ( ) \_ - + ? > < { } | [ ] = \ / , . (dot) ; " ' ' '. Also, the name cannot start with a digit.

- **Internal Name:** This field is disabled.
- **Data Type:** Select the type of data for the custom attribute. The options available are **String** and **Integer**.
- **Analytics:** This feature is not available for ECE at this time. Do not enable Analytics for custom attributes without consulting your Cisco Administrator.

The screenshot shows a 'Create Attribute' dialog box. The title bar is blue with the text 'Create Attribute' and a close button (X). Below the title bar is a section titled 'Basics'. There are four input fields: 'Name\*' with the value 'Charge', 'Internal name' (disabled), 'Data type' with a dropdown menu showing 'String', and 'Analytics' with a dropdown menu showing 'Do not enable'. At the bottom right, there are two buttons: 'Cancel' and 'Next'.

6. Click the **Next** button. On the Definition page, different options are available for the integer and string data type. Provide the following:
  - For Integer data type:
    - **Data Size:** The data size 9 is specified and it cannot be changed.
    - **Default Value:** Provide a default value for this field for the integer.
  - For String data type, provide the following details:
    - **Data size:** You can specify the maximum characters the custom attribute can have. The default value is 9. You can give a value between one and 4000. For example, if you give a value 10, then you cannot enter data exceeding 10 characters, in the custom field.
    - **String type:** This option gives you the flexibility to define how the data can be entered in the custom field. You have two options available:
      - **User specified in a text box:** You can provide an empty field where the user can type any data. You can also give a default value for the field.
      - **User-selected in the list of choice below:** Provide a list of possible values, from which the user can select one. You can specify an internal value and default value for the field. Provide these values, and click the **Toggle** button to make the

value selected by default and click the **Add** button to add it to the list. Multiple options can be added to the list and reordered.

Basics > Definition

Data Size\*

String Type

User specified in a text box

Default Value

User selected in the list of choices below

Internal value  Display value  Selected by Default  **Add**

Internal value	Display value	Selected by Default	Order
Ba	Check	<input type="checkbox"/>	<input type="text" value="1"/>

Allow multiple selections from the list

**Cancel** **Next**

7. Click the **Next** button. On the Translation page, you can define the display names and definitions for the attribute in other languages that are enabled for the partition.
  - In the Basics section, perform the following:
    - Click the **Toggle** button for Define display name of attribute in other languages field.
    - Enter a name into the field under the Display value column in relation to the desired language.
  - If you click the **User selected in the list of choices below** option when selecting the string type for the attribute's definition, the Definition section is available. In the Definition section, perform the following:
    - Click the **Toggle** button for Define display name of choices in other languages toggle.
    - Select a value from the **Choose list item** dropdown.
    - Enter a name into the field under the Display value column in relation to the desired language.

Create Attribute ✕

Basics > Definition > Translation

---

Basics

Define display name of attribute in other languages

---

Definition

Define display name of choices in other languages

Choose list item

Language	Display value
Czech	<input type="text" value="Check"/>
German	<input type="text" value="Check"/>
English	<input type="text" value="Check"/>
Polish	<input type="text" value="Check"/>

8. Click the **Finish** button.
9. The new attribute is listed under the Custom Attributes tab. In the table, you can modify the following fields:
  - **View:** Select this option if you want to show this attribute in the screens at the department level.
  - **Edit:** Select this option if you want to allow the agents to edit this field.
  - **Search:** Select this option if you want to make this attribute searchable. If you are adding this custom attribute to any of the search screens, make sure that this option is selected.
  - **Encrypt:** This option is enabled only if the data type selected is string.
10. Click the **Save** button.

When setting up custom attributes for call and chat, add them to the relevant callback and chat templates. For more information, see the 'Aria Chat Templates' and 'Callback Templates' section in *Enterprise Chat and Email Administrator's Guide to Chat and Collaboration Resources*.

## Modifying System Attributes

To modify system attributes:

1. In the partition-level Top menu, click the **Tools** option.
2. In the Left menu, navigate to **System Attributes**.
3. In the System Attributes space, select an attribute to modify.

- In the Edit Attributes space, click the checkboxes in the **View**, **Edit**, or **Encrypt** columns of the attributes.

Custom Attributes

New

Name	Internal name	Data type	Definition	<input type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input type="checkbox"/> Encrypt	Analytics	Actions
Name Ci...	name_ci...	Integer		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not ena...	...
state	state	String		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Not ena...	...
city code	city code	String		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Not ena...	...

Cancel Save

- In the Actions column, click the **Options** button and select **Edit** from the menu.
- In the Edit Attribute window click the **Next** button to move through sections. For more information, see [Creating Custom Attributes](#)
- Click the **Finish** button.

## Enabling Custom Attributes for Analytics

Analytics is not available for ECE at this time. Do not enable Analytics for custom attributes without consulting your Cisco systems administrator.

## About Utilities


These categories of tools are found in the Utilities section and are accessible at the Partition level. Utilities help administrators to diagnose and troubleshoot issues quickly and efficiently. A majority of these configurations are adjusted during the initial setup of the application and are not changed very frequently. The Partition Administrator user with the **Manage Application Security** action can use these utilities. This action is a part of default Partition Administrator role.

Utilities in the Administration Console have been broken down to the following sections:

- Admin Utilities
- Modifying Properties Utilities

### To access utilities:

- In the partition-level Top menu, click the **Tools** option.
- In the Left menu, navigate to **Utilities**.
- In the Utilities space, select a utility.

- From the **Actions** column, click the **Options**  button and select **Go** option to operate the utility.


## List User Sessions

---

This utility lists all the active sessions that are currently in progress on all application servers. The Partition Administrator user with the **Manage Application Security** action can use this utility. This action is a part of default Partition Administrator role. The main purpose of this utility is to see who is currently logged in and where they are logged in within the system, i.e. at the System or the Partition level. The information that is displayed cannot be changed. The user session information displayed includes:

- User Space
- User ID
- User Name
- User Type
- User Session ID
- Client IP
- Access Channel
- Session Creation Time (GMT)

### To use this utility:

- In the Utilities space, locate **List User Sessions**.
- From the Actions column, click the **Options**  button and select **Go**.
- 

From the Select filter field, provide either the **User ID** or the **User Name**.

List user sessions

User Session Information

Number of users logged into the system space: 0  
Number of users logged into the partition space: 1

Select filter  USER ID  USER NAME

USER SPACE	USER ID	USER NAME	USER TYPE	User Session ID	Client IP	ACCESS CHANNEL	SESSION CREATION TIME (GMT)
Partition	1	pa	Application User	D71d2ce0-Cf2...	10.10.57.63	Administration	2023-01-12 08:52:27.0

[Close](#)

# Terminate Sessions

This utility ends all active sessions of the user. The Partition Administrator user with the **Manage Application Security** action can use this utility. This action is a part of default Partition Administrator role. Sessions can be terminated by entering any of the following:

- User Session ID
- User ID
- X-egain-session
- Client IP

The User Session ID and User ID can be obtained from the **List User Sessions** utility.

To terminate sessions:

1. In the Utilities space, locate **Terminate Sessions**.
2. From the Actions column, click the **Options**  button and select **Go**.
3. On the Terminate Sessions page, enter either the User Session ID, User ID, X-egain-Session or Client IP and select one of the following options:
  - **Show Details:** This button shows the session details for the User Session ID or the User ID.
  - **Reset:** This button terminates all active sessions of the user.

### Terminate Sessions

This utility should be used to terminate sessions of user based on Session ID, User ID, X-egain-session or Client IP. You can get all the details from the 'List User sessions' utility

**IMPORTANT :** This utility will end all the active sessions of the user.

User Session ID:  **OR** User ID:  **OR**  
X-egain-session:  **OR** Client IP:

# Department Tools

- [About Screen Attribute Settings](#)
- [Modifying Screen Attribute Settings](#)
- [About User Attribute Settings](#)
- [Creating User Attribute settings](#)
- [Accessing Utilities](#)
- [Complete Activities](#)
- [Mask Content of Chat and Email Activities](#)

## About Screen Attributes

---

Screen Attributes allow you to enable, restrict, or reorder the attributes as they are displayed on a particular screen. Each department has its own set of screen attribute settings. Each screen has a number of attributes that cannot be removed.

For each department, you can customize the following screens:

- Agent Console - Information - Chat - Activity Details screen
- Agent Console - Inbox - Chat - Card - Additional Attributes
- Agent Console - Inbox - Mail - Card - Additional Attributes
- Agent Console - Inbox - My Monitor - Activity List screen
- Agent Console - Reply Pane - Call Track: General screen
- Administration Console - Workflows - Condition screen
- Administration Console - Workflows - Modify Object - True or False screen
- Agent Console - Information - Email Activity Details screen
- Agent Console - Customer - Contact Person Details screen
- Agent Console - Customer - Individual Customer Details screen
- Agent Console - Search - Activity - Advanced screen
- Agent Console - Search - Activity - Results screen
- Agent Console - Search - Contact Person - Advanced screen
- Agent Console - Search - Contact Person - Basic screen
- Agent Console - Search - Contact Person - Relationships screen
- Agent Console - Search - Contact Person - Results screen
- Agent Console - Search - Customer - Basic screen
- Agent Console - Search - Customer - Relationships screen
- Agent Console - Search - Customer - Results screen

Enterprise Chat and Email Partition Administrator


Service Apps Business Rules Data Adapters Language Tools Tools User

Items that contain... Items that contain...

Screen Attributes	Name	Description
User Attribute Setting	Agent Console - Information - Chat - Activity Details screen	Agent Console - Information - Chat - Activity Details screen
	Agent Console - Inbox - Chat - Card - Additional Attributes	Agent Console - Inbox - Chat - Card - Additional Attributes
	Agent Console - Inbox - Mail - Card - Additional Attributes	Agent Console - Inbox - Mail - Card - Additional Attributes
	Agent Console - Inbox - My Monitor - Activity List screen	Agent Console - Inbox - My Monitor - Activity List screen
	Agent Console - Reply Pane - Call Track:General screen	Agent Console - Reply Pane - Call Track:General screen
	Administration Console - Workflows - Condition screen	Administration Console - Workflows - Condition screen
	Administration Console - Workflows - Modify Object - True or F...	Administration Console - Workflows - Modify Object - True or F...
	Agent Console - Information - Email Activity Details screen	Agent Console - Information - Email Activity Details screen
	Agent Console - Customer - Contact Person Details screen	Agent Console - Customer - Contact Person Details screen
	Agent Console - Customer - Individual Customer Details screen	Agent Console - Customer - Individual Customer Details screen
	Agent Console - Search - Activity - Advanced screen	Agent Console - Search - Activity - Advanced screen
	Agent Console - Search - Activity - Results screen	Agent Console - Search - Activity - Results screen

## Modifying Screen Attributes

To modify screen attributes:

1. In the department-level Top menu, click the **Tools** option.
2. In the Left menu, navigate to **Screen Attributes**.
3. Select a screen to edit.
4. In the Edit Screen Attributes space, click the **Search and Add**  button and select attributes to add to the screen.

Before adding attributes to the search screens, make sure the attribute is searchable, as non-searchable attributes cannot be selected. For more details, see [Creating Custom Attributes](#).

5. In the Attributes section, from the Displayable column, click the **Toggle** button to specify if you want to display the attribute or not.
6. In the Order column, provide a numerical value for the order in which the attributes are displayed.

Edit Screen Attributes: Agent Console - Information - Chat - Activity  
Details screen

Attributes ↔ +

Display Na...	Displayable	Order	Object
Customer ...	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	chatses...
Entry point ...	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	chatses...
Host IP	<input checked="" type="checkbox"/>	<input type="text" value="3"/>	chatses...
Referrer na...	<input checked="" type="checkbox"/>	<input type="text" value="4"/>	chatses...
Referrer URL	<input checked="" type="checkbox"/>	<input type="text" value="5"/>	chatses...

Close Save

7. Click the **Save** button.

## About User Attribute Settings

---

These are department-specific settings. They let administrators restrict or allow a particular user to view or edit a particular attribute of a business object. Using this tool, administrators can control the level of access a user has in the system. Multiple user attribute settings can be created for various users depending on the expected level of their functioning. For example; a normal user in the system will not have the level of access similar to his supervisor.

Agents or supervisors can be assigned user attribute settings with different access levels determined in the system. Whenever a new user is created in the system, the administrator can assign one of the pre-determined user attribute settings to the user to function accordingly.

## Creating User Attribute Settings

---

To create user attribute settings:

1. In the department-level Top menu, click the **Tools** option.
2. In the Left menu, navigate to **User Attribute Setting**.
3. Click the **New** button.

4. In the Create User Attribute Setting space, on the General tab, set the following:

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

The screenshot shows the 'Create User Attribute Setting' form with the 'General' tab selected. The 'Name\*' field contains the text 'Agent Attribute Setting' and the 'Description' field contains 'An attribute setting for agents'.

5. Click the **Save** button.

6. In the Attributes tab, attributes for the objects are listed. Select the object and specify if you want to allow users to view, edit, or search the various attributes of the object.

The screenshot shows the 'Edit User Attribute Setting: Agent Attribute Setting' form with the 'Attributes' tab selected. On the left, a list of objects is shown with expandable arrows: 'Activity calltracking reply pane data', 'Activity Data', 'Activity Search Data', 'Contact person calltracking reply pane data', 'Contact Person Custom Attributes', 'Contact Person Data', 'Contact Person Search Data', 'Customer calltracking reply pane data', 'Customer Data', 'Customer Search Data', and 'Individual Customer Data'. On the right, there is a table with a header row containing 'Name', a dropdown arrow, and checkboxes for 'View' and 'Edit'. Below the header, the text 'No items to display in list.' is shown.


7. Click the **Save** button.

## Accessing Utilities

---

A department user with the **Manage Utilities** action can access utilities for the department. This action is a part of the default Administrator role.

### To access utilities:


1. In the department-level Top menu, click the **Tools** option.
2. In the Left menu, select the **Utilities** option.
3. In the Utilities space, select a utility.
4. From the Actions column, click the **Options**  button and select the **Run** option to operate the utility.

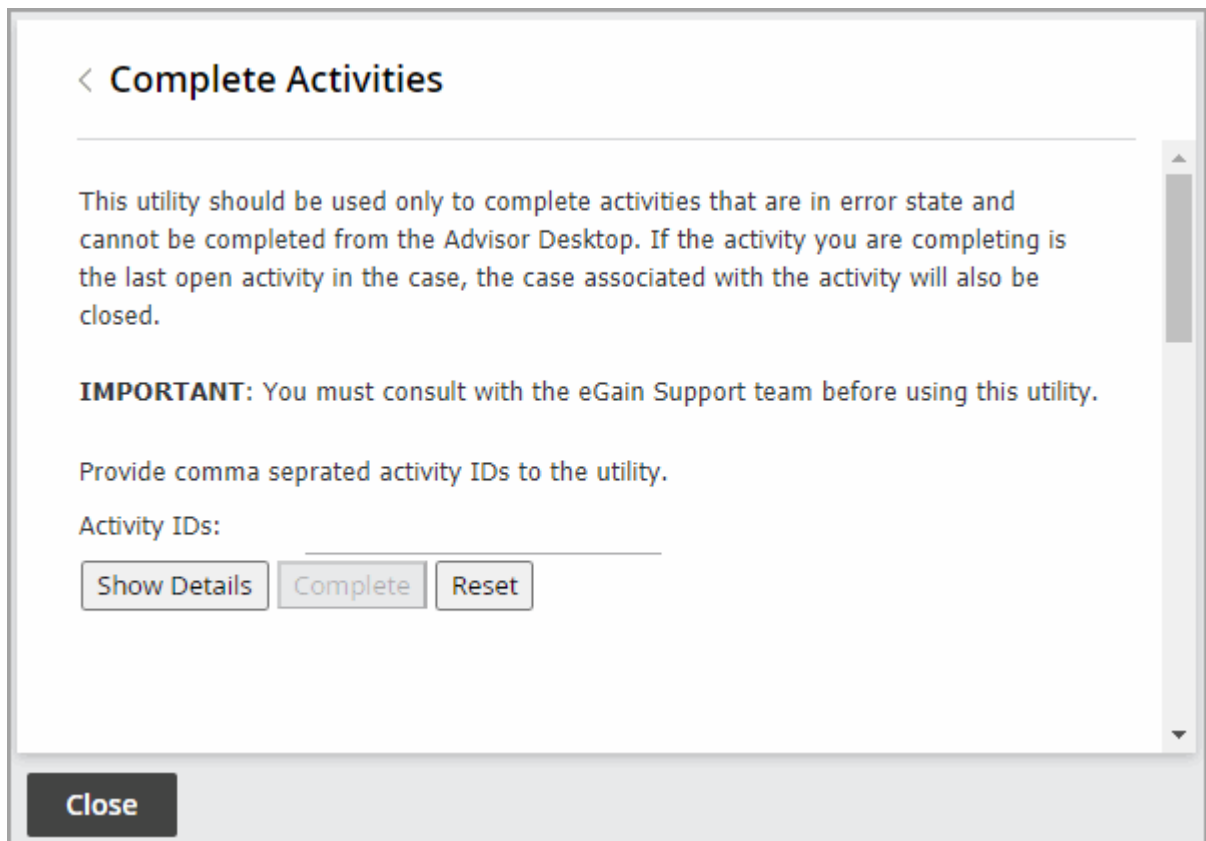
## Complete Activities

---

This utility is used to complete activities that are in error state and cannot be completed from the Agent Console. Using this utility ensures the graceful completion of an activity. If the activity that you complete using this utility is the last open activity in the case, then the case associated with the activity is also going to be closed. A department user with the **Manage Utilities** action can access this utility in the department. This action is a part of the default Administrator role.

### To use this utility:


1. In the Utilities space, locate **Complete Activities**.
2. From the Actions column, click the **Options**  button and select **Run**.
3. On the Complete Activities page, enter a value in the **Activity IDs** field and select one of the following options:
  - **Show Details:** This button shows the updated status for activities and associated cases.
  - **Complete:** This button completes the activities that are stuck in the Agent Console.
  - **Reset:** This button resets the values entered in the Activity IDs field.



## Mask Content of Chat and Email Activities

This utility masks email and chat activities that have already been completed. It is useful for troubleshooting masking of data for activities where the masking rules have not applied. The data masking rules that have been defined in the Administration Console are used to mask the content for these activities. For more information on data masking, see [About Data Masking](#). A department user with the **Manage Utilities** action can access this utility in the department. This action is a part of the default Administrator role.

To mask content of chat and email activities:

1. In the Utilities space, locate **Mask Content of Chat and Email Activities**.
2. From the Actions column, click the **Options**  button and select **Run**.
3. On the Mask Content of Chat and Email Activities page, provide the **Activity IDs** of the activities for which the content has to be masked.
4. Click the **Mask** button.

## < Mask Content of Chat and Email Activities

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
----	-------------	---------------	-----------------	--------	---------

Close

# Settings

- [About Settings](#)
- [Configuring Partition Settings](#)
- [Configuring Department Settings](#)
- [Editing User Setting Groups](#)
- [General Partition Settings](#)
- [General Department Settings](#)
- [Chat Settings](#)
- [Email Settings](#)
- [Knowledge Settings](#)
- [Language Settings](#)
- [Security 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 following four groups are available.

1. **Partition settings:** This group is available to administrators to control the resources at the partition level. These settings cannot be reset at lower levels.
2. **Department settings:** This group is available to administrators to control the resources at the department level. 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.

## Configuring Partition Settings

---

Configuring settings at the partition level affects all departments in the installation. Department-level settings can be changed here for all departments. To adjust settings for each individual department, navigate to the desired department and configure the settings there. For more information, see [Configuring Department Settings](#).

To configure partition settings:

1. In the global-level Top Menu, navigate to a section of the console that has settings you wish to adjust. You can navigate to one of the following:
  - **Chat and Messaging Settings:** Navigate to **Apps > Chat & Messaging > Settings**. For more information, see [Chat Settings](#).
  - **Email Settings:** Navigate to **Apps > Email > Settings**. For more information, see [Email Settings](#).
  - **General Partition Settings:** Navigate to **Apps > Settings**. For more information, see [General Partition Settings](#).
  - **Knowledge Settings:** Navigate to **Apps > Knowledge > Settings**. For more information, see [Knowledge Settings](#).
  - **CCE Integration Settings:** Navigate to **Integration > Settings**. For more information, see [CCE Integration Settings](#).
  - **Language Settings:** Navigate to **Language Tools > Settings**. For more information, see [Language Settings](#).
  - **Security Settings:** Navigate to **Security > Settings**. For more information, see [Security Settings](#).
2. In the settings workspace, navigate to the settings you wish to modify and make your changes.
3. Click the **Save** button.

## Configuring Department Settings

---

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

### Configuring Settings for a Department

---

To configure settings for a department:

1. In the department-level Top Menu, navigate to a section of the console that has settings you wish to adjust. You can navigate to one of the following:
  - **Chat and Messaging Settings:** Navigate to **Apps > Chat & Messaging > Settings**. For more information, see [Chat Settings](#).
  - **Email Settings:** Navigate to **Apps > Email > Settings**. For more information, see [Email Settings](#).
  - **General Department Settings:** Navigate to **Apps > Settings**. For more information, see [General Department Settings](#).
  - **Knowledge Settings:** Navigate to **Apps > Knowledge > Settings**. For more information, see [Knowledge Settings](#).
  - **Language Settings:** Navigate to **Language Tools > Settings**. For more information, see [Language Settings](#).
2. In the settings workspace, navigate to the settings you wish to modify and make your changes.
3. Click the **Save** button.

### Configuring Language Settings for a Department

---

To configure language settings for a department:

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

## Editing User Setting Groups

---

Administrators can allow a handful of department settings to be configured at the user level. These settings can be configured using the user settings group or the user preferences. In the user settings group the administrator can configure settings for a group of users within the same departments to have different values.

The user setting group is not the same as user group. A user can belong to multiple user groups but can belong to only one user settings group. The default setting group can be edited, but new setting groups cannot be created.

#### To edit a user setting group:

1. In the partition-level Top Menu, select the **User** option.
2. In the Left menu, navigate to **Setting Groups**.
3. In the **Edit Settings Group: Default User Setting Group** workspace, you can click the General, Attributes, and Relationship tabs.
4. In the General tab, you can edit the description of the group.
5. Next go to the Attributes tab to configure the values for the 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 users in the group, then in the **Editable at lower level** field click the checkbox to make the box empty and mark it as **Disabled**. Once it is set to **Disabled**, the value of the setting cannot be changed at the user level.
4. From the Relationships tab select users for the group, from the list of available users. Only the users who are not a part of any other user settings group are displayed.
5. Click the **Save** button.

## General Partition Settings

---

### Common Settings

---

#### To: Address for Notifications from Services

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

- **Access level:** Partition settings
- **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, and so on). Use this setting to specify the email address displayed in the "from" field of the notifications sent by the DSM.

- **Access level:** Partition settings

- **Default value:** —
- **Minimum value:** 0
- **Maximum value:** 255

## 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 deployment, make sure that you use a unique installation name for all your installations. This installation name is appended to the article IDs.

- **Access level:** Partition settings
- **Default value:** —
- **Minimum:** 0

## External URL of Application

In this setting, define the external-facing URL. This URL is used at the following places:

- URLs in reports notifications
  - Chat Entry Points
  - Single Sign-On Identity Provider configuration
- 
- **Access level:** Partition settings
  - **Default value:** https://external\_application\_url
  - **Minimum characters allowed:** 0
  - **Maximum length:** 100

## Security Settings

---

The following Settings can also be configured in **Security > Settings** at the partition level. For more information, see [Security Settings](#).

- Allow users to Change Password
- Inactive Time Out (Minutes)
- Session Time Out (Minutes)
- Allow Local Login for Partition Administrators
- Customer Departmentalization
- Password Complexity Policy
- Security Settings for Cookies

## 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.

- **Access level:** Partition settings
- **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.

- **Access level:** Partition settings
- **Default value:** 9
- **Minimum value:** 1
- **Maximum value:** 100

## Proxy Server Settings

---

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

- **Access level:** Partition settings
- **Default value:** Disabled
- **Value options:** Enabled, Disabled

### Server Hostname

Provide the fully qualified domain name of the proxy server.

- **Access level:** Partition settings

- **Default value:** —
- **Minimum value:** 0
- **Maximum value:** 1000

## Server Port

Provide the port number of the proxy server.

- **Access level:** Partition settings
- **Default value:** —
- **Minimum value:** 0
- **Maximum value:** 1000

## Authentication

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

- **Access level:** Partition settings
- **Default value:** Disabled
- **Value options:** Enabled, Disabled

## 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.

- **Access level:** Partition settings
- **Default value:** —
- **Minimum value:** 0
- **Maximum value:** 1000

## 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.

- **Access level:** Partition settings
- **Default value:** —
- **Minimum value:** 0
- **Maximum value:** 1000

## 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, Reports (in the Reports Console), Alarm workflows (in the Administration Console), and Abandoned chats (in the Administration Console). The address to which these notifications are sent is specified in the object's properties and the 'From' email address is defined in the **From: address for notifications from services** setting.

Configure the settings described in this section for the server to send notifications to administrators.

### SMTP Server Type

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

- **Access level:** Partition settings
- **Default value:** Never
- **Value options:** SMTP, ESMTP

### Use SMTP

If the SMTP Server type setting is set to ESMTP, then this should be used for the server.

- **Access level:** Partition settings
- **Default value:** Never
- **Value options:** Never, If authorization fails

### Authentication Type

In this setting, you can select the kind of authentication to use to connect to the servers.

- **Access level:** Partition settings
- **Default value:** OAuth 2.0
- **Value options:** OAuth 2.0, Basic Authentication

### Server Name

If the **Authentication Type** is set as **Basic Authentication**, provide the server name.

- **Access level:** Partition settings
- **Default value:** —
- **Minimum value:** 0
- **Maximum value:** 256

### User Name (ESMTP)

If the **Server Type** setting is set as **ESMTP** and the **Authentication Type** setting is set as **Basic Authentication**, provide the user name to connect to the mail server.

- **Access level:** Partition settings
- **Default value:** —
- **Minimum value:** 0
- **Maximum value:** 255

## Password

If the **Server Type** setting is set to **ESMTP** and the **Authentication Type** setting is set as **Basic Authentication**, provide the password to connect to the mail server.

- **Access level:** Partition settings
- **Default value:** —
- **Minimum value:** 0
- **Maximum value:** 255

## Verify Password

Verify the password you provided in the Password field.

- **Access level:** Partition settings
- **Default value:** —
- **Minimum value:** 0
- **Maximum value:** 255

## Connection Type

If the **Authentication Type** is set as **Basic Authentication**, select the authentication connection type for the server to use.

- **Access level:** Partition settings
- **Default value:** Plain text
- **Value options:** Plain text, SSL, TLS

## Server Port

If the **Authentication Type** is set as **Basic Authentication**, provide the port number of the SMTP server.

- **Access level:** Partition settings
- **Default value:** 25
- **Minimum value:** 1
- **Maximum value:** 65536

## Email Address

If the **Authentication Type** is set as **OAuth 2.0**, provide the email address.

Note: The address provided here should be same as defined for the **From: address for notifications from services** setting.

- **Access level:** Partition settings
- **Default value:** —

## OAuth Registered App

If the **Authentication Type** is set as **OAuth 2.0**, select an OAuth app you have configured.

- **Access level:** Partition settings
- **Default value:** —
- **Value options:** —

## Server Type

If **OAuth 2.0** is selected as the **Authentication Type**, the server types to choose depend on the OAuth provider. If **Gmail** is selected as the OAuth provider, the server type option is **SMTP**, while if **Microsoft Office 365** is the OAuth provider, the available option is **Graph API**.

- **Access level:** Partition settings
- **Default value:** —
- **Value options:** Graph API or SMTP

## Address

This field is populated automatically when the provider is selected. If the provider is Gmail, then the value populated is **smtp.gmail.com** and if Microsoft Office 365 is the provider, then the value populated is **graph.microsoft.com**.

- **Access level:** Partition settings
- **Default value:** —
- **Value options:** smtp.gmail.com or graph.microsoft.com

## Shared Mailbox

This option is visible only when Microsoft Office 365 is the provider.

**Access level:** Partition settings

**Default value:** —

**Value options:** Yes, No

## Authorization Code

You can click the **Generate** button to generate the authorization code as part of the authentication process.

## General Department Settings

---

The following settings can be configured at the department level. For more information about each setting, see [General Department Settings](#).

- Number of Activities Per Page
- Enable Conversation Stream
- Date and Time Format
- Date Format
- Business Calendar Timezone
- Agent Inbox Preference
- Refresh Interval (Seconds)
- Number of Activities to be Monitored for Service Level
- Service Email and Chat Activities at the Same Time
- Service Email and Phone Activities at the Same Time
- Service Chat and Phone Activities at the Same Time
- Agent Guidance Notifications

## General Department Settings

---

### Activity Assignment Settings

---

#### Number of Activities Per Page

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

- **Access level:** Department settings
- **Default value:** 20
- **Minimum value:** 0
- **Maximum value:** —
- **Editable at lower level:** Yes

## Common Settings

---

### 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.

- **Access level:** Department settings
- **Default value:** Yes
- **Value options:** Yes, No
- **Editable at lower level:** Yes

### Date and Time Format

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

- **Access level:** Department settings
- **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
- **Editable at lower level:** Yes

## Date Format

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

- **Access level:** Department settings
- **Default value:** 09/22/2019 (shows current date)
- **Value options:**
  - 09/22/2019
  - Sep/22/2019
  - September 22 2019
  - 2019-09-22
  - 22/09/2019
  - 22-09-2019
  - 22 Sep 2019
  - Sep 22, 2019
  - 22.09.2019
- **Editable at lower level:** Yes

## Business Calendar Timezone

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

- **Access level:** Department settings
- **Default value:** (GMT-05:00)Eastern Standard Time (US and Canada)

## Agent Inbox Preference

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

- **Access level:** Department settings
- **Default value:** Chat
- **Value options:** Chat, Mail
- **Editable at lower level:** Yes

## Supervisor Monitor Settings

---

### Refresh Interval (seconds)

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

- **Access level:** Department settings
- **Default value:** 30
- **Minimum value:** 10
- **Maximum value:** 6000
- **Editable at lower level:** Yes

### Number of Activities to be Monitored for Service Level

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

- **Access level:** Department settings
- **Default value:** 10
- **Minimum value:** 1
- **Maximum value:** 1000

## Activity Handling Settings

---

### 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.

- **Access level:** Partition settings, Department settings
- **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 in a chat session.
  - **No:** Agents cannot respond to email activities that are already assigned to them. The **Send**, and **Send and Complete** buttons are disabled for emails. Also, no new emails get assigned to agents while they are in a chat session. Agents cannot create outbound emails while they are in a chat session.
- **Editable at lower level:** Yes

## Service Email and Phone Activities at the Same Time

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

- **Access level:** Department settings
- **Default value:** No
- **Value options:**
  - **Yes:** Agents can continue to respond to email activities that are already assigned to them. The **Send** and **Send and Complete** buttons are enabled for emails. However, no new emails get assigned to agents while they are on a phone call. If agents are associated with an outbound MRD, they can create outbound emails during a phone call.
  - **No:** Agents cannot respond to email activities that are already assigned to them. The **Send** and **Send and Complete** buttons are disabled for emails. Also, no new emails get assigned to agents while they are on a phone call. Agents cannot create outbound emails while they are on a phone call.

## 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.

- **Access level:** Department settings
- **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. If agents are associated with an outbound MRD, they can create outbound chats during 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. Agents cannot create outbound chats while they are on a phone call.

## 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.

- **Access level:** Department settings
- **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.

## Chat Settings

---

### Activity Assignment 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.

##### [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.

- **Access level:** Partition settings
- **Default value:** Enabled
- **Value options:** Enabled, Disabled

##### [EXPIRY TIME FOR AUTO-PUSHBACK OF CHATS \(SECONDS\)](#)

Use this setting to define the time, in seconds, 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.

- **Access level:** Partition settings
- **Default value:** 120
- **Minimum value:** 30
- **Maximum value:** 12600

##### [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.

- **Access level:** Partition settings
- **Default value:** No
- **Value options:** Yes, 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.

- **Access level:** Partition settings
- **Default value:** Percentage
- **Value options:** Absolute, Percentage
- **Editable 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.

- **Access level:** Partition settings
- **Default value:** 5
- **Minimum value:** —
- **Maximum value:** —
- **Editable at lower level:** Yes

## 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.

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.

- **Access level:** Partition settings, Department settings, User settings
- **Default value:** Key
- **Value options:** Key, Activity ID, Case ID, When Created, Customer name, Subject, Activity sub status, Queue name
- **Editable 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.

- **Access level:** Partition settings, Department settings, User settings
- **Default value:** Descending
- **Value options:** Ascending, Descending
- **Editable 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 Agent Console. 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.

- **Access level:** Partition settings, Department settings
- **Default value:** 30
- **Minimum value:** 30
- **Maximum value:** 600
- **Editable at lower level:** Yes

## 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Yes
- **Value options:** Yes, No
- **Editable at lower level:** Yes

## Activity Handling Settings

---

### Chat - Force Resolution Code

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

- **Access level:** Partition settings, Department settings
- **Default value:** No

- **Value options:** Yes, No
- **Editable at lower level:** Yes

### Chat - Force Activity Categorization

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

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** Yes, No
- **Editable at lower level:** Yes

### Chat - Agent Chat Message Maximum Length

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

- **Access level:** Partition settings, Department settings
- **Default value:** 800
- **Minimum value:** 60
- **Maximum value:** 2000

### Require Activity Note on Transfer

Use this setting to decide if agents are required to add a note to the activity before transferring it to another agent or queue.

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** Yes, No

### 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Optional
- **Value options:** Optional, Required
- **Editable at lower level:** Yes

### 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Yes
- **Value options:** Yes, No
- **Editable at lower level:** Yes

### 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.

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** Yes, No
- **Editable at lower level:** Yes

## Common Chat Settings

---

### 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.

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** Yes, No
- **Editable at lower level:** Yes

### 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Yes
- **Value options:** Yes, No
- **Editable at lower level:** Yes

## Chat Service Level Settings

---

### 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.

- **Access level:** Partition settings, Department settings
- **Default value:** 600
- **Minimum value:** 0
- **Maximum value:** 3600
- **Editable at lower level:** Yes

### 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.

- **Access level:** Partition settings, Department settings
- **Default value:** All chats handled including abandoned
- **Value options:** All chats handled including abandoned, All chats handled excluding abandoned
- **Editable at lower level:** Yes

### Chat - Daily Service Level Timezone

Use this setting to select the time zone to be used for the daily service level for chats.

- **Access level:** Partition settings, Department settings
- **Default value:** (GMT-05:00) Eastern Standard Time (US and Canada)
- **Editable at lower level:** Yes

## Preferred Agent Assignment for Activity Settings

These settings assist in configuring the application to route incoming chat and messaging activities according to a preferred agent preference. With preferred agent assignment enabled, the preferred Agent ID is passed with a NEW\_TASK request to Unified CCE, which can then leverage it to perform the necessary routing and assignments. The application can then route activities to the preferred agent based on the configurations of the following settings.

You need to add the preferred agent ID node in the UCCE script for the preferred agent assignment to work seamlessly.

### Enable preferred agent assignment

Use this setting to enable the preferred agent assignment setting.

- **Access level:** Department settings
- **Default value:** All Queues
- **Value options:** All Queues; None

### Set last assigned agent as preferred agent

Use this setting to automatically set the agent who most recently handled a customer's chat or messaging activity as the preferred agent for the customer.

- **Access level:** Department settings
- **Default value:** Enabled
- **Value options:** Enabled; Disabled

### Allow agent to set preferred agent

Use this setting to allow agents to mark themselves as the preferred agent for a customer.

- **Access level:** Department settings
- **Default value:** Disabled
- **Value options:** Enabled; Disabled

### Allow agent to reset preferred agent

Use this setting to allow agents to clear the selected preferred agent for a customer. This removes the preferred agent from the customer's account and the customer no longer has a preferred agent assigned.

- **Access level:** Department settings
- **Default value:** Disabled
- **Value options:** Enabled; Disabled

### Assign to preferred agent

Use this setting to determine the routing method based on preferred agent settings.

- **Access level:** Department settings
- **Default value:** Available
- **Value options:** Always; Logged in; Available

### Ignore max load for preferred agent assignment

Use this setting to allow preferred agent routing to ignore the max load for an agent. Enabling this setting ensures that new chat and messaging activities are assigned to the customer's preferred agent even if the total number of activities that is currently assigned to the agent is at or exceeding the agent's max load setting.

- **Access level:** Department settings

- **Default value:** Disabled
- **Value options:** Enabled; Disabled

### Preferred agent assignment duration

Use this setting to determine the length of time that preferred agent routing should be active for a new chat activity before standard routing is used to assign the activity. If this is set to **Always**, preferred agent assignment routing takes priority and is always active. If this is set to **Number of days**, the **Preferred agent assignment duration in days** setting becomes active and can be set to determine the number of days the preferred agent assignment routing is active for an activity.

- **Access level:** Department settings
- **Default value:** Always
- **Value options:** Always; Number of Days

### Preferred agent assignment duration in days

Use this setting to determine the number of days that preferred agent assignment routing should be active for new chat activities. If this number of days is exceeded and the activity still has not been routed to the preferred agent, the activity is then routed to the next available agent with the appropriate permissions.

- **Access level:** Department settings
- **Default value:** 7
- **Minimum value:** 1
- **Maximum value:** 365

### Auto-pushback chats from preferred agent

Use this setting to decide if new chats assigned to agents should be automatically pushed back from the preferred 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. For more details, see [Chat Auto-Pushback Settings](#).

- **Access level:** Department settings
- **Default value:** Enabled
- **Value options:** Enabled; Disabled

## Email Settings

---

### Common Email Settings

---

#### 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 to identify the language of the activity.

- **Access level:** Partition settings
- **Default value:** 10
- **Minimum value:** 1 KB
- **Maximum value:** 1024 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.

- **Access level:** Partition settings
- **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.

- **Access level:** Partition settings
- **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.

### 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Do not change
- **Value 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.

- **Editable at lower level:** Yes

## 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.

- **Access level:** Partition settings, Department settings
- **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

## 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Activity ID
- **Value options:** Activity ID, Activity Priority, Case ID, Contact point, Department name, Subject, When created, Activity type, Activity sub status
- **Editable 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Ascending
- **Value options:** Ascending, Descending
- **Editable 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 mail inbox.

- **Access level:** Partition settings, Department settings

- **Default value:** Yes
- **Value options:** No, Yes
- **Editable at lower level:** Yes

## Dispatcher and Retriever Settings

---

### 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, auto-replies 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.

- **Access level:** Partition settings
- **Default value:** 25
- **Minimum value:** 1
- **Maximum value:** 150

### 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, auto-replies 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.

- **Access level:** Partition settings
- **Default value:** 100
- **Minimum value:** 100
- **Maximum value:** 1000

### Notification Mails Auto BCC

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

- **Access level:** Partition settings

- **Default value:** —
- **Minimum value:** 0
- **Maximum value:** 255

### Number of Emails to Retrieve

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

- **Access level:** Partition settings
- **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.

- **Access level:** Partition settings
- **Default value:** 16
- **Minimum value:** 2
- **Maximum value:** 50

### 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.

- **Access level:** Partition settings
- **Default value:** 1000 KB
- **Minimum value:** 100
- **Maximum value:** 1000 KB

## Workflow Settings

---

### 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.

- **Access level:** Partition settings
- **Default value:** 3
- **Minimum value:** 3
- **Maximum value:** 100

### 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.

- **Access level:** Partition settings
- **Default value:** 1440
- **Minimum value:** 360
- **Maximum value:** 1440

### Include Original Message for Auto Acknowledgement and Auto Reply

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

- **Access level:** Partition settings, Department settings
- **Default value:** Enable
- **Value options:** Disable, Enable
- **Editable at lower level:** Yes

### From Email Address for Alarm

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

- **Access level:** Partition settings, Department settings
- **Default value:** —
- **Minimum value:** 0
- **Maximum value:** 255
- **Editable 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.

- **Access level:** Partition settings, Department settings
- **Default value:** You have received a new activity
- **Value options:** —
- **Editable at lower level:** Yes

## 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
- **Default value:** You have received a new activity (id = ``activity\_id) from customer identified by ``contact\_point\_data
- **Value options:** —
- **Editable at lower level:** Yes

## Block all Attachments

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

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

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** Yes, No

## Action on Blocked Attachments

Use this setting to decide what should be done with all the blocked attachments. You can either restore the quarantined attachments from the database or you can delete them. Agents must have the **Restore Attachment** action assigned to them to restore the attachment from the database.

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

- **Access level:** Partition settings, Department settings
- **Default value:** Quarantine
- **Value options:**
  - **Quarantine:** The attachment is saved in the database and a notification email is sent to the administrator.
  - **Delete:** The attachment is deleted.

- **Editable at lower level:** Yes

## 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.

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

- **Access level:** Partition settings, Department settings
- **Default value:** Inbound emails only
- **Value options:** Inbound email only, Both inbound and outbound emails
- **Editable at lower level:** Yes

## Activity Assignment Settings

---

### 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.

- **Access level:** Partition settings
- **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.

- **Access level:** Partition settings, Department settings
- **Default value:** 10
- **Minimum value:** 1
- **Maximum value:** 25
- **Editable 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Most overdue

- **Value options:** Most overdue, Due Soonest, Highest Priority, Newest, Oldest
- **Editable at lower level:** Yes

### 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. The following alerts are displayed: 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.

- **Access level:** Partition settings, Department settings
- **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.
- **Editable at lower level:** Yes

### 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Enabled
- **Value options:** Disabled, Enabled
- **Editable at lower level:** Yes

### 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.

- **Access level:** Partition settings, Department settings
- **Default value:** 30
- **Minimum value:** 0
- **Maximum value:** 21600 (15 Days)

- **Editable at lower level:** Yes

### Activity Type for Autopushback

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

- **Access level:** Partition settings, Department settings
- **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" are pushed back to the queues.
  - **Both new and incomplete activities:** All the activities are pushed back to the queues.
- **Editable 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.

- **Access level:** Partition settings, Department settings
- **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.
- **Editable at lower level:** Yes

## Activity Handling Settings

---

### 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.

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** No, Yes
- **Editable 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.

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** No, Yes
- **Editable at lower level:** Yes

## Require Activity Note on Transfer

Use this setting to decide if agents are required to add a note to the activity before transferring it to another agent or queue.

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** Yes, No

## 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Yes
- **Value options:** Yes, No
- **Editable at lower level:** Yes

## 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Basic
- **Value options:** None, Basic, Complete
- **Editable at lower level:** Yes

## Personalized Activity Assignment Settings

The personalized activity assignment feature assists in configuring the application to route incoming 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 Agent ID is passed with a NEW\_TASK request to Unified CCE when next email reply (activity

ID 1003) from the customer comes in. Unified CCE can then leverage it to perform the necessary routing and assignments.

#### [PERSONALIZED ACTIVITY ASSIGNMENT](#)

- **Access level:** Partition settings, Department settings
- **Default value:** Logged in
- **Value options:** Always, Disable

#### [ENABLE PERSONALIZED ACTIVITY ASSIGNMENT FOR FORWARDED ACTIVITIES](#)

Use this setting to enable personalized activity assignment for forwarded emails.

- **Access level:** Partition settings, Department settings
- **Default value:** Enabled
- **Value options:** Enabled, Disabled

#### [ENABLE PERSONALIZED ACTIVITY ASSIGNMENT TO FOREIGN USERS](#)

Use this setting to enable personalized activity assignment feature for foreign users in a department.

- **Access level:** Partition settings, Department settings
- **Default value:** Enabled
- **Value options:** Enabled, Disabled

#### [ENABLE PERSONALIZED ACTIVITY ASSIGNMENT ONLY TO USERS WITH PERMISSIONS ON QUEUE](#)

Use this setting to enable personalized activity assignment feature for just users with permissions for the queue.

- **Access level:** Partition settings, Department settings
- **Default value:** Disabled
- **Value options:** Enabled, Disabled

## Knowledge Settings

---

### eGain Knowledge System

---

This setting only applies to systems that have purchased Knowledge add-ons.


Use this setting to identify an external knowledge system as the source of knowledge for configuration with digital channels, such as chat or email. The URL for the knowledge system must be provided here in order to configure queues to use external knowledge bases for Solve.

- Access Level: Partition settings; Department settings
- Default value: —
- Minimum: —

- **Maximum:** —
- **Editable at lower level:** Yes

## KB Primary Language

---

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

- **Access level:** Partition settings, Department settings
- **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
- **Editable 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Custom
- **Minimum:** 0
- **Maximum:** 225
- **Editable at lower level:** Yes

## Language Settings

---

Many of these language settings can be managed at the Partition and Department level. These control features such as the auto spellcheck function and treatment of special characters. These settings are applied to all departments located under the partition.

**Note:** The All Departments Language Settings are not the same as the actions and functions managed through the Language Tools option in the Top menu.

## 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.

- **Access level:** Partition settings, Department settings

- **Default value:** No
- **Value options:** Yes, No
- **Editable 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.

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** Yes, No
- **Editable 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.

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** Yes, No
- **Editable 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.

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** Yes, No
- **Editable 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.

- **Access level:** Partition settings, Department settings

- **Default value:** No
- **Value options:** Yes, No
- **Editable at lower level:** Yes

## Auto Spellcheck

---

Use this setting to enable automatic spell check for emails, tasks, and so on. This setting is not used for chat activities. For chat, use the **Chat - Auto spellcheck** setting.

- **Access level:** Partition settings, Department settings
- **Default value:** Enable
- **Value options:** Disable, Enable
- **Editable at lower level:** Yes

## Auto Blockcheck

---

Use this setting to check the content of emails, tasks, and so on 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 [Viewing and Adding Blocked Words](#).

- **Access level:** Partition settings, Department settings
- **Default value:** Enable
- **Value options:** Enable, Disable
- **Editable 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.

- **Access level:** Partition settings, Department settings
- **Default value:** No
- **Value options:** Yes, No
- **Editable at lower level:** Yes

## Include Original Message Text During Spell Check

---

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

- **Access level:** Partition settings, Department settings

- **Default value:** No
- **Value options:** Yes, No
- **Editable at lower level:** Yes

## Chat - Auto Blockcheck

---

Use this setting to check the chat messages for blocked words. The list of blocked words is set from the Dictionaries node in the Administration Console. For details, see [Viewing and Adding Blocked Words](#).

- **Access level:** Partition settings, Department settings
- **Default value:** Enable
- **Value options:** Enable, Disable
- **Editable 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.

- **Access level:** Partition settings, Department settings
- **Default value:** Disable
- **Value options:** Disable, Enable
- **Editable at lower level:** Yes

## Preferred Dictionary of the User

---

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

This setting is only available under the Language Tools > Settings section of an individual department

- **Access level:** Partition settings, Department settings
- **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
- **Editable at lower level:** Yes

# Security Settings

---

## 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.

- **Access level:** Partition settings
- **Default value:** Yes
- **Value options:** Yes, No

## 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.

- **Access level:** Partition settings
- **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 to the application by providing their user name and password and a new user session is created.

- **Access level:** Partition settings
- **Default value:** 60
- **Minimum:** 5
- **Maximum:** 1440

## Allow Local Login for Partition Administrators

---

While this setting applies to partition administrators that utilize single sign-on, it is not required for single sign-on to function. For more information, see [Configuring Single Sign-On for Partition Administrators](#).

Users outside this partition, or without this permission, will not be able to log in to the application with this URL.

- **Access level:** Partition settings
- **Default value:** Yes
- **Value options:** Yes, No

## 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.

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.

- **Access level:** Partition settings
- **Default value:** No
- **Value options:** No, Yes

# Appendix

- [Maximum Limits](#)

## Maximum Limits

---

The following tables contain the maximum limits for various objects that can be created in the Administration Console.

### Chat

Object	Maximum Number
Chat Entry Points	1000
Call Variables	75
Messaging Adapters	25

### Email

Object	Maximum Number
Email Alias	1000
Email Delivery Exceptions	1000
Blocked Extensions	25
Masking Patterns	100
Service Levels	25

## Administration

<b>Object</b>	<b>Maximum Number</b>
Service Processes	100
Service Instances	25
Identity Providers	25
Purge Jobs	25
Shift Labels	75
Day Labels	75
Calendars	75
Transfer Codes	75
Not Ready Reason Codes	75
Dictionary	25
Authentication Configuration	25
Access Links	75
Usage Links	75
Link Groups	75
User Roles	25
Supervision Monitors	100