Enterprise Chat and Email Administrator’s Guide to Administration Console, Release 11.5(1)

For Unified Contact Center Enterprise

August 2016

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

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.

Enterprise Chat and Email Administrator’s Guide to Administration Console: For Unified Contact Center Enterprise. November 21, 2016

Contents

Preface

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

About This Guide

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Documentation Feedback

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

We appreciate your comments.

Field Alerts and Field Notices

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

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

Document Conventions

This guide uses the following typographical conventions.

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

Document conventions

Acronyms and Initialisms

Acronyms and initialisms used in this document are listed here:

- ARM: Agent Reporting and Management
- CSA: Cisco Security Agent
- CTI: Computer Telephony Integration
- EAAS: External Agent Assignment Service
- JDBC: Java Database Connectivity
- MR: Media Routing
- MRD: Media Routing Domain
- Packaged CCE: Packaged Contact Center Enterprise
- PG: Peripheral Gateway
- PIM: Peripheral Interface Manager
- SNMP: Simple Network Management Protocol
- UI: User Interface
- Unified CCE: Unified Contact Center Enterprise

Other Learning Resources

Various learning tools are available within the product, as well as on the product CD and our web site. You can also request formal end-user or technical training.

Online Help

The product includes topic-based as well as context-sensitive help.

Use	To view
? **Help** button	Topics in *Enterprise Chat and Email Help*; the Help button appears in the console toolbar on every screen.
F1 keypad button	Context-sensitive information about the item selected on the screen.

Online help options

Document Set

The Enterprise Chat and Email documentation is available in the `Documents` folder on the product CD. The latest versions of all Cisco documentation can be found online at http://www.cisco.com

The document set contains the following guides:

- *System Requirements for Enterprise Chat and Email*
- *Enterprise Chat and Email Installation Guide*
- *Enterprise Chat and Email Browser Settings Guide*

User guides for agents and supervisors

- *Enterprise Chat and Email Agent's Guide*
- *Enterprise Chat and Email Supervisor's Guide*

User guides for administrators

- *Enterprise Chat and Email Administrator's Guide to Administration Console*
- *Enterprise Chat and Email Administrator's Guide to Routing and Workflows*
- *Enterprise Chat and Email Administrator's Guide to Chat and Collaboration Resources*
- *Enterprise Chat and Email Administrator's Guide to Email Resources*
- *Enterprise Chat and Email Administrator's Guide to Reports Console*
- *Enterprise Chat and Email Administrator's Guide to System Console*
- *Enterprise Chat and Email Administrator's Guide to Tools Console*

1

Console Basics

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

Important Administration Tasks

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

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

The next section describes each of these concepts in detail.

Key Terms and Concepts

System and Business Areas

The application has two areas:

- **System area:** Used by system administrators to set up and manage system resources such as host machines and services. It has two consoles:
  - Administration Console
  - System Console

  Very few users need access to this area as it is used only for system administration tasks.
- **Business area:** The main part of the installation, used by business users to perform their tasks. It has all seven consoles:

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

Partitions and Departments

When the application is installed, a partition is created by the installation program, with one department in it. This department is called `Service` and can be renamed.

You can create additional departments to:

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

Settings

Settings are selective properties of business objects and are used to configure the way the system works. For example, security settings help you configure the following properties of user passwords - the expiry time period for passwords, the characters allowed in passwords, etc. Settings are administered in groups. The available groups are:

- System settings group
- Partition settings group
- Department settings group
- User settings group

For more information, see "Settings" on page 36.

Users

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

Users can be created at three levels:

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

Two users are created during the installation:

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

For more information, see "Users" on page 120.

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," "Edit customer," and "Add notes." You can create user roles as per the needs of your organization, and assign these roles to your employees. To ease your task, the system comes with some default user roles. You can use these, and if required, create your own user roles. You can assign one or more roles to a group of users or an individual user.

For more information, see "Users" on page 120.

User Groups

User groups are a collection of users that share similar functions or roles in the system. Groups make it much easier to manage user accounts. Like users, user groups can also be created in the system partition, business partition, and departments. A standard user group called **All Users in** *Department_Name* is created in each department. Every new user in the department is automatically included in this group.

For more information, see "Users" on page 120.

Email Infrastructure

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

The following objects can be configured for emails:

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

permanent bounceback indicates that an irreparable reason (such as invalid email address) caused the email to bounce back. A temporary bounceback indicates that a temporary reason (such as out of office reply, destination server down, etc.) caused the email to bounce back.

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

Chat and Collaboration Infrastructure

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

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

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

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

Data Masking for Email and Chat

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

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

Data masking is available for emails and chats. For more information, see "Data Masking" on page 134.

Workflows

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

- Alarm workflows
- Inbound workflows
- Outbound workflows

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

Queues

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

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

Service Levels

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

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

Calendars

You can create a business calendar for your organization. It allows you to set up working and non-working hours and days for employees in your department. To create your business calendar, it is essential that you first create shifts and day labels.

- **Shift labels:** According to the working hours of your company, you can organize various shifts for agents in your department. It also allows you to create shifts for holidays and extra working hours.
- **Day labels:** Day labels enable you to assign time slots to the shifts that you have created in the Shift label. You cannot create day labels, if you have not created shift labels first.
- **Calendars:** Use the day labels to form a calendar for the work days in a week. You can also specify exceptional days, such as holidays or an extra working day. Please note that you can have only one active calendar for each department.

For more information, see "Business Calendars" on page 174.

Classifications

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

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

For more information, see "Classifications" on page 182.

Dictionaries

Dictionaries refer to a list of words stored in the system for reference. Agents use dictionaries to check spellings in outgoing emails. Each department comes with 13 predefined dictionaries and one of them is configured as the default dictionary. A department can have only one default dictionary and it can be changed according to the business requirements.

For more information, see "Dictionaries" on page 186.

Macros

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

You can create business object macros for:

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

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

For more information, see "Macros" on page 190.

Solve

Solve is a knowledge app that can easily be embedded into the agent desktop to quickly enable Voice, Email and Chat agents with the powerful eGain Knowledge resources. These resources can greatly assist agents in quickly resolving customer issues and answering questions. Solve is currently available only for systems integrated with Unified CCE. For more information, see the *eGain for Unified CCE Companion Guide*.

Archive Jobs

Old activities can be archived by setting up scheduled or on-demand archive jobs. For more information, see "Archive" on page 194.

Sharing of Business Objects

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

System Level

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

Administration Console

- Roles, users, and user groups
- Settings

System Console

- Service Processes
- Loggers
- Hosts

Partition Level

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

Administration Console

- Roles, users, and user groups
- Settings: partition and department settings
- Integration options: integrate with Unified CCE, configure Solve
- Security settings: data masking rules, CORS, SSO, attachments, rich text content policies, reCaptcha
- Departments: Departments are created (new or copies of existing departments) and department sharing is managed by partition administrators.

System Console

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

Tools Console

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

Department Level

Administration Console

Except for users, any of the following objects cannot be shared with other departments. However, the foreign users can manage these objects in the departments they are shared with. Access to these objects is controlled by roles and permissions.

- Settings
- Roles, users, and user groups: Users can be shared with other departments, and are called *foreign users* in the departments they are shared with. See details in "Sharing Users with Other Departments" on page 182.
- Business calendars
- Queues, service levels, and workflows
- Chat infrastructure
- Email infrastructure
- Data masking
- Classifications
- Dictionaries
- Macros
- Secure Messaging
- Archive jobs

KB Console

- KB Articles
  - Not shared
  - Exception: Foreign users can view and create articles in the departments they are shared with.

Reports Console

- Not shared
- Exception: Foreign users can run reports on the departments they are shared with.

Supervision Console

- Not shared
- Exception: Foreign users can create monitors in the departments they are shared with.

Tools Console

- Not shared

- Exception: Foreign users can manage objects in the departments they are shared with.

Agent Console

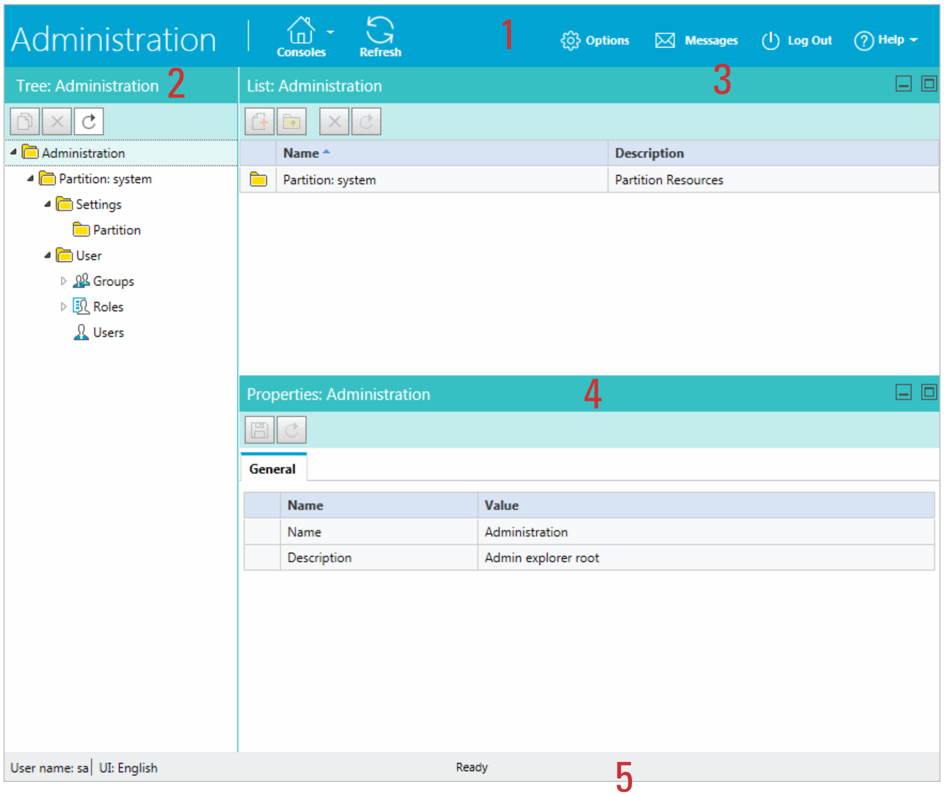
- Not shared
- Exceptions:
  - Customers: If customer departmentalization is not enabled (see “Customer Departmentalization” on page 61), agents can search and view customers across departments. And, when an agent creates an activity for a customer that already exists in another department, they will see the complete history of the customer (all cases and activities).
  - Foreign users can work on activities from departments they are shared with.

Elements of the User Interface

The console user interface has five functional areas:

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

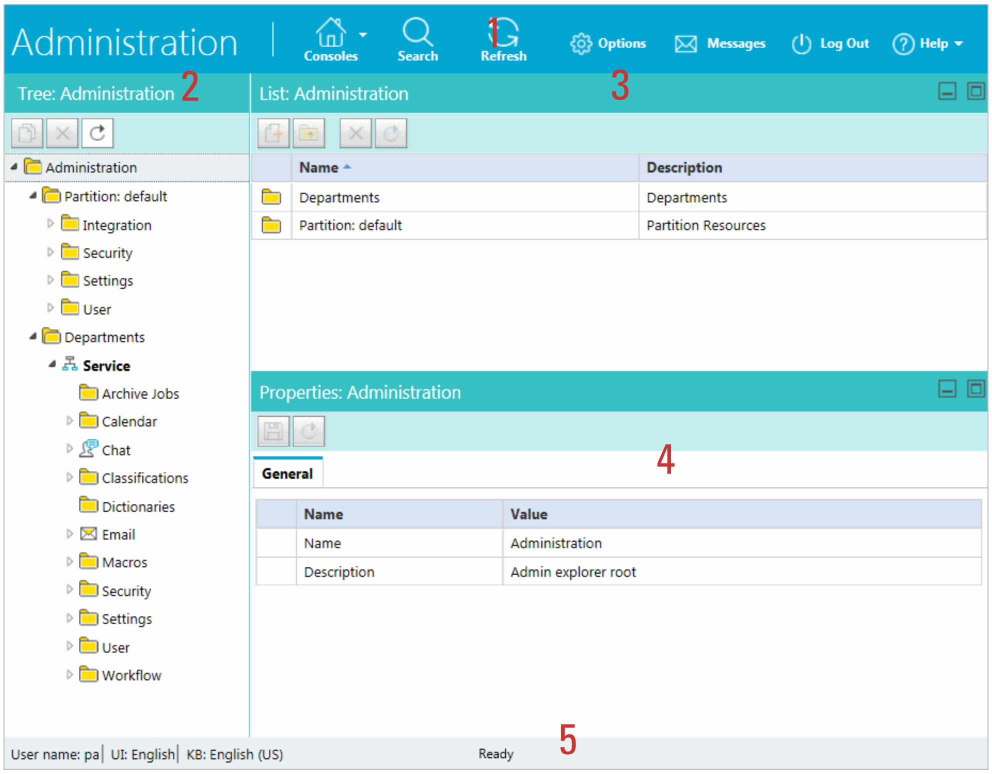
   To expand all first and second level nodes with a single click, shift + click the plus [+] button next to the topmost node. The contents of all first and second level nodes are displayed in the Tree pane.
3. **List pane:** The List pane displays first-level contents of the folder selected in the Tree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



Name	Description
Partition: system	Partition Resources

Name	Value
Name	Administration
Description	Admin explorer root

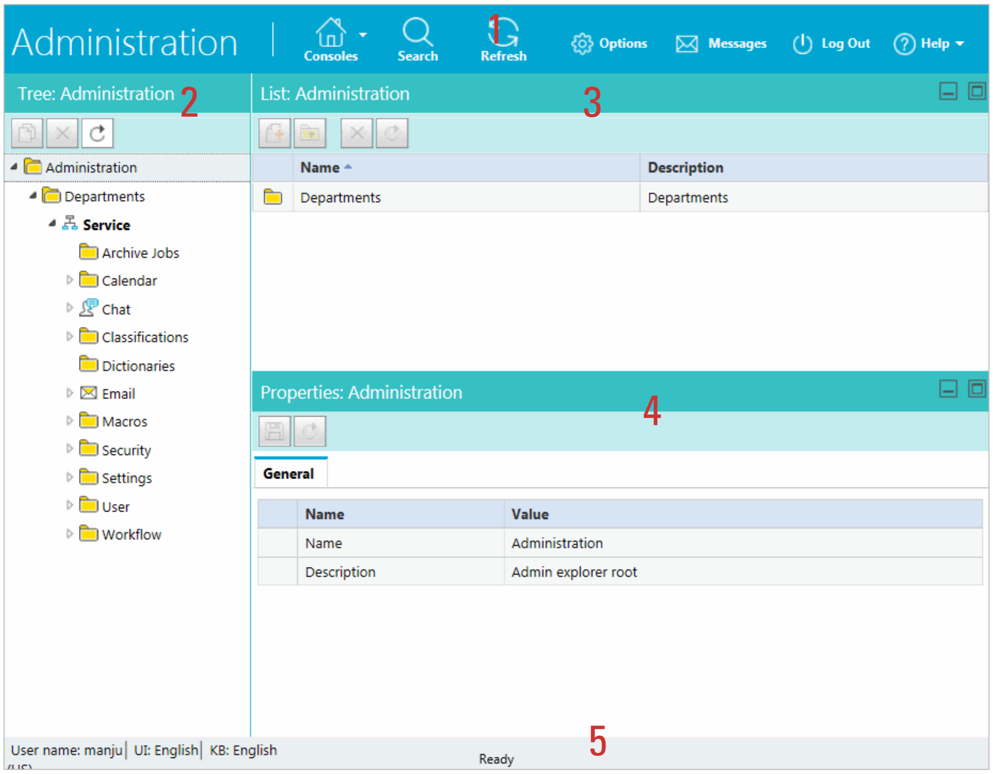
Elements of the Administration Console available in the system partition



Name	Description
Departments	Departments
Partition: default	Partition Resources

Name	Value
Name	Administration
Description	Admin explorer root

Elements of the Administration Console available in the business partition



Name	Description
Departments	Departments

Name	Value
Name	Administration
Description	Admin explorer root

User name: manju | UI: English | KB: English (US)

Ready

Elements of the Administration Console available in a department

2

Unified CCE Integration

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

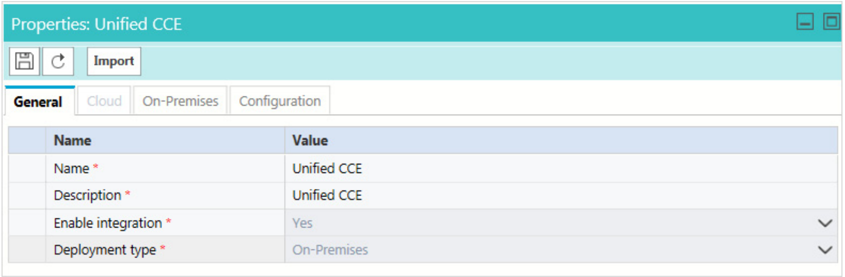
About Unified CCE Integration

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

Configuring Integration

To integrate ECE with Unified CCE:

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

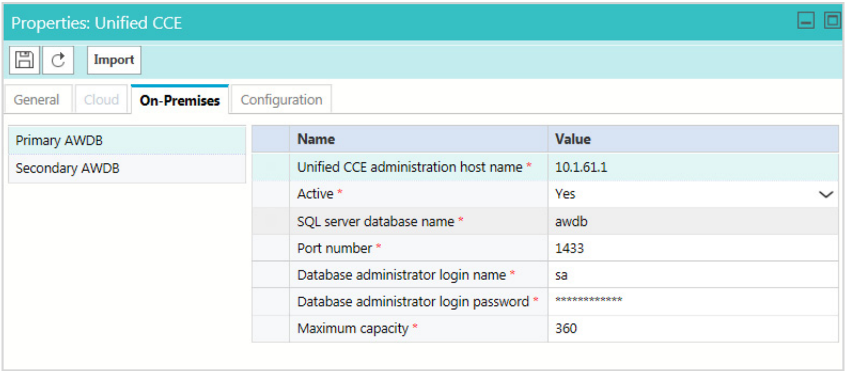


Name	Value
Name *	Unified CCE
Description *	Unified CCE
Enable integration *	Yes
Deployment type *	On-Premises

View the general properties

4. In the Properties pane, on the On-Premises tab, provide the following details for the Primary AWDB section:
   - **Unified CCE administration host name:** The server name or IP address of the host on which Packaged CCE or Unified CCE is installed.
   - **Active:** Set to **Yes**.
   - **SQL server database name:** The name of the AWDB database.
   - **Port number:** Set the value to match the database port configured in MSSQL for this database. By default the value is set to 1433.
   - **Database administrator login name:** The database administrator’s user name.
   - **Database administrator login password:** The database administrator’s password.

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

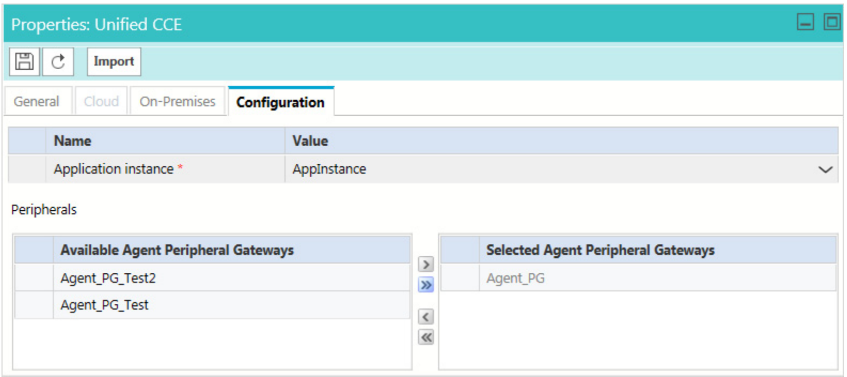


Name	Value
Unified CCE administration host name *	10.1.61.1
Active *	Yes
SQL server database name *	awdb
Port number *	1433
Database administrator login name *	sa
Database administrator login password *	************
Maximum capacity *	360

Provide the primary AWDB server details

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

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



Name	Value
Application instance *	AppInstance

Available Agent Peripheral Gateways
Agent_PG_Test2
Agent_PG_Test

Selected Agent Peripheral Gateways
Agent_PG

Provide configuration details

8. Click the **Save** 💾 button. You system is now connected with Unified CCE. To complete the integration, you must import the MRDs users and skill groups from the Unified CCE system. For more information, see "Importing Data" on page 33.

Importing Data

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

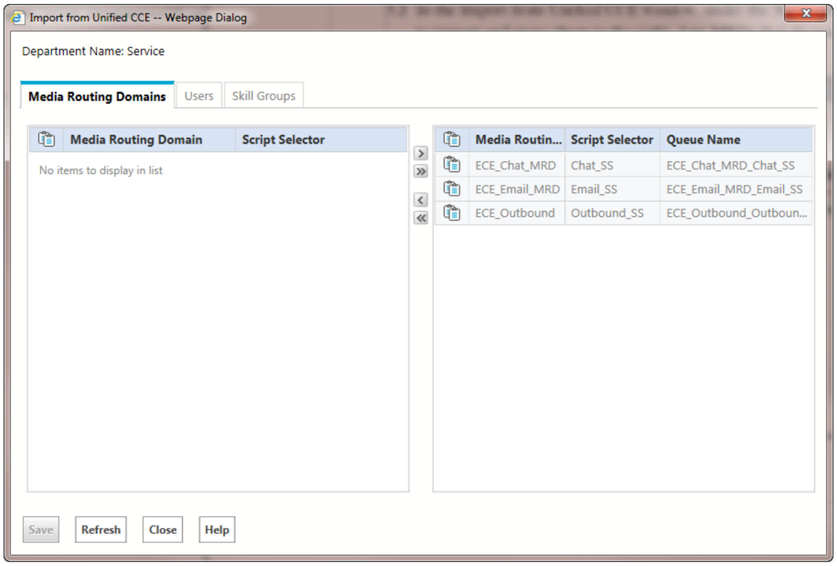
- **Media Routing Domains (MRDs):** These are shown as queues upon importing to a selected department.
- **Users:** These are shown as users upon importing to a selected department.
- **Skill Groups:** These are shown as user groups upon importing to a selected department.

Importing Media Routing Domains

The MRDs available for importing are decided based on the media classes configured in the partition level setting: Media Class Names (page 45). 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 Tree pane, browse to **Administration > Partition:** *Partition Name* **> Integration > Unified CCE > Unified CCE**.
2. In the List pane toolbar, select the **Unified CCE**.
3. In the Properties pane, click the **Import** button.
4. From the Select Department window, select the department to which you are importing the MRDs. If you only have one department in your system, this step is skipped.
5. In the Import from Unified CCE window, under the Media Routing Domains tab, select the MRDs you wish to import and move them to the right. Any MRDs that do not have script selectors, or that have already been imported, are not shown.



Department Name: Service

Media Routing Domain	Script Selector
No items to display in list	

Media Routin...	Script Selector	Queue Name
ECE_Chat_MRD	Chat_SS	ECE_Chat_MRD_Chat_SS
ECE_Email_MRD	Email_SS	ECE_Email_MRD_Email_SS
ECE_Outbound	Outbound_SS	ECE_Outbound_Outboun...

Import MRDs

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.

7. Click the **Save** button.

Importing Users

To import Unified CCE users:

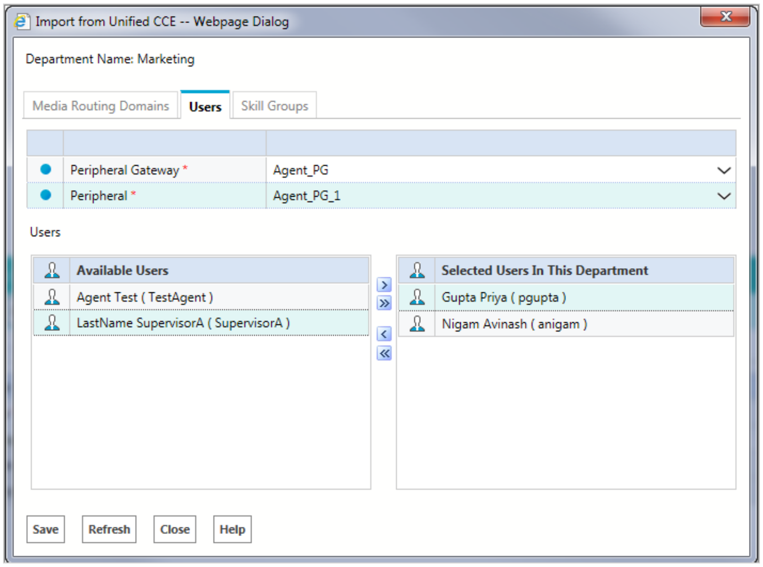
1. In the Tree pane, browse to **Administration > Partition:** *Partition Name* **> Integration > Unified CCE > Unified CCE**.

2. In the List pane toolbar, select **Unified CCE**.

3. In the Properties pane, click the **Import** button.

4. From the Select Department window, select the department to which you are importing the users. If you only have one department in your system, this step is skipped.

5. In the Import from Unified CCE window, click the Users tab and set the following:
   - ❍ Select the peripheral gateway from the dropdown.
   - ❍ Select the appropriate peripheral.
   - ❍ Select the users from the Available Users list if you wish to import and move them to the Select Users in this Department list.



Department Name: Marketing

●	Peripheral Gateway *	Agent_PG
●	Peripheral *	Agent_PG_1

Users

Available Users	Selected Users In This Department
Agent Test (TestAgent)	Gupta Priya (pgupta)
LastName SupervisorA (SupervisorA)	Nigam Avinash (anigam)

Import users

6. Click the **Save** button.

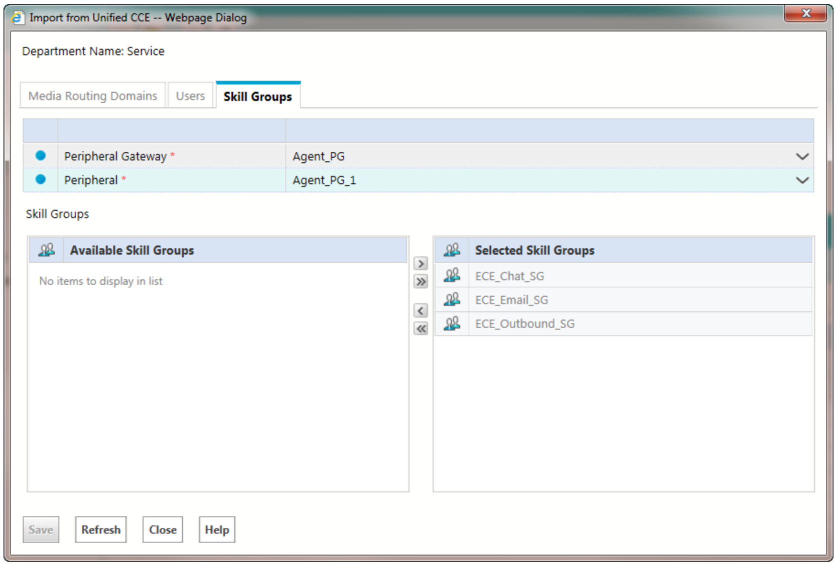
   Once users have been imported to ECE, they can log into the application using their Unified CCE login credentials. The login credentials of a user in ECE is case-sensitive and must match their Unified CCE credentials.

Newly imported users may still need to have user roles assigned. For more information about assigning user roles, see "Editing Department Users" on page 126.

Importing Skill Groups

To import skill groups:

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


Import from Unified CCE -- Webpage Dialog

Department Name: Service

Peripheral Gateway *: Agent_PG

Peripheral *: Agent_PG_1

Skill Groups

Available Skill Groups: No items to display in list

Selected Skill Groups: ECE_Chat_SG, ECE_Email_SG, ECE_Outbound_SG

Import skill groups

6. Click the **Save** button.

3

Settings

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

About Settings

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

Settings are administered in groups. The available groups are:

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

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

4. **User settings group:** If administrators want settings within a department to have different values for different users, they can achieve it by configuring user settings groups. Only a subset of department settings is available as part of this group. A department comes with a default user settings group and all the users created in that department automatically become a part of the default group. Administrator can make these settings available to individual users as user preferences. Users can configure these settings according to their choice. This group includes:
    a. Activity settings
    b. Activity pushback settings
    c. Common settings
    d. General settings
    e. Knowledge base settings
    f. Monitoring settings
    g. Spell checker settings
    h. User settings

Settings to Configure After Installation

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

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

Mandatory Settings

At the Partition Level

Make sure you configure the following settings:

- To: address for notifications from services (page 66)
- From: address for notifications from services (page 66)
- Notification mails SMTP Server (page 67)
- Default SMTP server (page 69)

Configure the following partition-level settings only if you use ESMTP protocol for exception and spam emails and notifications.

- Notification mails SMTP user name (page 69)

- Notification mails SMTP password (page 69)

At the Department Level

Configure the following setting for each department.

- From email address for alarm (page 72)

Optional Settings

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

At the Partition Level

- Customer departmentalization (page 61)
- Inactive time out (page 57)
- Session time out (page 57)
- Exception mail redirection to address (page 64)
- Exception mail redirection from address (page 64)

At the Department Level

- Business calendar timezone (page 57)

Configuring Settings

Configuring System Partition Settings

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

To configure a system partition setting:

1. Log in to the system partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Context_Root_Name* **> Settings > Partition**.
3. In the List pane, select the Partition settings group.

   The Properties pane refreshes to show the attributes of the group.
4. Next, in the Properties pane, go to the Attributes tab to configure values for settings. From the list, select a setting to modify. In the **Value** field provide a value for the setting.
5. Click the **Save** 💾 button.

Configuring Business Partition Settings

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

To configure a business partition setting:

1. Log in to the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration >** *Partition_Name* **> Settings > Partition**.
3. In the List pane, select the partition settings group.

   The Properties pane refreshes to show the attributes of the group.
4. Next, in the Properties pane, go to the Attributes tab to configure values for settings. From the list, select a setting to modify. In the **Value** field provide a value for the setting.
5. Click the **Save** 🖫 button.

Configuring Department Settings

To configure a department setting:

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

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

   a. In the **Value** field provide a value for the setting.

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

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

Configuring User Settings

To configure a user setting:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> Settings > User.**
2. In the List pane, select a user settings group.

   The Properties pane refreshes to show the attributes of the group.
3. 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. In the **Can be reset at lower level** field select **No**. Once the value is set to **No**, the value of the setting cannot be changed at user level. By default it is set to **Yes**.
4. Click the **Save** button.

Creating User Settings Groups

Administrator can allow a handful of department setting to be configured at 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.

Note that 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.

To create a user settings group:

1. In the Tree pane browse to **Administration > Departments >** *Department_Name* **> Settings > User**.
2. In the List pane click the **New** button.

   The Properties pane refreshes to show the attributes of the group.
3. In the General tab provide the name and description. The name of the group cannot be changed once the setting is saved.
4. Click the **Save** button. The Attributes and Relationship tabs are enabled only after the settings group is saved.
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 **Can be reset at lower level** field select **No**. Once it is set to **No**, the value of the setting cannot be changed at user level. By default it is set to **No**. If it is set to Yes then the users in that group can change the value of the setting from User Preferences.
6. 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.

7. Click the **Save** 💾 button.

Unified CCE Integration Settings

Agent Availability Settings After Completion of Call

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

Mark Agent Ready After Completion of Call

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

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

Event Reason Code to Track Agent State

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

- Type: Partition settings group
- Subtype: Unified CCE integration
- Data type: Integer
- Default value: 32767
- Value options: -

Allow Activity Transfer to Agents Who Are Not Available

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

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

Allow Transfer of Activities to Integrated Queues in Other Departments

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

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

Chat Watchdog Interval (Seconds)

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

- Type: Partition settings group
- Subtype: Unified CCE Integration
- Data type: Integer
- Default value: 70
- Minimum value: 70
- Maximum value: 350

Enable Chat Queueing

This allows customers to initiate new chats even when all agents are working at their maximum capacity. The chat requests are then queued in Unified CCE to wait for the next available agents. The maximum time for which a chat is queued is defined by the **Chat Watchdog Interval** (page 44) setting.

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

Maximum Wait Time for Login Response From UCCE (Seconds)

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

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

Media Class Names

This setting refers to the names of the media classes configured in Unified CCE. If the media class names have been changed in Unified CCE from their default names, they must also be changed here to match. Note that media class names are case sensitive.

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

- Type: Partition settings group
- Subtype: Unified CCE integration
- Data type: String
- Default values:
  - Voice media class: Cisco_Voice
  - Chat media class: ECE_Chat
  - Email media class: ECE_Email
  - Outbound media class: ECE_Outbound
- Value options: The secondary window allows for custom Media Classes to be designated.

Proactive Monitoring Refresh Interval (Seconds)

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

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

Reason Code for Agent Not Ready

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

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

Starvation Time for Activities

The maximum time the system will wait to send a routing request for an activity. After the time limit set in these settings is met, the request for the waiting activity is sent first. Priority sequence for activities is - delayed callback, chat, and email. For example, if the system is overloaded with multiple callback activities, and is unable to process a chat activity, then after the starvation time of chat activity, it will process the chat activity first before processing the next call activity.

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

Common Settings

Installation Name

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

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

- Default value: —

Web Server URL or Load Balancer URL

In this setting define the Web server URL or the Load Balancer URL if your installation has multiple web servers.

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

Shortening Base URL

Use this setting to define the base URL for shortening purposes.

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

Date Format

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

- Type: Department settings group, User settings group
- Subtype: Common
- Data type: Enumeration
- Default value: 09/22/2016 (shows current date)
- Value options:
  - 09/22/2016
  - Sep/22/2016
  - September 22 2016
  - 2016-09-22
  - 22/09/2016
  - 22-09-2016
  - 22 Sep 2016

- Sep 22, 2016
- 22.09.2016

- Can be reset at lower level: Yes

Date and Time Format

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

- Type: Department settings group, User settings group
- Subtype: Common
- Data type: Enumeration
- Default value: 09/22/2015 3:15:30 PM (shows current date and time)
- Value options:
  - 09/22/2015 3:15:30 PM
  - Sep/22/2015 3:15:30 PM
  - September 22 2015 3:15:30 PM
  - 2015-09-22 3:15:30 PM
  - 22/09/2015 3:15:30 PM
  - 22-09-2015 3:15:30 PM
  - 22 Sep 2015 3:15:30 PM
  - Sep 22, 2015 3:15:30 PM
  - 22.09.2015 3:15:30 PM
- Can be reset at lower level: Yes

Security Settings for Cookies

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

Secure the Cookies Created by Application for Consoles and Knowledge Portals

Enable this setting to secure all the cookies created by the application for user consoles (For example, Agent Console, Administration Console, etc.). When this setting is enabled, you must configure SSL for accessing the ECE application. For details, see the *Enterprise Chat and Email Installation Guide*. If SSL is not configured, users will not be able to access the application. You can enable this setting only while accessing the application using the HTTPS protocol.

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

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

Secure the Cookies Created by Application for Customer Websites

Enable this setting to secure all the cookies created by the application for the customer websites.

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

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

Proxy Server Settings

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

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

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

Use Server

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

- Type: Partition settings group
- Subtype: Common

- Data type: Enumeration
- Default value: No
- Value options: Yes, No

Server Hostname

Provide the fully qualified domain name of the proxy server.

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

Server Port

Provide the port number of the proxy server.

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

Authentication

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

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

Username

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

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

Password

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

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

Logger Settings

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

Maximum Backups of Log Files

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

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

Default Size in MB

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

- Type: System partition settings group
- Subtype: Logger
- Data type: Integer
- Default value: 5
- Minimum value: —
- Maximum value: —

Default Log Level

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

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

User Account Settings

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

Password Complexity Policy

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

- Type: Partition settings group
- Subtype: Security
- Data type: String
- Default value: ((?=.*[0-9])(?=.*[a-z]|[A-Z]).{8,20})
- Default failure message: The password does not comply with the password policy. Password should be at least of 8 characters having a mix of numbers and alphabets.

- Minimum value: 0
- Maximum value: 1000
- Can be reset at lower level: No

Login Name Minimum Length

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

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

Login Password Case Sensitive

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

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

Password Life Time

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

- Type: Department settings group
- Subtype: Security
- Data type: Integer
- Default value: 0

- Minimum value: 0
- Maximum value: —
- Can be reset at lower level: No

Password Life Time Unit

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

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

Allow Users to Change Password

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

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

Unsuccessful Attempts Time Frame

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

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

- Can be reset at lower level: No

Unsuccessful Attempts Time Unit

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

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

Maximum Number of Unsuccessful Timed Attempts

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

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

Maximum Number of Unsuccessful Attempts

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

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

Maximum Inactivity Time Frame

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

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

Maximum Inactivity Time Unit

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

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

Allow Local Login for Partition Administrators

While this setting applies to partition administrators that utilize Single Sign-On for SAML 2.0, it is not required for Cisco IDS to function. See "Single Sign-On" on page 152 for more information.

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

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

User Session Settings

Inactive Time Out (Minutes)

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

- Type: Partition settings group
- Subtype: Security
- Data type: Integer
- Default value: 30
- Minimum: 5
- Maximum: 1440

Session Time Out (Minutes)

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

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

Business Calendar Settings

Business Calendar Timezone

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

- Type: Department settings group
- Subtype: General
- Data type: Enumeration
- Default value: (GMT-05:00)Eastern Standard Time (US and Canada)

- Value options:

  (GMT-12:00) Eniwetok, Kwajalein

  (GMT-11:00) Midway Island, Samoa

  (GMT-10:00) Hawaii

  (GMT-09:00) Alaska-Standard

  (GMT-08:00) Alaska-Daylight

  (GMT-08:00) Pacific Standard Time (US & Canada)

  (GMT-07:00) Pacific Daylight Time (US & Canada)

  (GMT-07:00) Arizona

  (GMT-07:00) Mountain Standard Time (US & Canada)

  (GMT-06:00) Mountain Daylight Time (US & Canada)

  (GMT-06:00) Central America

  (GMT-06:00) Central Standard Time (US & Canada)

  (GMT-05:00) Central Daylight Time (US & Canada)

  (GMT-06:00) Mexico City-Standard

  (GMT-05:00) Mexico City-Daylight

  (GMT-06:00) Saskatchewan

  (GMT-05:00) Bogota, Lima, Quito

  (GMT-05:00) Eastern Standard Time (US & Canada)

  (GMT-04:00) Eastern Daylight Time (US & Canada)

  (GMT-05:00) Indiana (East)

  (GMT-04:00) Atlantic Standard Time (Canada)

  (GMT-03:00) Atlantic Daylight Time (Canada)

  (GMT-04:00) Caracas, La Paz

  (GMT-04:00) Santiago-Standard

  (GMT-03:00) Santiago-Daylight

  (GMT-03:30) Newfoundland-Standard

  (GMT-02:30) Newfoundland-Daylight

  (GMT-03:00) Brasilia-Standard

  (GMT-02:00) Brasilia-Daylight

  (GMT-03:00) Buenos Aires, Georgetown

  (GMT-03:00) Greenland-Standard

  (GMT-02:00) Greenland-Daylight

  (GMT-02:00) Mid-Atlantic Standard Time

(GMT-01:00) Mid-Atlantic Daylight Time

(GMT-01:00) Azores-Standard

(GMT) Azores-Daylight

(GMT-01:00) Cape Verde Is.

(GMT) Monorovia, Casablanca

(GMT) Greenwich Mean Time; Dublin, Edinburgh, London-Standard

(GMT+01:00) Dublin, Edinburgh, London-Daylight

(GMT+02:00) Dublin, Edinburgh, London-Double Summer

(GMT+01:00) Berlin, Stockholm, Rome, Bern, Vienna, Amsterdam-Standard

(GMT+02:00) Berlin, Stockholm, Rome, Bern, Vienna, Amsterdam-
Daylight

(GMT+01:00) Prague, Belgrade, Bratislava, Ljubljana, Budapest-Standard

(GMT+02:00) Prague, Belgrade, Bratislava, Ljubljana, Budapest-Daylight

(GMT+01:00) Paris, Madrid, Brussels, Copenhagen-Standard

(GMT+02:00) Paris, Madrid, Brussels, Copenhagen-Daylight

(GMT+01:00) Lisbon, Warsaw, Sarajevo, Sofija, Skopje, Vilnius, Zagreb-Standard

(GMT+02:00) Lisbon, Warsaw, Sarajevo, Sofija, Skopje, Vilnius, Zagreb-Daylight

(GMT+01:00) West Central Africa

(GMT+02:00) Athens, Istanbul, Minsk-Standard

(GMT+03:00) Athens, Istanbul, Minsk-Daylight

(GMT+02:00) Bucharest-Standard

(GMT+02:00) Bucharest-Daylight

(GMT+02:00) Cairo-Standard

(GMT+03:00) Cairo-Daylight

(GMT+02:00) Harare, Pretoria

(GMT+02:00) Helsinki, Riga, Tallinn-Standard

(GMT+03:00) Helsinki, Riga, Tallinn-Daylight

(GMT+02:00) Israel

(GMT+03:00) Baghdad-Standard

(GMT+04:00) Baghdad-Daylight

(GMT+03:00) Kuwait, Nairobi, Riyadh

(GMT+03:00) Moscow, St. Petersburg-Standard

(GMT+04:00) Moscow, St. Petersburg-Daylight

(GMT+03:30) Tehran-Standard

(GMT+04:30) Tehran-Daylight

(GMT+04:00) Abu Dhabi, Muscat

(GMT+04:00) Baku, Tbilisi, Yerevan-Standard

(GMT+05:00) Baku, Tbilisi, Yerevan-Daylight

(GMT+04:30) Kabul

(GMT+05:00) Ekaterinburg-Standard

(GMT+06:00) Ekaterinburg-Daylight

(GMT+05:00) Islamabad, Karachi, Tashkent

(GMT+05:30) Bombay, Calcutta, Madras, New Delhi, Colombo

(GMT+05:45) Kathmandu

(GMT+06:00) Almaty, Novosibirsk-Standard

(GMT+06:00) Almaty, Novosibirsk-Daylight

(GMT+06:00) Astana, Dhaka, Sri Jayawardenepura

(GMT+06:00) Rangoon

(GMT+07:00) Bangkok, Jakarta, Hanoi

(GMT+07:00) Krasnoyarsk

(GMT+08:00) Beijing, Hong Kong, Chongqing, Urumqi

(GMT+08:00) Irkutsk, Ulaan Bataar

(GMT+08:00) Kuala Lumpur, Perth, Singapore, Taipei

(GMT+09:00) Tokyo, Osaka, Sapporo, Seoul

(GMT+09:00) Yakutsk

(GMT+09:30) Adelaide-Standard

(GMT+10:30) Adelaide-Daylight

(GMT+09:30) Darwin

(GMT+10:00) Brisbane

(GMT+10:00) Canberra, Melbourne, Sydney-Standard

(GMT+11:00) Canberra, Melbourne, Sydney-Daylight

(GMT+10:00) Guam, Port Moresby

(GMT+10:00) Hobart-Standard

(GMT+11:00) Hobart-Daylight

(GMT+10:00) Vladivostok

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

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

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

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

(GMT+13:00) Tonga

- Can be reset at lower level: No

Customer Information Settings

Customer Departmentalization

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

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

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

Incoming Email Settings

Number of Emails to Retrieve

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

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

Maximum Email Size for Retriever (MB)

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

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

Maximum Body Size for Retriever (KB)

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

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

Message Note for Large Body

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

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

Action for Large Email

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

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

Parse Date in Email Header

When this setting is enabled, the Retriever Service gets the "Receive date" or "Send date" from the email header and stores the date in the email tables in the database. If the setting is disabled, the retriever stores the date when the activity for the email was created in the system.

- Type: Partition settings group
- Subtype: Email retriever
- Data type: Enumeration
- Default value: No
- Value options:
  - **No**: The Retriever Service stores the activity creation date in the email tables.
  - **Yes**: The Retriever Service stores the "Receive date" or "Send date" in the email table.

Exception Email Settings

Exception emails are the emails which the Retriever Service fails to parse or store in the database.

Action On Exception Emails

Use this setting to decide what the Retriever Service should do with the emails it was unable to retrieve (such as, emails that could not be parsed, emails that could not be inserted in the database, etc.).

- Type: Partition settings group
- Subtype: Email retriever
- Data type: Enumeration
- Default value: Redirect and write to file
- Value options:

- Delete: Emails are deleted.
- Write to file: Emails are saved in the *Cisco_Home*\eService\storage\1\mail\Exception Emails\RxExcepEmails.txt file. The size of this file is defined in the "Exception mail maximum file size (megabyte)" setting.
- Redirect and write to file: Emails are redirected to another email address configured in the "Exception mail redirection to address" settings and they are also saved in the *Cisco_Home*\eService\storage\1\mail\Exception Emails\RxExcepEmails.txt file. The size of this file is defined in the "Exception mail maximum file size (megabyte)" setting.

Exception Mail Redirection From Address

Use this setting to specify the email address displayed in the "from" field of the redirected exception emails.

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

Exception Mail Redirection To Address

Use this setting to specify the email address to which the redirected exception emails should be sent.

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

Exception Mails Auto Bcc

Provide the email address to which the Bcc copy of the exception email should be sent.

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

SMTP Flag

If the value selected in the “Default SMTP Protocol” setting is “ESMTP”, this setting needs to be configured to decide if the SMTP protocol should be used if the authentication fails.

- Type: Partition settings group
- Subtype: Email dispatcher-Mail
- Data type: Enumeration
- Default value: Never
- Value options:
  - Never: The switch to SMTP protocol (if ESMTP authentication fails) is not allowed.
  - If authentication fails: The switch to SMTP protocol (if ESMTP protocol fails) is allowed if the ESMTP authentication fails.

Outgoing Email Settings

Maximum Body Size for Dispatcher (KB)

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

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

Maximum Email Size for Dispatcher (MB)

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

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

- Type: Partition settings group
- Subtype: Email dispatcher - Common
- Data type: Integer
- Default value: 25
- Minimum value: 16
- Maximum value: 150

To: Address for Notifications From Services

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

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

From: Address for Notifications From Services

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

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

Notification Settings for the Retriever Service

Notification emails are sent to administrators when the Retriever Service is unable to retrieve emails because of some errors, including:

- Retriever fails to parse emails

- Retriever fails to insert emails in the database
- Retriever fails to connect to the Mail Server
- Retriever fails to retrieve attachments

Configure the settings described in this section to send out notifications to administrators.

The address to which these notifications are sent, is specified in the “To: address for notifications from services” setting and the from email address is specified in the “From: address for notifications from services” setting.

Notification Mails Auto Bcc

Provide the email address to which the Bcc copy of the notification email should be sent to.

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

Notification Mail Dispatching SMTP Preference

To be able to send notification emails out of the system, you need to configure the various properties of the mail server to be used to send the emails. The properties are configured through a group of settings (called the SMTP preferences). In this setting, specify the set of SMTP preferences to be used for sending notification emails. If you do not specify a value in this setting, the “Default SMTP preferences” are used to send out the notification emails.

The SMTP preference set includes the following settings: Notification mails SMTP server, Notification mails SMTP protocol, Notification mails SMTP port, SMTP Flag, Notification mails SMTP user name, and Notification mails SMTP password.

You can choose to use the “Default SMTP preferences” to send out the notification emails. If you want to do that, do not set any values in the settings that are part of the notification SMTP preferences and the system will automatically use the “Default SMTP preferences” to send out the notification emails.

- Type: Partition settings group
- Subtype: Email retriever
- Data type: String
- Default value: Mail.NotificationEmails
- Minimum value: 0
- Maximum value: 255

Notification Mails SMTP Server

In this setting provide the name of the outgoing server to be used to send out notification emails.

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

Notification Mails SMTP Protocol

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

- Type: Partition settings group
- Subtype: Email dispatcher-Mail
- Data type: Enumeration
- Default value: SMTP
- Value options: SMTP, ESMTP

Notification Mails SMTP Port

In this setting provide the port of the outgoing server.

- Type: Partition settings group
- Subtype: Email dispatcher-Mail
- Data type: Integer
- Default value: 25
- Value options: —

SMTP Flag

If the value selected in the “Default SMTP Protocol” setting is “ESMTP”, this setting needs to be configured to decide if the SMTP protocol should be used if the authentication fails.

- Type: Partition settings group
- Subtype: Email dispatcher-Mail
- Data type: Enumeration
- Default value: Never
- Value options:
    - Never: The switch to SMTP protocol (if ESMTP authentication fails) is not allowed.
    - If authentication fails: The switch to SMTP protocol (if ESMTP protocol fails) is allowed if the ESMTP authentication fails.

Notification Mails SMTP User Name

If the value selected in the “Default SMTP Protocol” setting is “ESMTP”, provide the user name to be used to connect to the mail server.

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

Notification Mails SMTP Password

If the value selected in the “Default SMTP Protocol” setting is “ESMTP”, provide the password to be used to connect to the mail server.

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

Notification Email Settings

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

Also, notification emails are sent to administrators to notify about various conditions in the system (specifically services) that need attention. The address to which these notifications are sent, is specified in the “To: address for notifications from services” setting and the from email address is specified in the “From: address for notifications from services” setting.

The settings described in this section are not used for the Retriever Service as this service has its own separate set of settings for sending notifications. For more details, see “Notification Settings for the Retriever Service” on page 66.

Default SMTP Server

In this setting provide the name of the outgoing server.

- Type: Partition settings group

- Subtype: Email dispatcher - Generic
- Data type: String
- Default value: —
- Minimum value: 0
- Maximum value: 256

Default SMTP Protocol

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

- Type: Partition settings group
- Subtype: Email dispatcher - Generic
- Data type: Enumeration
- Default value: SMTP
- Value options: SMTP, ESMTP

Default SMTP Port

In this setting provide the port of the outgoing server. The value of the setting cannot be changed from the UI.

- Type: Partition settings group
- Subtype: Email dispatcher - Generic
- Data type: String
- Default value: 25
- Value options: —

SMTP Flag

If the “Default SMTP Protocol” setting is set as “ESMTP” this setting needs to be configured to decide if the SMTP protocol should be used if the authentication fails.

- Type: Partition settings group
- Subtype: Email dispatcher - Generic
- Data type: Enumeration
- Default value: Never
- Value options:
  - Never: The switch to SMTP protocol (if ESMTP authentication fails) is not allowed.
  - If authentication fails: The switch to SMTP protocol (if ESMTP protocol fails) is allowed if the ESMTP authentication fails.

Default SMTP User Name

If the "Default SMTP Protocol" setting is set as "ESMTP", provide the user name to be used to connect to the mail server.

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

Default SMTP Password

If the "Default SMTP Protocol" setting is set as "ESMTP", provide the password to be used to connect to the mail server.

- Type: Partition settings group
- Subtype: Email dispatcher - Generic
- Data type: Encrypted
- Default value: —
- Minimum value: 0
- Maximum value: 255

Blocked Attachments Settings

Email - Criteria for blocking attachments

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

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

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

Block All Attachments

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

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

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

Action on Blocked Attachments

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

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

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

Workflow Settings

From Email Address for Alarm

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

- Type: Department settings group
- Subtype: Common

- Data type: String
- Default value: —
- Minimum value: 0
- Maximum value: 255
- Can be reset at lower level: No

Include Original Message for Auto Acknowledgement 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.

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

Auto Response Number

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

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

Auto Response Time

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

- Type: Partition settings group
- Subtype: Workflow engine

- Data type: Integer
- Default value: 1440
- Minimum value: 360
- Maximum value: 1440

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

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

- **Do not change:** The original email address set in the From field is retained.
- **Use default alias of destination department:** The From email address is set to the default alias configured for the department. Make sure that a default alias is configured for the department.
- **Force agents to select “From” email address:** The value of the “From” field is reset to “Please select an email address” and agents are required to pick the From address while sending out the email.

- Type: Department setting group
- Subtype: Activity
- Data type: Enumeration
- Default value: Do not change
- Value options: Do not change, Use default alias of destination department, Force agents to select “From” email address
- Can be reset at lower level: No

Activity Assignment Settings

Personalized Activity Assignment Settings

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

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

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

Personalized Activity Assignment

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

- Type: Department settings group
- Subtype: Queue
- Data type: Enumeration
- Default value: Logged in
- Value options:
  - **Logged in:** Activities are assigned to the agent only when the agent is logged in to the application and is available for emails (Availability options in agent inbox are selected).
  - **Always:** Activities are always assigned to the agent whether the agent is logged in or not.
  - **Disable:** Personalized activity assignment is disabled.
- Can be reset at lower level: No

Enable Personalized Activity Assignment for Forwarded Emails

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

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

Enable Personalized Activity Assignment for Foreign Users

Use this setting to enable personalized activity assignment feature for foreign users in a department.

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

Enable Autopushback

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

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

Autopushback Time (Minutes After Logout)

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

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

Activity Type for Autopushback

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

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

- Both new and incomplete activities: All the activities will be pushed back to the queues.

- Can be reset at lower level: Yes

Activities to Pull First

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

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

Maximum Activities to Display for Pull

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

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

Maximum Activities to Pull at a Time

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

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

Monitor Settings

Common Settings for Monitors

Refresh Interval (Seconds)

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

- Type: Department settings group, User settings group
- Subtype: Monitoring
- Data type: Integer
- Default value: 30
- Minimum value: 10
- Maximum value: 6000
- Can be reset at lower level: Yes

Number of Activities to be Monitored for Service Level

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

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

Chat - SLA for Response Time (Seconds)

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

- Type: Department settings group

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

Chat - Daily Service Level Sample Set Definition

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

- Type: Department settings group
- Subtype: Monitoring
- Data type: Enumeration
- Default value: All chats handled including abandoned
- Value options: All chats handled including abandoned, All chats handled excluding abandoned
- Can be reset at lower level: No

Notification Settings for System Monitors

Use these settings to send out notifications for the monitors configured in the system partition. These settings are available in the Administration Console of the system partition.

Default SMTP Server

Use this setting to specify the outgoing server to be used for sending out notifications for monitors configured in the system partition.

- Type: Partition settings group
- Subtype: Email dispatcher - Generic
- Data type: String
- Default value: —
- Minimum value: 0
- Maximum value: 256

Default SMTP Protocol

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

- Type: Partition settings group

- Subtype: Email dispatcher - Generic
- Data type: Enumeration
- Default value: SMTP
- Value options: SMTP, ESMTP

Default SMTP Port

In this setting provide the port of the outgoing server. The value of the setting cannot be changed from the UI.

- Type: Partition settings group
- Subtype: Email dispatcher - Generic
- Data type: String
- Default value: 25
- Value options: —

SMTP Flag

If the value selected in the “Default SMTP Protocol” setting is “ESMTP”, this setting needs to be configured to decide if the SMTP protocol should be used if the authentication fails.

- Type: Partition settings group
- Subtype: Email dispatcher - Generic
- Data type: Enumeration
- Default value: Never
- Value options:
  - Never: The switch to SMTP protocol (if ESMTP authentication fails) is not allowed.
  - If authentication fails: The switch to SMTP protocol (if ESMTP protocol fails) is allowed if the ESMTP authentication fails.

Default SMTP User Name

If the value selected in the “Default SMTP Protocol” setting is “ESMTP”, provide the user name to be used to connect to the mail server.

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

Default SMTP Password

If the value selected in the "Default SMTP Protocol" setting is "ESMTP", provide the password to be used to connect to the mail server.

- Type: Partition settings group
- Subtype: Email dispatcher - Generic
- Data type: Encrypted
- Default value: —
- Minimum value: 0
- Maximum value: 255

Activity Handling Settings

Common Settings for Activities

Alert Agent When Activity Is Assigned

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

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

Send Agent an Email When Activity Is Assigned

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

- Type: Department settings group, User settings group
- Subtype: Common

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

Alert Subject

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

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

Alert Body

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

- Type: Department settings group
- Subtype: Common
- Data type: String
- Default value: You have received a new activity (id = ``activity_id) from customer identified by ``contact_point_data
- Value options: —
- Can be reset at lower level: No

Force Activity Categorization

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

- Type: Department settings group
- Subtype: Activity

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

Force Resolution Code

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

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

Email Activity Settings

Include Message Header in Reply

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

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

Add Contact Point on Compose

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

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

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

Language Detection Threshold (KB)

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

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

Service Email and Phone Activities at the Same Time

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

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

Service Email and Chat Activities at the Same Time

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

- Type: Department settings group
- Subtype: Activity
- Data type: Enumeration
- Default value: No

- Value options:
  - **Yes:** Agents can continue to respond to email activities that are already assigned to them. The Send and Send and Complete buttons are enabled for emails. However, no new emails get assigned to agents while they are in a chat session. If agents are associated with an outbound MRD, they can create outbound emails while they are in a chat session.
  - **No:** Agents cannot respond to email activities that are already assigned to them. The Send and Send and Complete buttons are disabled for emails. Also, no new emails get assigned to agents while they are in a chat session. Agents cannot create outbound emails while they are in a chat session.
- Can be reset at lower level: No

Chat Activity Settings

Chat - Force Activity Categorization

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

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

Chat - Force Resolution Code

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

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

Inbox Settings

Common Settings for Inboxes

Number of Activities Per Page

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

- Type: Department settings group, User settings group
- Subtype: Activity
- Data type: Long
- Default value: 20
- Minimum value: 0
- Maximum value: —
- Can be reset at lower level: Yes

Agent Inbox Preference

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

- Type: Department settings group, User settings group
- Subtype: General
- Data type: Enumeration
- Default value: Chat
- Value options: Chat, Main
- Can be reset at lower level: Yes

Main Inbox Settings

Inbox Sort Column

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

- Type: Department settings group, User settings group
- Subtype: Activity
- Data type: Enumeration

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

Inbox Sort Order

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

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

Email - Enable Sound Alert

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

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

Chat Inbox Settings

Chat - Inbox Sort Column

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

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

- Type: Department settings group, User settings group

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

Chat - Inbox Sort Order

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

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

Chat Supervisor Inbox Settings

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.

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

Spelling and Blocked Words Settings

Preferred Dictionary of the User

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

- Type: Department settings group, User settings group
- Subtype: Spell checker
- Data type: String
- Default value: —
- Value options: Danish Dictionary, Swedish Dictionary, Finnish Dictionary, Norwegian (Bokmaal) Dictionary, Italian Dictionary, Dutch Dictionary, Portuguese Dictionary, French Dictionary, Spanish Dictionary, German Dictionary, English (UK) Dictionary, English (US) Dictionary

Auto Spellcheck

Use this setting to enable automatic spell check for emails, tasks, etc. This setting is not used for chat activities. For chat, use the Chat - Auto Spellcheck setting.

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

Chat - Auto Spellcheck

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

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

Auto Blockcheck

Use this setting to check the content of emails, tasks, etc for blocked words. This setting is not used for chat activities. For chat, use the Chat - Auto Blockcheck setting. The list of blocked words is set from the Dictionaries node in the Administration Console. For details, see "Adding Blocked Words" on page 189.

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

Chat - Auto Blockcheck

Use this setting to check the chat messages for blocked words. The list of blocked words is set from the Dictionaries node in the Administration Console. For details, see "Adding Blocked Words" on page 189.

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

Include Original Message Text During Spell Check

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

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

Ignore Words With Only Upper Case Letters

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

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

Ignore Words With a Mixture of Upper and Lower Case Letters

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

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

Ignore Words With Only Numbers or Special Characters

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

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

Ignore Words That Contain Numbers

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

- Type: Department settings group, User settings group
- Subtype: Spell checker

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

Ignore Web Addresses and File Names

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

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

Split Contracted Words

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

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

Search Settings

Maximum Number of Records to Display for Search

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

- Type: Partition settings group

- Subtype: Common
- Data type: Integer
- Default value: 100
- Minimum value: 10
- Maximum value: 5000

Maximum Number of Records to Display for NAS Search

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

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

Knowledge Base Settings

KB Primary Language

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

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

Custom Language Label

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

- Type: Department settings group

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

Chat Settings

Chat Auto-Pushback Settings

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

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

Enable Auto-Pushback of Chats

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

Type: Partition settings group

Subtype: Chat

Data type: Enumeration

Default value: Yes

Value options: Yes, No

Expiry Time for Auto-Pushback for Chats (Minutes)

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

- Type: Partition settings group
- Subtype: Chat
- Data type: Integer
- Default value: 2
- Minimum value: 2

- Maximum value: 30

Make Agent Unavailable on Auto-Pushback of Chats

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

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

Chat Agent Session Settings

Chat - Agent Chat Message Maximum Length

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

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

Show Smiley in Agent Chat Toolbar

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

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

Chat - Display Timestamp in Agent Chat Console

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

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

Chat - Display Timestamp in Completed Chat Transcript

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

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

Chat - Customer Offline Interval

In this setting configure the time interval (in seconds) at which a check is made to see if the customer is connected to the chat session. If the customer is disconnected, the customer connection status in the Agent Console is changed to “Disconnected”. When this setting is left blank, no check is done.

- Type: Department settings group
- Subtype: Activity
- Data type: Integer
- Default value: 10
- Minimum value: 2
- Maximum value: 30
- Can be reset at lower level: No

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

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

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

Chat - Enable Sound Alert

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

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

Reason for Chat Transfer

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

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

4 Users

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

About Users, Groups, Roles, and Actions

Users

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

Users operate at three levels:

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

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

Two users are created during the installation:

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

User Groups

User groups are a collection of users that share similar functions or roles in the system. Groups make it much easier to manage user accounts. User groups cannot be created manually in ECE, they can only be created by importing skill groups. To learn more about importing skill groups, see "Importing Skill Groups" on page 35.

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

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

User Roles

A role is nothing but a set of permissible actions for various business resources. An agent's role, for instance, would include actions such as "View Agent Console," "Edit customer," and "Add notes." The system comes with some default user roles and templates for roles. You can assign one or more roles to a group of users or an individual user.

The default user roles are:

- **Administrator:** The administrator is the manager of the department, and has access to the Administration console. You will find that there are two types of administrators that the system allows you to create; Partition Administrator and Department Administrator. Let us see the difference between these two roles. A partition administrator has to be created while installing the application, but additional partition administrators can be created later. The partition administrator is responsible for both her partition and for the departments contained within her partition. To know more about the role of a partition administrator, see "Partition Administrator" on page 104.

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

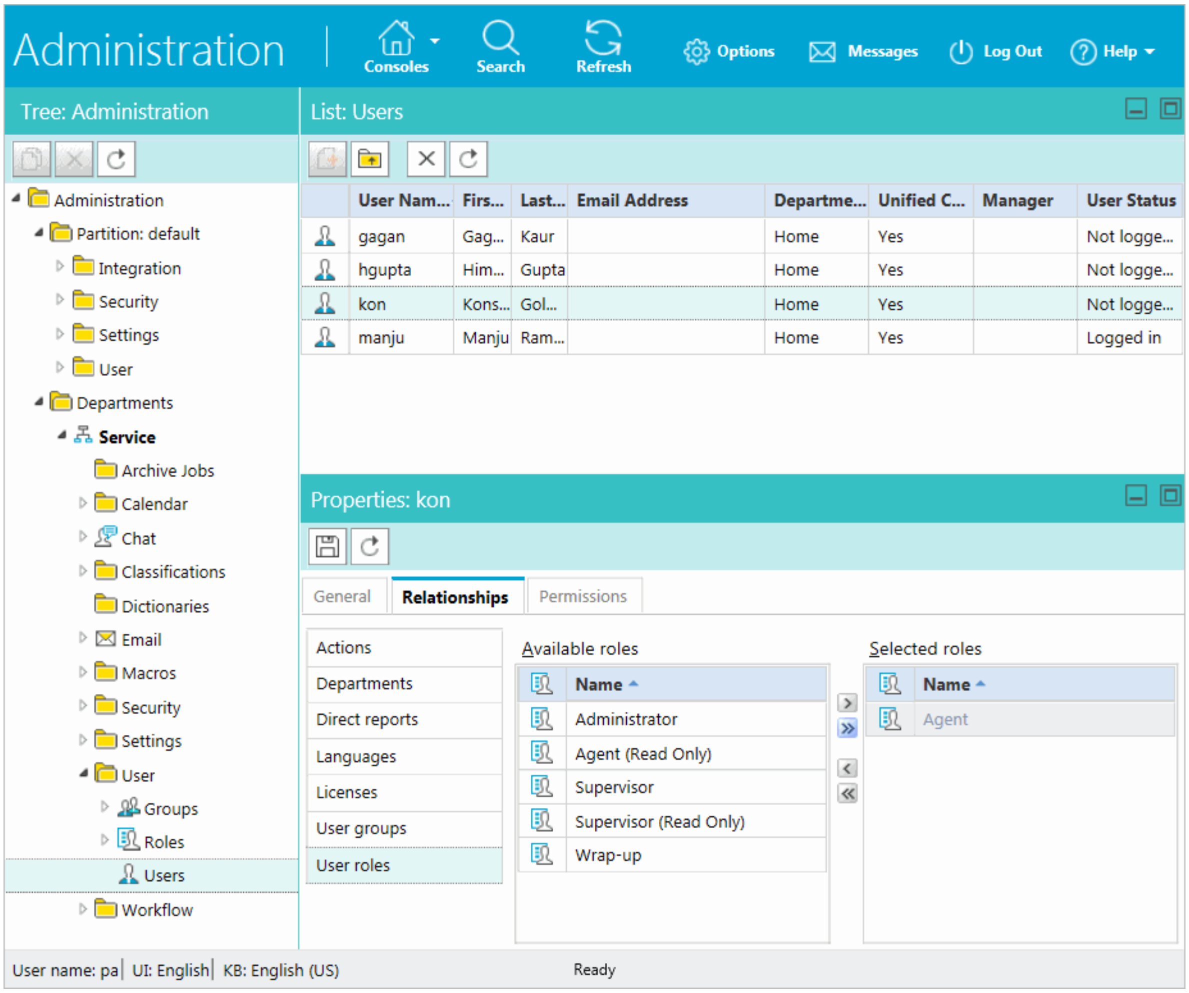
- **Agent:** An agent is a person who handles customer queries, who is directly in contact with the customer. He has access to the Agent console. Agents are imported into the system by the partition administrator from Unified CCE.

- **Agent (Read Only):** An agent (read only) will have access to the Agent console, but he will not be able to compose replies for the customer queries. He can only view them. This role can be assigned to trainees.

- **Supervisor:** A supervisor has access to the Supervision Console, and creates monitors for queues, user groups, and users in a department. They can also create and run reports from the Reports Console.

- **Supervisor (Read Only):** A user with the supervisor (read only) role can create and run monitors. Such a user cannot create reports, but can run the reports for which the user has view and run permissions.

- **Wrap-up:** Along with the agent role, assign the wrap-up role to users or user groups that are mapped to agents and skill groups of Unified CCE. Agents with this role go in wrap-up mode after they send and complete an activity. After completing the wrap-up tasks, agents click the **End Wrap-up** button to complete the activity and change their mode to available.



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

Available roles

Name
Administrator
Agent (Read Only)
Supervisor
Supervisor (Read Only)
Wrap-up

Selected roles

Name
Agent

User name: pa | UI: English | KB: English (US) Ready

Selecting user roles

Actions

When selecting a role for a users, you must consider the work that the person with that role can handle. Actions define this work. All default user roles have already been assigned certain actions. You can view these actions by clicking on any role and you can use these actions to create new roles.

Permissions

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

Important Things to Note About Picking and Pulling Activities

- **Emails:** Agents can pick emails from agents and queues that belong to the same MRD. For agents who belong to a Skill Group, MRD is identified by the mapping between Skill Group and MRD. For agents who are part of a Precision Queue (PQ), the MRD is identified by the Attributes assigned to that agent and the mapping between PQ and Attributes that are used in the PQ routing steps. **Agents with Supervisor Role** can pick from the from the supervisory queue for the MRD to which they belong to. Additionally, **Agents with Administrator Role** can pick from the default exception queue and from the supervisory queue for the MRD to which they belong to.
- **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 Activities

- **Emails:** Agents can transfer incoming emails to agents and queues that belong to the same MRD. For agents who belong to a Skill Group, the MRD is identified by the mapping between Skill Group and MRD. For agents who are part of a Precision Queue (PQ), the MRD is identified by the Attributes assigned to that agent and the mapping between PQ and Attributes that are used in the PQ routing steps. However, outbound emails created by agents can only be transferred to users and not to queues. There is no transfer to department 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. 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.
- **Chats:** Agents can transfer chats to queues and agents that belong to the same MRD. For agents who belong to a Skill Group, the MRD is identified by the mapping between Skill Group and MRD. For agents who are part of a Precision Queue (PQ), the MRD is identified by the Attributes assigned to that agent and the mapping between PQ and Attributes that are used in the PQ routing steps. They cannot transfer to departments. To be able to transfer a chat to an agent, the agent must be logged in to the application and should not have met the concurrent task limit. If these requirements are not met, the agent is not displayed in the Transfer Activities window. To be able to transfer to a queue, an agent who belongs to that queue's MRD must be logged in and ready.

What are the Actions Assigned to the Default Roles?

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

System Administrator

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

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

Actions assigned to the System Administrator role

Partition Administrator

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

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

Actions assigned to the Partition Administrator role

Administrator

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

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

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

Actions assigned to the Administrator role

Agent

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

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

Actions assigned to the Agent role

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

Resource Name	Actions Permitted	Description
Activity	Create	Enables the **New Activity** button in the Main Inbox toolbar.
	Complete	Enables the **Complete** button in the Reply pane toolbar when working on email activities, custom activities, or tasks. Also enables the **Send & Complete** button in the Reply pane toolbar if the **Send Email** action is also assigned to the agent.
	Pin	Enables the **Pin/Unpin** button in the in the Main Inbox toolbar.
	Unpin	Allows an agent to pull the pinned activities from other agents.
	Pull Next Activities	Enables the **Pull** button in the Main Inbox toolbar. To be able to pull activities using this button, the agent needs: ▸ **Pull Activities** action for routing queues. ▸ **Pull Activities** permission on queues. For chats, the following action is also required: ▸ **Pull Next Chat Activity** action for chats.
	Pull Selected Activities	Enables the **Pick** button in the Main Inbox toolbar. To be able to pull activities (other than chats) using this button, an agent needs: ▸ **Pull Activities** action for routing queues. ▸ **Pull Activities** action for users. ▸ **Pull Activities** permission on queues. ▸ **Pull Activities** permission on users.
	Transfer Activities	Enables the **Transfer** button in the Main Inbox toolbar, the Chat Inbox toolbar, and the Reply pane toolbar. To be able to transfer activities using this button, an agent needs: ▸ **Transfer Activities** action for routing queues. ▸ **Transfer Activities** action for users. ▸ **Transfer Activities** permission on queues. ▸ **Transfer Activities** permission on users.
	Assign Classification	Enables the **Save** button in the Classify section of the Information pane, so that agents can assign categories and resolution codes to activities.
Case	Edit	Allows an agent to edit the case details. Enables the **Save** button in the Information pane, Case section. The **Case status** field is enabled only if the agent has the **Close Case** action.
	Close Case	Allows an agent to close an open case. It enables the **Close Case** button in the Inbox pane toolbar (Inbox Tree pane > My Work > Cases > My Cases > Open). If the agent has the **Edit case** action, it also enables the **Case status** field in the Information pane, Case section.
	Change Case	Allows an agent to change the case of an activity and associate it with an existing case. It enables the **Change Case** button in the Information pane, Case section.
	Create Case	Allows an agent to create new cases. When a new case is created, the old case associated with the activity is closed and the activity is associated with the new case. It enables the **Create Case** button in the Information pane, Case section.

Resource Name	Actions Permitted	Description
Chat	Complete Chat Activity	Enables the **Complete** button in the Chat pane toolbar.
	Leave Chat Activity	Enables the **Leave** button in the Chat pane toolbar. Allows an agent to leave a chat without completing the activity. The activity gets completed only when the customer closes the chat session.
	Pull Next Chat Activity	Enables the **Pull** button. Allows an agent to pull chat activities from queues. To be able to pull chat activities the agent also needs: ▸ **Pull Next Activities** action for activities ▸ **Pull Activities** action for routing queues ▸ **Pull Activities** permission on queues
	Transfer Chat Activity	Enables the **Transfer** button in the Chat pane toolbar. Allows an agent to transfer chats to other agents, queues, and departments. To be able to transfer chats using this button, the agent needs: ▸ **Transfer Activities** action for routing queues ▸ **Transfer Activities** action for users ▸ **Transfer Activities** permission on queues ▸ **Transfer Activities** permission on users

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

Resource Name	**Actions Permitted**	**Description**
Filter Folder	Create	Enables the **New** and **Properties** buttons in the Inbox Tree pane toolbar. Using these buttons, agents can create and edit search folders and personal folders in their inbox.
	Delete	Enables the **Delete** button in the Inbox Tree pane toolbar. Using this button, agents can delete search folders and personal folders from their inbox.
KB Folder	View Folder	Agents can only view articles in the folders on which they have the **View Folder** permission. All agents have permissions to view articles in the following standard folders and it cannot be removed - headers, footers, greetings, signatures, quick links, and quick responses. But, if any folders are created under these standard folders, then administrators can select not to give **View Folder** permission on those folders.
	Add Notes	Allows agents to view, delete, and add notes. It enables the **Notes** button.
Macro	View	Allows agents to view and use macros in emails, chats, tasks, and custom activities. It enables the **Add macro** button in the reply pane.
Notes	View	Allows an agent to view notes associated with cases, activities, customers, and customer associations. It displays the **View notes** option in the Notes window, which can be accessed using the **Notes** button from the following panes: ▸ Main Inbox toolbar ▸ Chat Inbox toolbar ▸ Reply pane ▸ Chat pane ▸ Information pane, in the following sections: Activity, Case, History, and Customer.
	Add	Allows an agent to add notes to cases, activities, customers, and customer associations. It displays the **Add notes** option in the Notes window, which can be accessed using the **Notes** button from the following panes: ▸ Main Inbox ▸ Chat Inbox ▸ Reply pane ▸ Chat pane ▸ Information pane, in the following sections: Activity, Case, History, and Customer. If an agent has the **View Notes** action, it also enables the **Add** button in the Notes window. It displays the **Add notes** option in the Notes window, which can be accessed using the **Notes** button from the following panes: ▸ Main Inbox ▸ Chat Inbox ▸ Reply pane ▸ Chat pane ▸ Information pane, in the following sections: Activity, Case, History, and Customer.
	Delete	Allows an agent to delete the notes associated with cases, activities, customers, and customer associations. It enables the **Delete button** in the Notes window. The Notes window can be accessed using the **Notes** button from the following panes: ▸ Main Inbox ▸ Chat Inbox ▸ Reply pane ▸ Chat pane ▸ Information pane, in the following sections: Activity, Case, History, and Customer. The Notes window can only be accessed by agents with the **View Notes** action.

Resource Name	Actions Permitted	Description
Routing Queue	Pull Activities	Allows agents to pull activities from routing queues. To be able to pull activities from queues, an agent needs: ▸ **Pull Next Activities** or **Pull Selected Activities** action for activities ▸ **Pull Activities** permission on routing queues For chats, the following action is also required: ▸ **Pull Next Chat Activity** action for chats
	Transfer Activities	Allows agents to transfer activities to routing queues. To be able to transfer activities to queues, an agent needs: ▸ **Transfer Activities** action for activities ▸ **Transfer Activities** permission on queues
System Resource	View Agent Console	Allows an agent to access the Agent Console.
User	Pull Activities	Allows agents to pull activities from other agents. To be able to pull activities from other agents, an agent needs: ▸ **Pull Selected Activities** action for activities ▸ **Pull Activities** permission on users
	Transfer Activities	Allows agents to transfer activities to other agents. To be able to transfer activities to other agents, an agent needs: ▸ **Transfer Activities** action for activities ▸ **Transfer Activities** permission on users

Some important actions assigned to the Agent role

Agent (Read Only)

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

Resource Name	Actions Permitted
Agent Console	View
User	View
Category	View
Customer	View
Filter Folder	Create, Delete
Notes	View
KB Folder	View
Product Catalog	View
Resolution Codes	View
Macro	View
Activity	Print
Case	Print
Queue	View

Actions assigned to the Agent (read only) role

Supervisor

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

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

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

Actions assigned to the Supervisor role

Supervisor (Read Only)

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

Resource Names	Actions Permitted
Supervision Console	View
Agent Console	View
Reporting Console	View
User	View
Customer	View
Association	View
Aliases	View
Blocked Address	View
Blocked File Extension	View
Chat Entry Point	Create, View, Edit, Delete
Chat Template Set	Create, View, Edit, Delete
Inbox Folder	Create, Delete
Delivery Exceptions	View
Categories	View
Filter Folder	View
Notes	View
Product Catalog	View
Resolution Codes	View
KB Folder	View
Macro	View
Activity	Print
Case	Print
Monitor	Create, Edit, Delete, Run
Reports	View, Run
Queue	View

Actions assigned to the Supervisor (read only) role

Wrap-up

The various actions assigned to the Wrap-up role are listed in the following table.

Resource Names	Actions Permitted
Activity	Wrap Email Activity
Chat	Wrap Chat Activity

Action assigned to the Wrap-up role

Restoring User Roles

Important: **Additional user roles cannot be created in ECE.**

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

To restore a role:

1. In the Tree pane, browse to the Users node. Based on where you want to restore a user role, do one of the following:
   - If you are a system administrator, go to the system partition and browse to **Administrator > Partition:** *Context_Root_Name* **> User > Roles.**
   - If you are a partition administrator, go to the business partition and browse to **Administrator > Partition:** *Partition_Name* **> User > Roles.**
   - If you are a department administrator, browse to **Administration > Departments >** *Department_Name* **> User > Roles.**
2. In the List pane, select the role you want to restore to its default state.
3. In the Properties pane toolbar, click the **Restore Defaults** button.

Managing User Groups

User groups are created in the system by importing skill groups from Unified CCE to the application. New user groups cannot be manually created within the application. If you wish to remove the user groups from the application you can delete it, however, the user group can be created once again by importing the corresponding skill group. If an ECE user group is mapped to a Unified CCE skill group, and the Unified CCE skill group is deleted, when the ECE user group is clicked, a warning appears indicating that the user group will be unmapped in ECE. To learn more about importing skill groups, see "Importing Data" on page 33.

Deleting User Groups

To delete a user group:

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

Managing Users

System and partition administrators are created in the system during the installation and additional system or partition administrators can be created within the application later. All other users must be imported from Unified CCE. Users cannot be manually created within the application. To learn more about importing users, see "Importing Users" on page 34.

This section talks about:

- Creating System Administrators on page 118
- Creating Partition Administrators on page 122
- Editing Department Users on page 126
- Deleting Users on page 131
- Assigning Manager of Users on page 132

Creating System Administrators

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

To create a system administrator:

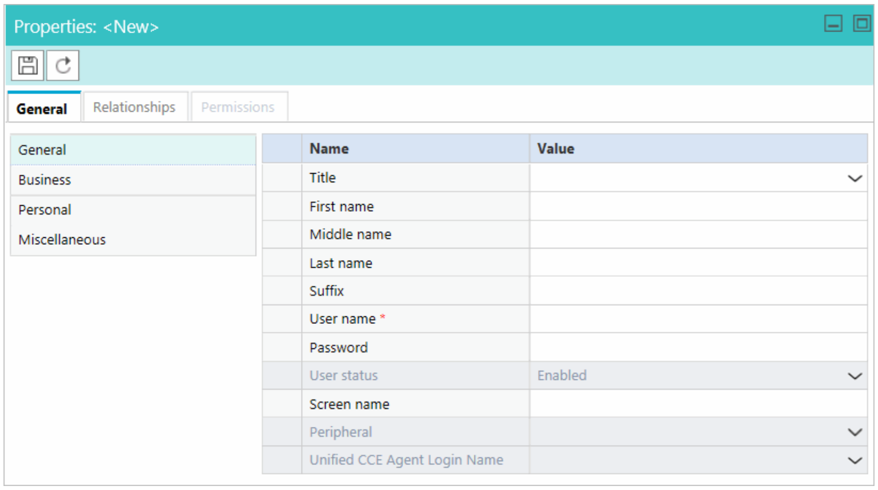
1. Log in to the system partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Context_Root_Name* **> User > Users.**
3. In the List pane toolbar, click the **New** ⊞ button
4. In the Properties pane, on the General tab, set the following:

a. In the General section, provide the following details.

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

The following fields are optional.

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



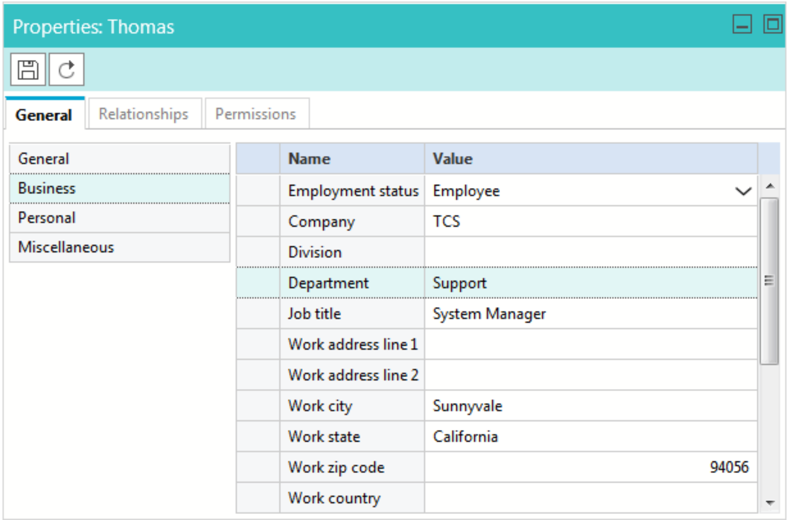
Name	Value
Title	
First name	
Middle name	
Last name	
Suffix	
User name *	
Password	
User status	Enabled
Screen name	
Peripheral	
Unified CCE Agent Login Name	

Set general properties

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

- **Employment status:** The options available are - Customer, Employee, Partner, and Reseller.
- **Company**
- **Division**
- **Department**
- **Job title**
- **Work address line 1**
- **Work address line 2**
- **Work city**
- **Work state**
- **Work zip code**

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

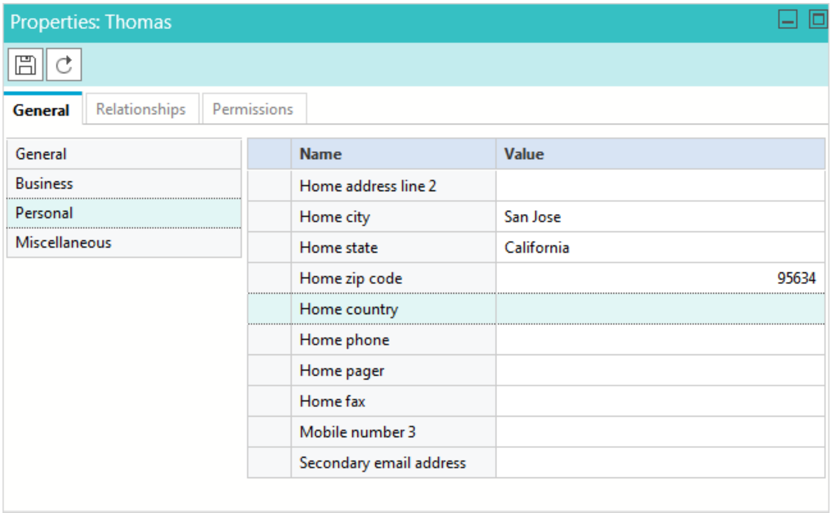


Name	Value
Employment status	Employee
Company	TCS
Division	
Department	Support
Job title	System Manager
Work address line 1	
Work address line 2	
Work city	Sunnyvale
Work state	California
Work zip code	94056
Work country	

Set business properties

c. Next, go to the Personal section, and provide the following information. All the fields are optional.

- **Home address line 2**
- **Home city**
- **Home state**
- **Home zip code**
- **Home country**
- **Home phone**
- **Home pager**
- **Home fax**
- **Mobile number 3**
- **Secondary email address**

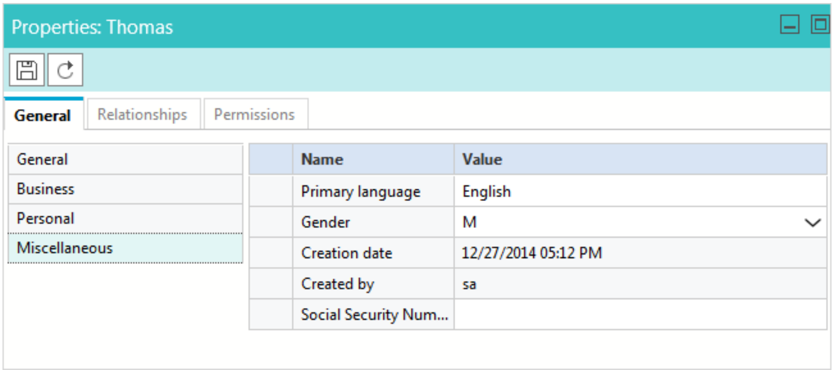


Name	Value
Home address line 2	
Home city	San Jose
Home state	California
Home zip code	95634
Home country	
Home phone	
Home pager	
Home fax	
Mobile number 3	
Secondary email address	

Set personal properties

d. Finally, go to the Miscellaneous section, and provide the following information. All the fields are optional.

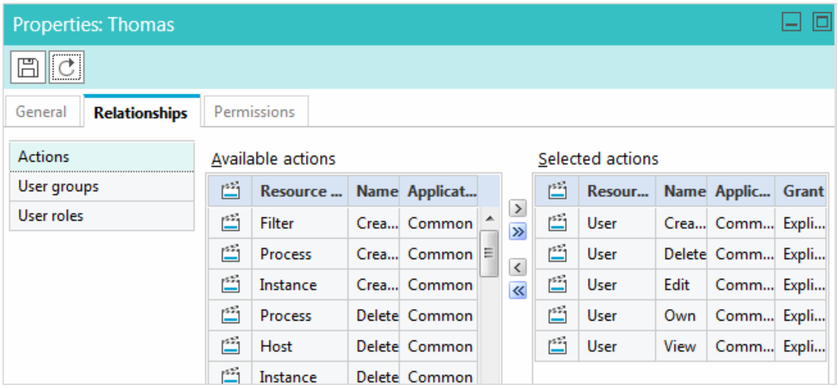
- **Primary language**
- **Gender**
- **Creation date**: This field displays the name of the user who created the user. The value is populated automatically when the user is saved and it cannot be changed.
- **Created by**: This field displays the date and time when the user is created. The value is populated automatically when the user is saved and it cannot be changed.
- **Social Security Number**



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

Set miscellaneous properties

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



Properties: Thomas

General | **Relationships** | Permissions

- Actions
- User groups
- User roles

Available actions

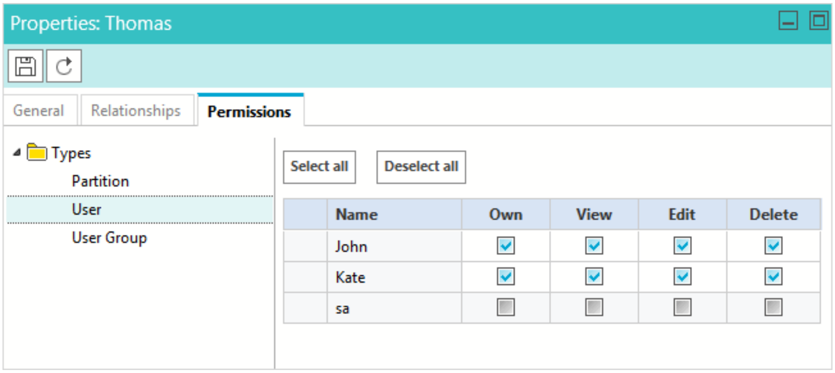
Resource ...	Name	Applicat...
Filter	Crea...	Common
Process	Crea...	Common
Instance	Crea...	Common
Process	Delete	Common
Host	Delete	Common
Instance	Delete	Common

Selected actions

Resour...	Name	Applic...	Grant
User	Crea...	Comm...	Expli...
User	Delete	Comm...	Expli...
User	Edit	Comm...	Expli...
User	Own	Comm...	Expli...
User	View	Comm...	Expli...

Select actions

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



Properties: Thomas

General | Relationships | **Permissions**

- Types
  - Partition
  - User
  - User Group

Select all | Deselect all

Name	Own	View	Edit	Delete
John	☑	☑	☑	☑
Kate	☑	☑	☑	☑
sa	□	□	□	□

Set permissions

8. Click the **Save** button.

Creating Partition Administrators

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

To create a partition administration:

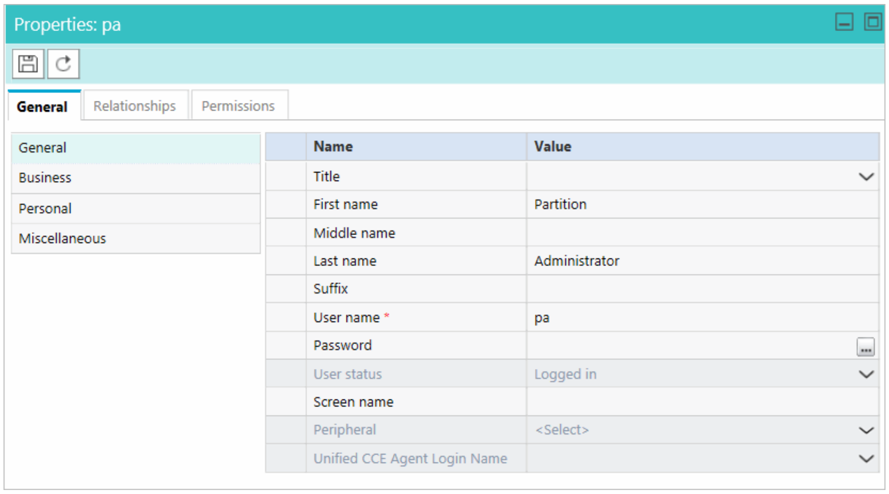
1. Log in to the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> User > Users.**
3. In the List pane toolbar, click the **New** button.
4. In the Properties pane, on the General tab, set the following:

a. In the General section, provide the following details:

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

The following fields are optional.

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

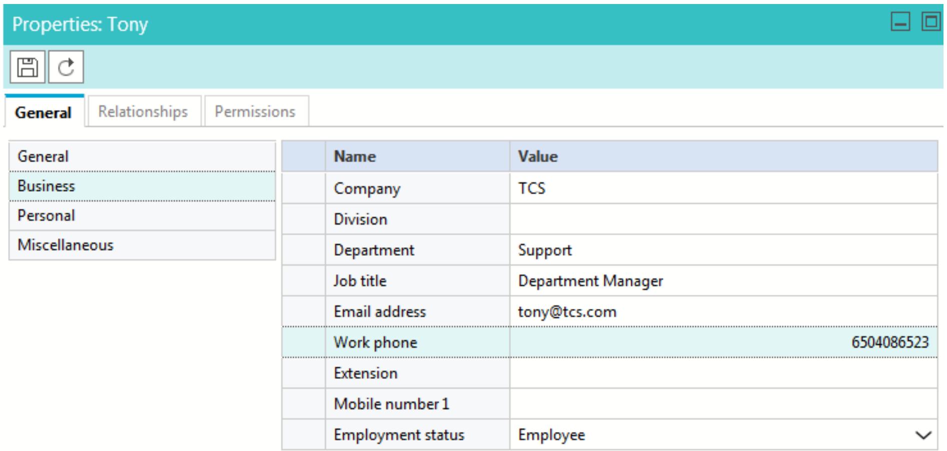


Name	Value
Title	
First name	Partition
Middle name	
Last name	Administrator
Suffix	
User name *	pa
Password	
User status	Logged in
Screen name	
Peripheral	<Select>
Unified CCE Agent Login Name	

Set general properties

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

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

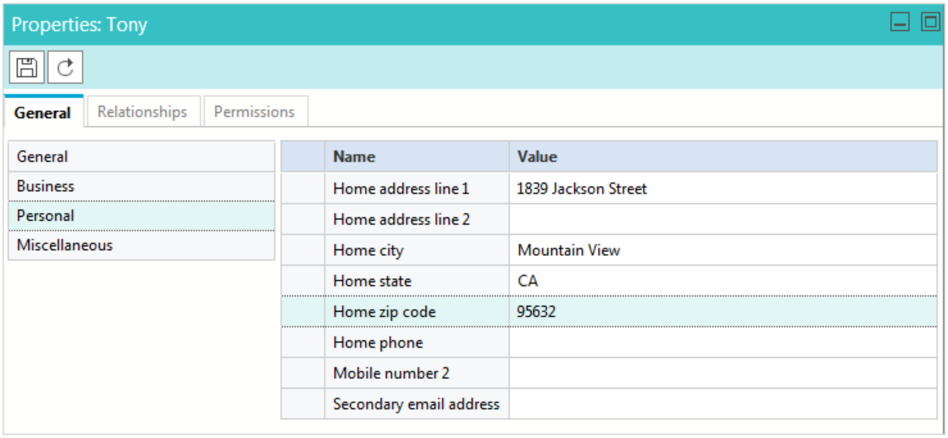


Name	Value
Company	TCS
Division	
Department	Support
Job title	Department Manager
Email address	tony@tcs.com
Work phone	6504086523
Extension	
Mobile number 1	
Employment status	Employee

Set business properties

c. Next, go to the Personal section, and provide the following information. All the fields are optional.

- **Home address line 1**
- **Home address line 2**
- **Home city**
- **Home state**
- **Home zip code**
- **Home phone**
- **Mobile number 2**
- **Secondary email address**

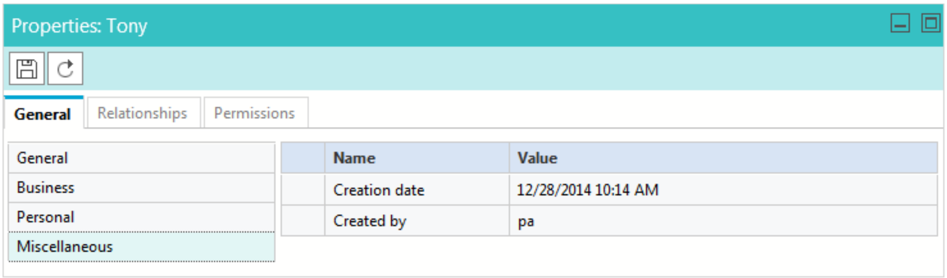


Name	Value
Home address line 1	1839 Jackson Street
Home address line 2	
Home city	Mountain View
Home state	CA
Home zip code	95632
Home phone	
Mobile number 2	
Secondary email address	

Set personal properties

d. Finally, go to the Miscellaneous section. The following information is displayed.

- **Creation date**: This field displays the name of the user who created the user. The value is populated automatically when the user is saved and it cannot be changed.
- **Created by**: This field displays the date and time when the user is created. The value is populated automatically when the user is saved and it cannot be changed.

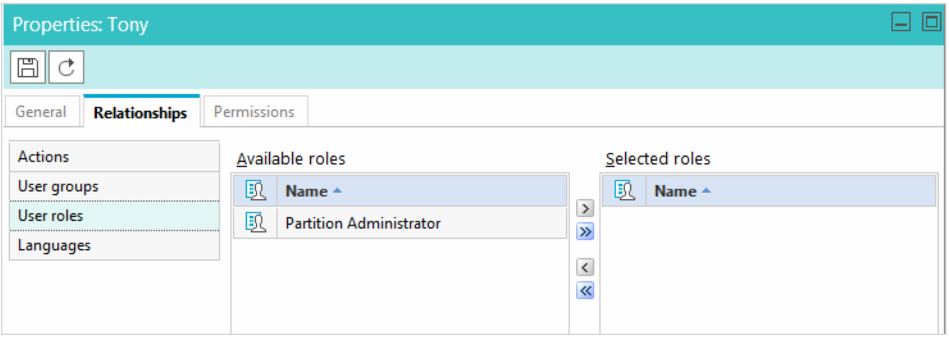


Name	Value
Creation date	12/28/2014 10:14 AM
Created by	pa

View miscellaneous properties

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

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



Available roles

Name
Partition Administrator

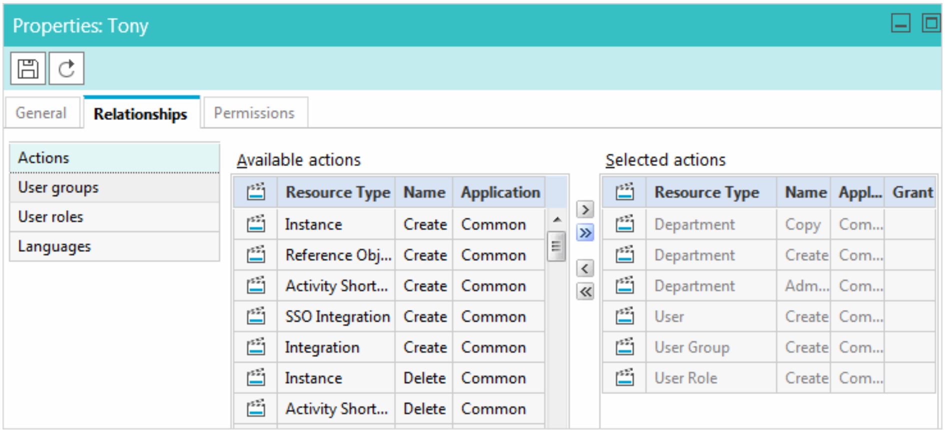
Selected roles

Name

Select user roles

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

   It is highly recommended that you do not assign actions directly to user. You should always use roles with the actions and assign the roles to the user. This makes user management easier.



Available actions

Resource Type	Name	Application
Instance	Create	Common
Reference Obj...	Create	Common
Activity Short...	Create	Common
SSO Integration	Create	Common
Integration	Create	Common
Instance	Delete	Common
Activity Short...	Delete	Common

Selected actions

Resource Type	Name	Appl...	Grant
Department	Copy	Com...	
Department	Create	Com...	
Department	Adm...	Com...	
User	Create	Com...	
User Group	Create	Com...	
User Role	Create	Com...	

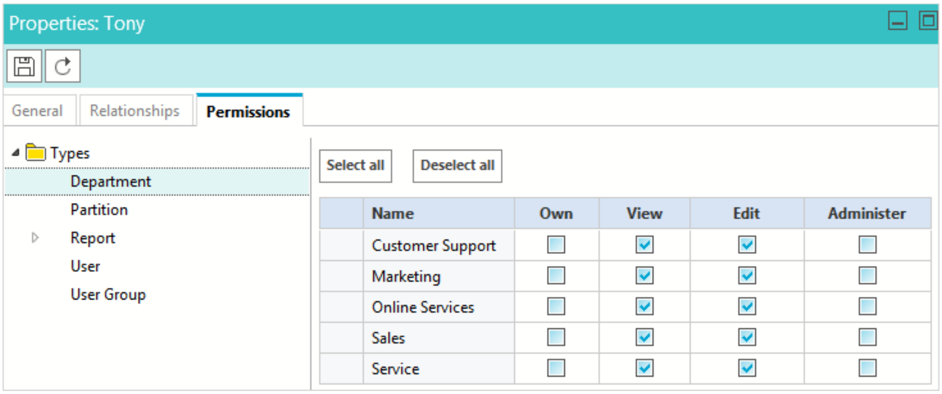
Select actions

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

6. Click the **Save** button to enable the various options in the Permissions tab.

7. On the Permissions tab, assign permissions for the following objects.

   - **Department:** Own, View, Edit, Administer
   - **Partition:** Own, View, Edit, Administer
   - **Report:** View, Run, Edit, Delete, Schedule
   - **User:** Own, View, Edit, Delete
   - **User group:** Own, View, Edit, Delete, Own, View Edit, Delete



Name	Own	View	Edit	Administer
Customer Support	□	☑	☑	□
Marketing	□	☑	☑	□
Online Services	□	☑	☑	□
Sales	□	☑	☑	□
Service	□	☑	☑	□

Set permissions

8. Click the **Save** button.

Editing Department Users

Department users cannot be created within ECE and can only be imported from Unified CCE or Packaged CCE. A majority of the properties for these users are edited and controlled there. For more information, see "Importing Data" on page 33.

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

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

To edit a department user:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> User > Users.**
2. In the List pane toolbar, select a user.
3. In the Properties pane, on the General tab, set the following.

   a. In the General section, provide the following details.

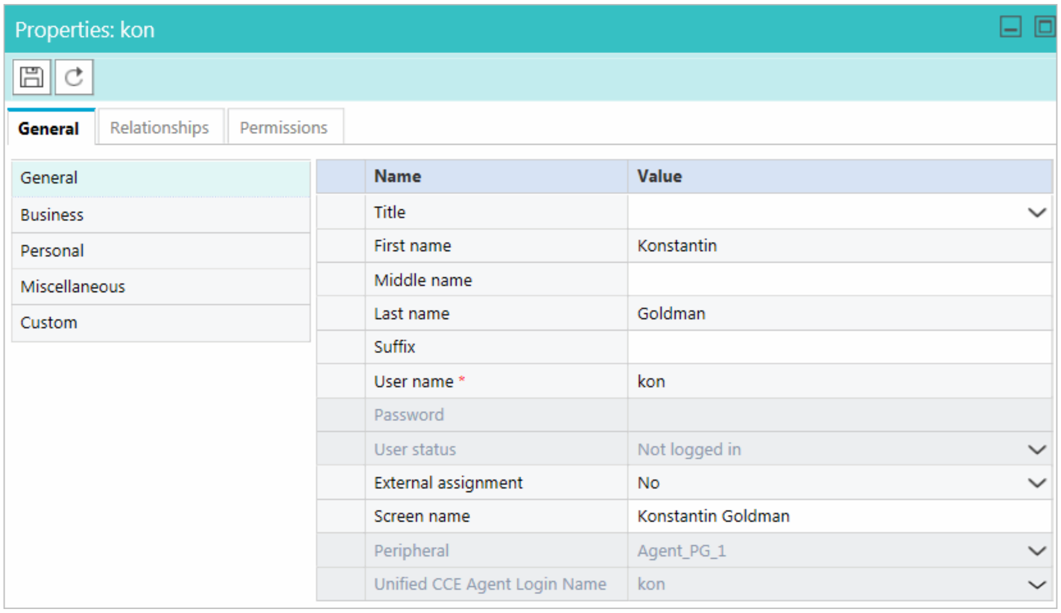
      - **User name**: This name is used by the user to log in to the application. This is managed in Unified CCE and cannot be changed here.
      - **First name:** First name of the user. This is managed in Unified CCE and cannot be changed here.
      - **Last name:** Last name of the user. This is managed in Unified CCE and cannot be changed here.

- **Password**: Password of the user. This is managed in Unified CCE and cannot be changed here.
- **Screen name:** The screen name of the chat agent. This is the name displayed to chat customers in the Customer Console. You can change the value in this field. This is a required field for users who have the ECE Chat license. You can use the same screen name for more than one user in the system.
- **User status**: The status of users cannot be adjusted here. The following statuses can be displayed: Enabled, Disabled, Logged in, and Not logged in.
- **Peripheral:** This field is disabled.
- **Unified CCE Agent Login Name:** This field is disabled.

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

The following fields are optional.

- **Title**
- **Middle name**
- **Suffix**
- **External assignment:** This field is not in use and the value of the field cannot be changed.



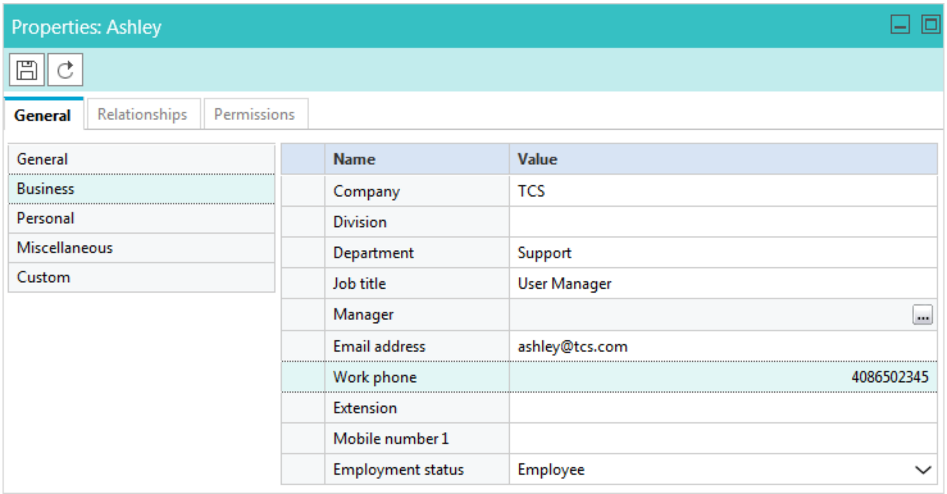
Name	Value
Title	
First name	Konstantin
Middle name	
Last name	Goldman
Suffix	
User name *	kon
Password	
User status	Not logged in
External assignment	No
Screen name	Konstantin Goldman
Peripheral	Agent_PG_1
Unified CCE Agent Login Name	kon

Set general properties

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

- **Company**
- **Division**
- **Department**
- **Job title**
- **Manager:** Here you can set the manager of a user. For more details, see "Assigning Manager of Users" on page 132.

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

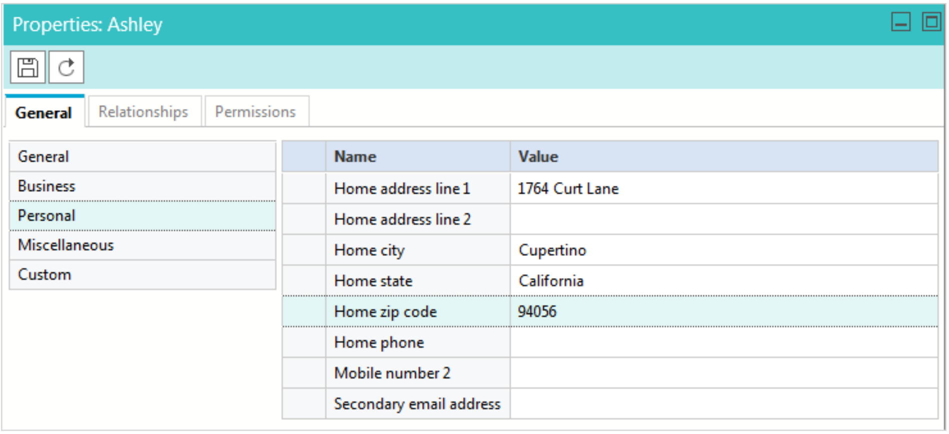


Name	Value
Company	TCS
Division	
Department	Support
Job title	User Manager
Manager	...
Email address	ashley@tcs.com
Work phone	4086502345
Extension	
Mobile number 1	
Employment status	Employee

Set business properties

c. Next, go to the Personal section, and provide the following information. All the fields are optional.

- **Home address line 1**
- **Home address line 2**
- **Home city**
- **Home state**
- **Home zip code**
- **Home phone**
- **Mobile number 2**
- **Secondary email address**

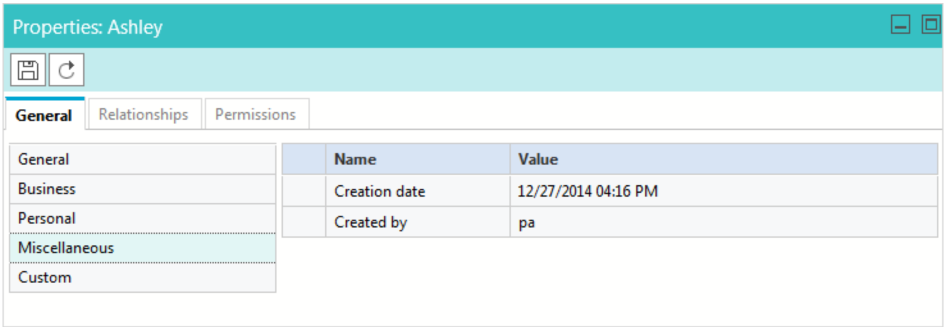


Name	Value
Home address line 1	1764 Curt Lane
Home address line 2	
Home city	Cupertino
Home state	California
Home zip code	94056
Home phone	
Mobile number 2	
Secondary email address	

Set personal properties

d. Next, go to the Miscellaneous section. The following information is displayed.

- **Creation date**: This field displays the name of the user who created the user. The value is populated automatically when the user is saved and it cannot be changed.
- **Created by**: This field displays the date and time the user is created. The value is populated automatically when the user is saved and it cannot be changed.



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

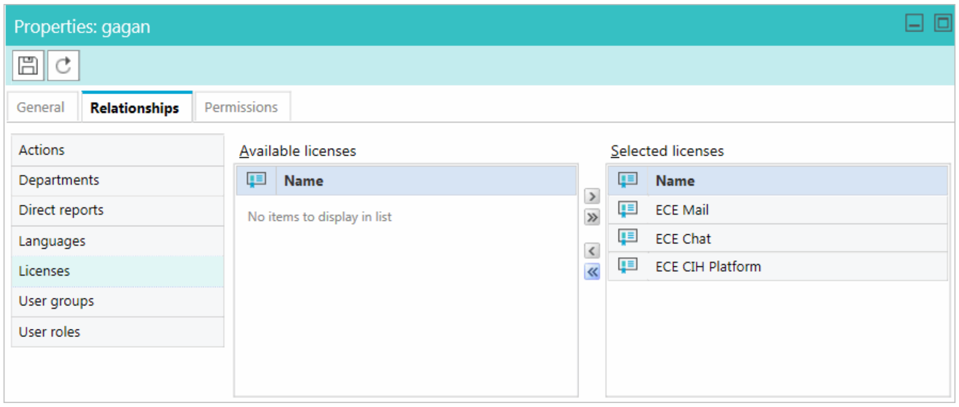
View miscellaneous properties

e. Below, the Custom section is not in use.

f. Next, go to the Relationships tab, and set the following.

a. First, go to the Licenses tab and assign licenses to the user. The following licenses are available:

- ECE CIH Platform
- ECE Mail
- ECE Chat



Available licenses

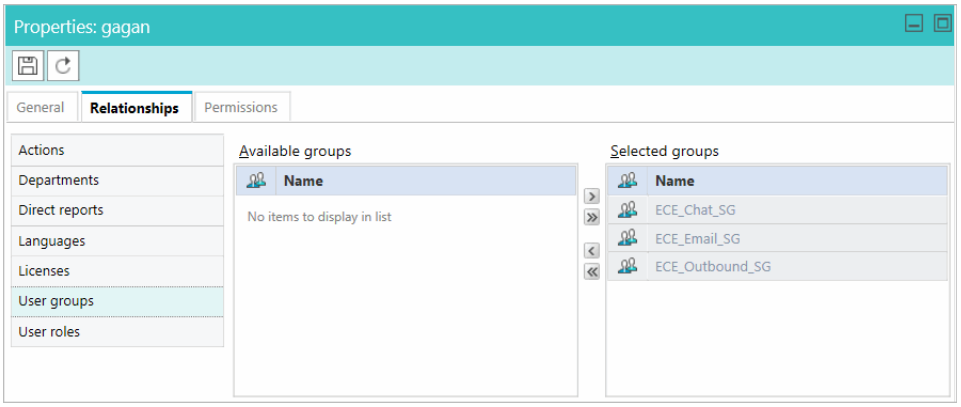
Name
No items to display in list

Selected licenses

Name
ECE Mail
ECE Chat
ECE CIH Platform

Select licenses

b. In the User groups section you can see which user groups to which the user belongs. These groups are determined by the skill groups in which the user belongs in Unified CCE. For more information about skill groups, see Importing Skill Groups on page 35.



Available groups

Name
No items to display in list

Selected groups

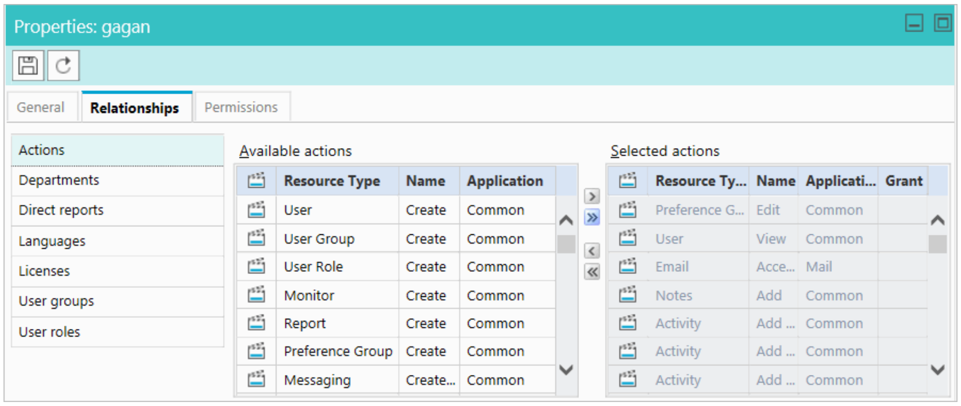
Name
ECE_Chat_SG
ECE_Email_SG
ECE_Outbound_SG

Select user groups

c. Go to the User roles section and select the roles to be assigned to the user. If you want to view the actions that come as part of the selected role, save the user and go to the Actions tab to see the list of actions.

d. Next, go to the Actions section, and view the list of actions assigned to the user. Here you can also assign additional actions to the user. You can identify how actions are assigned from the Grant field in the Selected actions section. The actions assigned explicitly show the value “Explicit”. If you want to allow the user to import and export content for translations from the Knowledge Base Console, assign the “Import Translation” and “Export Translation” actions to the user.

It is highly recommended that you do not assign actions directly to user. You should always use roles with the actions and assign the roles to the user. This makes user management easier.



Available actions

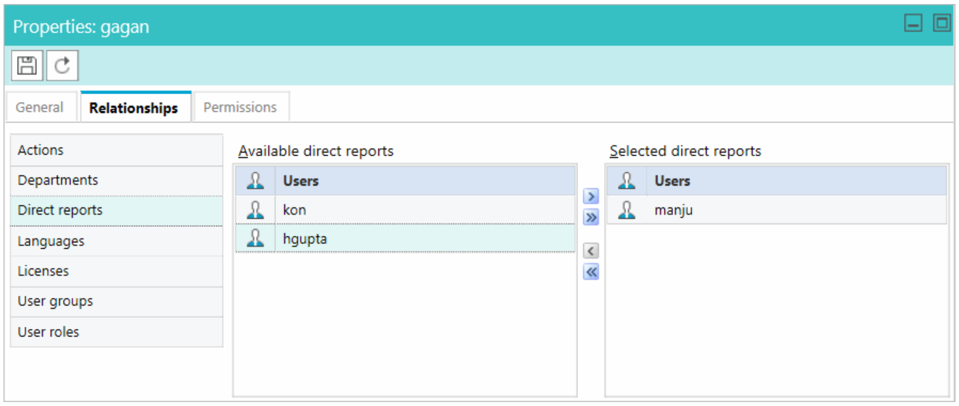
Resource Type	Name	Application
User	Create	Common
User Group	Create	Common
User Role	Create	Common
Monitor	Create	Common
Report	Create	Common
Preference Group	Create	Common
Messaging	Create...	Common

Selected actions

Resource Ty...	Name	Applicati...	Grant
Preference G...	Edit	Common	
User	View	Common	
Email	Acce...	Mail	
Notes	Add	Common	
Activity	Add ...	Common	
Activity	Add ...	Common	
Activity	Add ...	Common	

e. Next, in the Languages section, select the primary KB language for the user.

f. Next, in the Direct reports section you can select the users who reports to this user. For more details, see “Assigning Manager of Users” on page 132.



Available direct reports
Users
kon
hgupta

Selected direct reports
Users
manju

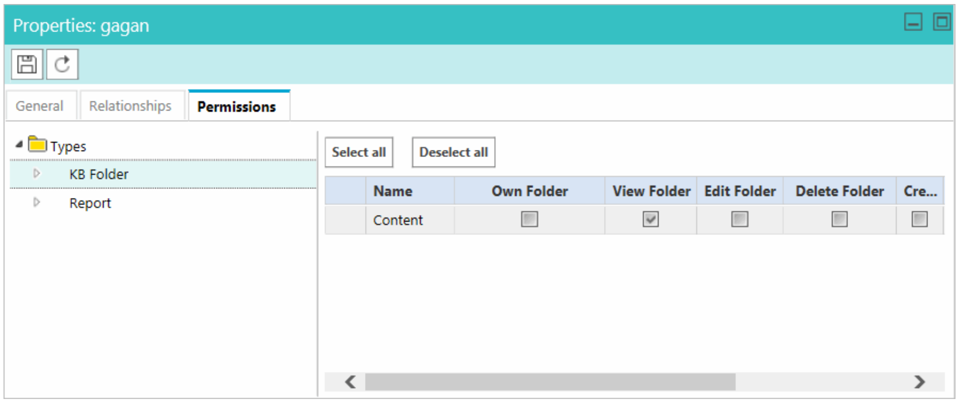
Select users for direct reports

4. Click the **Save** button to enable the various options in the Permissions tab.

5. On the Permissions tab, the permissions for the following objects are assigned.

   ❍ **KB Folder:** Own folder, View folder, Edit folder, Delete folder, Create folder, Create article, Edit article, Delete article, Suggest article, Manage suggestions, View personal folder

   ❍ **Report:** Own, View, Edit, Delete, Schedule



Name	Own Folder	View Folder	Edit Folder	Delete Folder	Cre...
Content	□	☑	□	□	□

Assign permissions

6. Click the **Save** button.

Deleting Users

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

To delete a user:

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

- If you are deleting a system administrator, go to the system partition and browse to **Administrator > Partition:** *Context_Root_Name* **> User > Users.**
- If you are deleting a partition administrator, go to the business partition and browse to **Administrator > Partition:** *Partition_Name* **> User > Users.**
- If you are a department administrator, browse to **Administration > Departments >** *Department_Name* **> User > Users.**

2. In the List pane, select the user you want to delete.
3. In the List pane toolbar, click the **Delete** ☒ button.
4. A message appears asking to confirm the deletion. If the user has created any monitors in the Supervision Console, a message is displayed to inform that all the monitors created by the user will be deleted. Click **Yes** to delete the user.

Assigning Manager of Users

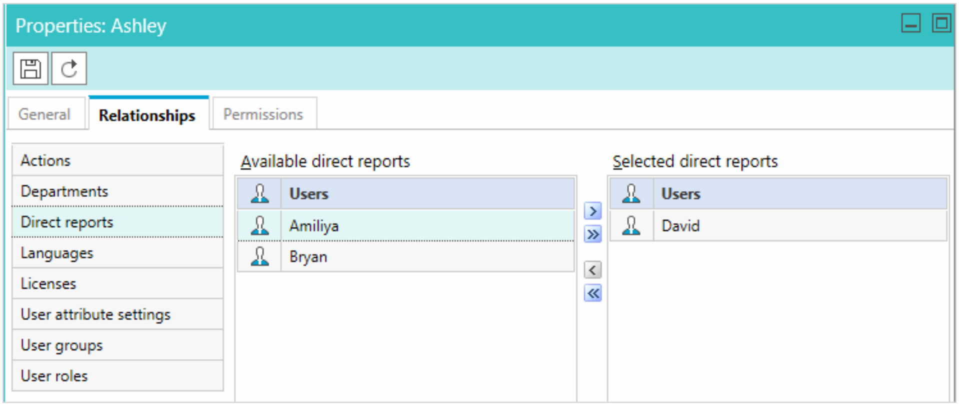
A manager can monitor the activities and cases assigned to agents from the Agent Console. The manager has a read only view of the activities and cases assigned to the users reporting to him.

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

You cannot assign managers of user groups.

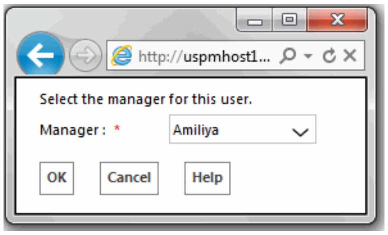
To assign a manager of a user:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> User > Users**.
2. In the List pane, select a user and do one of the following:
   - If you are editing the properties of the manager, then in the Properties pane, go the Relationships tab and in the Direct reports section, select the users who report to the selected user. The user becomes the manager of the selected users.



Select the users reporting to this user

- If you are assigning the manager of the user, then in the General tab, go to the Business section and in the Manager field click the **Assistance** ⋯ button. The Select Manager window appears. Select a manager for the user and click the **OK** button.

  Select the manager for this user.

  Manager : * Amiliya

  Select a manager of the user

3. Click the **Save** button.

5 Data Masking

About Data Masking

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

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

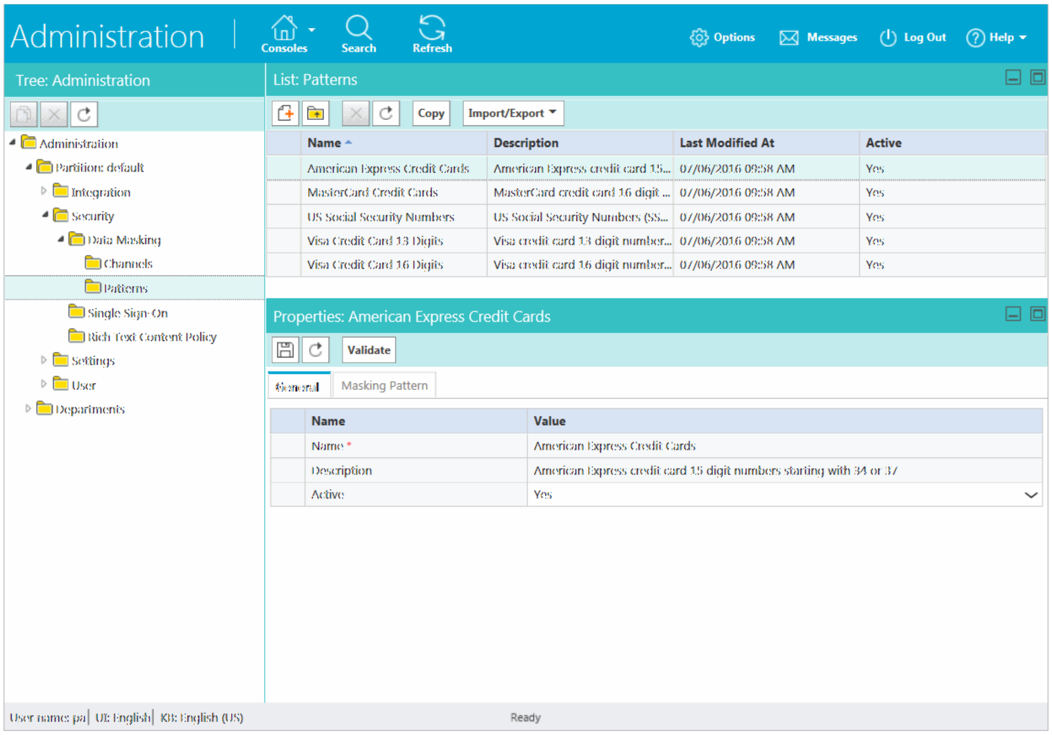
Data masking is available for emails and chats.

About Patterns

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

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

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



Name	Description	Last Modified At	Active
American Express Credit Cards	American Express credit card 15...	07/06/2016 09:58 AM	Yes
MasterCard Credit Cards	MasterCard credit card 16 digit ...	07/06/2016 09:58 AM	Yes
US Social Security Numbers	US Social Security Numbers (SS...	07/06/2016 09:58 AM	Yes
Visa Credit Card 13 Digits	Visa credit card 13 digit number...	07/06/2016 09:58 AM	Yes
Visa Credit Card 16 Digits	Visa credit card 16 digit number...	07/06/2016 09:58 AM	Yes

Name	Value
Name *	American Express Credit Cards
Description	American Express credit card 15 digit numbers starting with 34 or 37
Active	Yes

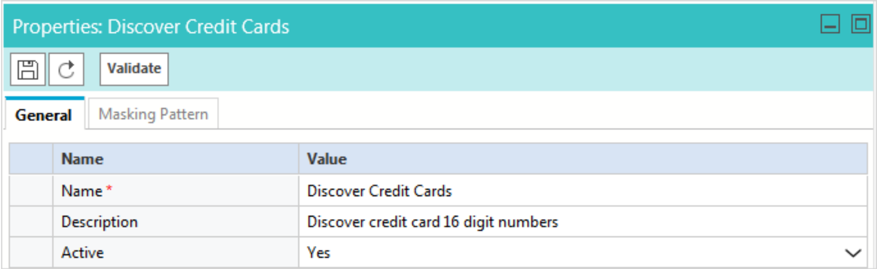
Out-of-the-box patterns

Creating Patterns

To create a pattern:

1. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security> Data Masking > Patterns**.
2. In the List pane toolbar, click the **New** button.
3. In the Properties pane, on the General tab, set the following:
   - **Name:** Type a name for the pattern.
   - **Description:** Provide a description for the pattern that explains what type of masking is done by the pattern.

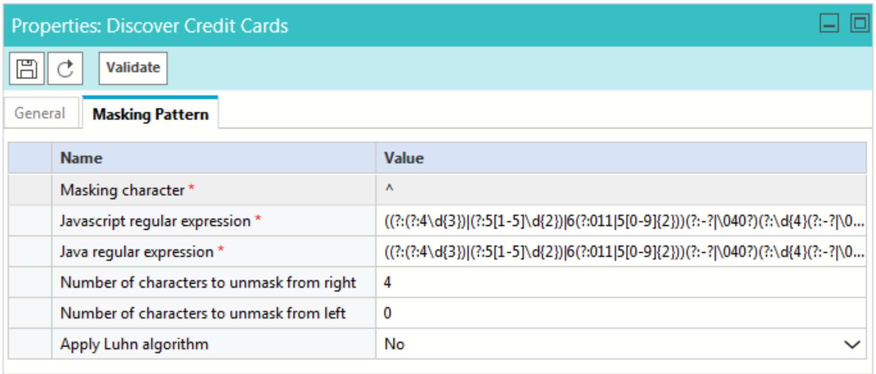
- **Active:** Make the pattern active when it is ready for use. Only active patterns can be applied to channels. Once a pattern is made active and used in channels, it can be made inactive only after the association from the channels is removed.



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

Set the general properties

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



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

Configure the pattern properties

5. Click the **Save** button.

Creating Patterns in XML File

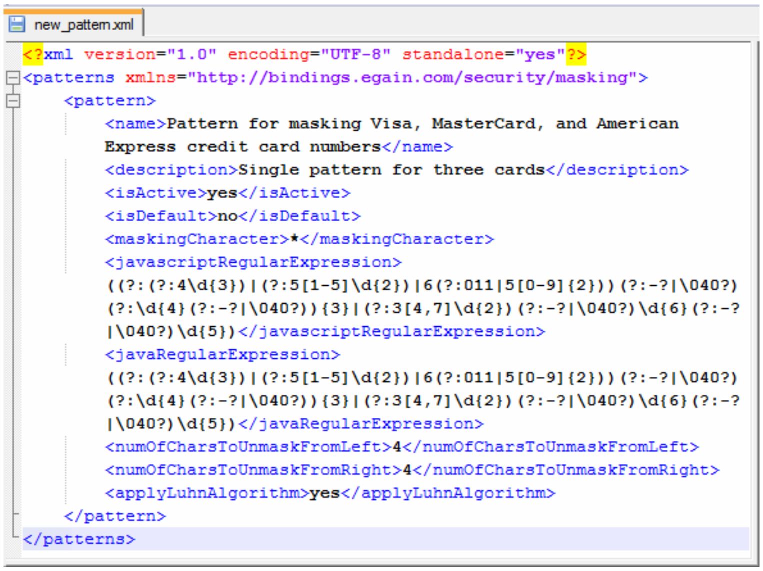
While preparing a file for importing patterns, keep in mind that:

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

The following table lists the names of the properties as they appear in the file and on the UI. For the description of each field, see "Creating Patterns" on page 136.

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

A sample pattern looks like:



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<patterns xmlns="http://bindings.egain.com/security/masking">
    <pattern>
        <name>Pattern for masking Visa, MasterCard, and American
        Express credit card numbers</name>
        <description>Single pattern for three cards</description>
        <isActive>yes</isActive>
        <isDefault>no</isDefault>
        <maskingCharacter>*</maskingCharacter>
        <javascriptRegularExpression>
        ((?:(?:4\d{3})|(?:5[1-5]\d{2})|6(?:011|5[0-9]{2}))(?:-?|\040?)
        (?:\d{4}(?:-?|\040?)){3}|(?:3[4,7]\d{2})(?:-?|\040?)\d{6}(?:-?
        |\040?)\d{5})</javascriptRegularExpression>
        <javaRegularExpression>
        ((?:(?:4\d{3})|(?:5[1-5]\d{2})|6(?:011|5[0-9]{2}))(?:-?|\040?)
        (?:\d{4}(?:-?|\040?)){3}|(?:3[4,7]\d{2})(?:-?|\040?)\d{6}(?:-?
        |\040?)\d{5})</javaRegularExpression>
        <numOfCharsToUnmaskFromLeft>4</numOfCharsToUnmaskFromLeft>
        <numOfCharsToUnmaskFromRight>4</numOfCharsToUnmaskFromRight>
        <applyLuhnAlgorithm>yes</applyLuhnAlgorithm>
    </pattern>
</patterns>
```

A sample XML file

Exporting Masking Patterns

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

To export patterns:

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

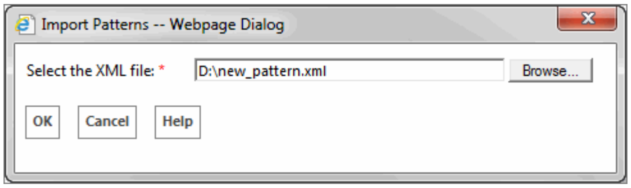
Importing Masking Patterns

Only XML files can be used to import patterns.

To import a pattern:

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

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



Import Patterns -- Webpage Dialog

Select the XML file: * D:\new_pattern.xml

Provide the location the location file

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

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

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

Copying Patterns

To copy a pattern:

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

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

Deleting Patterns

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

To delete a pattern:

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

Validating Masking Patterns

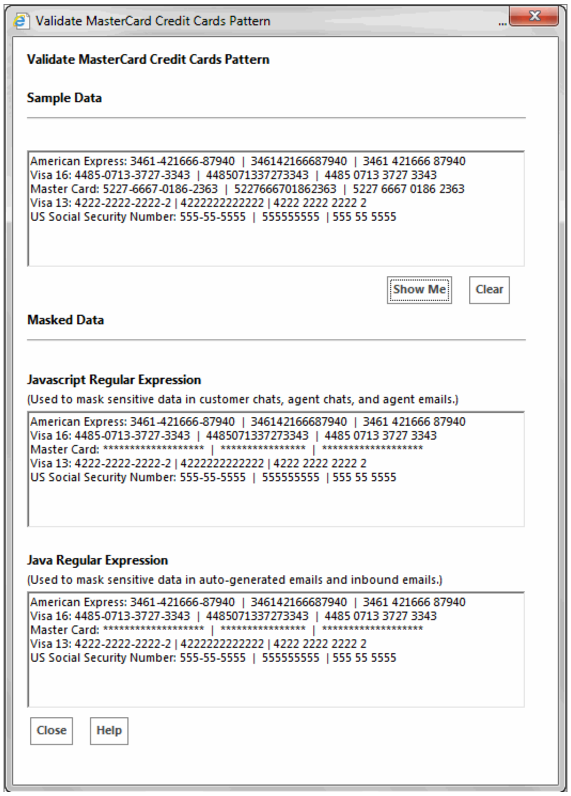
Validating Individual Patterns

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

To validate a pattern:

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

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



Validate MasterCard Credit Cards Pattern

Validate MasterCard Credit Cards Pattern

Sample Data

```
American Express: 3461-421666-87940  |  346142166687940  |  3461 421666 87940
Visa 16: 4485-0713-3727-3343  |  4485071337273343  |  4485 0713 3727 3343
Master Card: 5227-6667-0186-2363  |  5227666701862363  |  5227 6667 0186 2363
Visa 13: 4222-2222-2222-2 | 4222222222222 | 4222 2222 2222 2
US Social Security Number: 555-55-5555  |  555555555  | 555 55 5555
```

Masked Data

Javascript Regular Expression

(Used to mask sensitive data in customer chats, agent chats, and agent emails.)

```
American Express: 3461-421666-87940  |  346142166687940  |  3461 421666 87940
Visa 16: 4485-0713-3727-3343  |  4485071337273343  |  4485 0713 3727 3343
Master Card: *******************  |  ****************  |  *******************
Visa 13: 4222-2222-2222-2 | 4222222222222 | 4222 2222 2222 2
US Social Security Number: 555-55-5555  |  555555555  | 555 55 5555
```

Java Regular Expression

(Used to mask sensitive data in auto-generated emails and inbound emails.)

```
American Express: 3461-421666-87940  |  346142166687940  |  3461 421666 87940
Visa 16: 4485-0713-3727-3343  |  4485071337273343  |  4485 0713 3727 3343
Master Card: *******************  |  ****************  |  *******************
Visa 13: 4222-2222-2222-2 | 4222222222222 | 4222 2222 2222 2
US Social Security Number: 555-55-5555  |  555555555  | 555 55 5555
```

Validate patterns

Validating Masking Patterns Applied to Channels

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

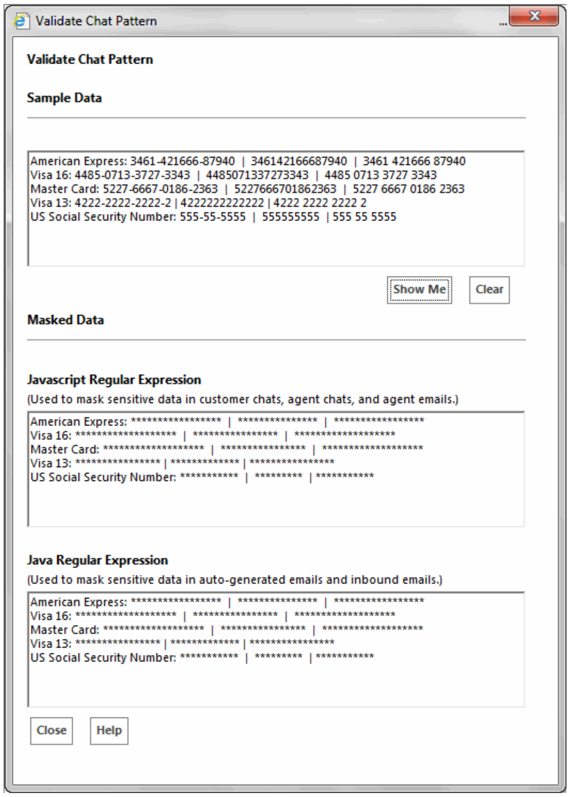
To validate patterns applied to channels:

1. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security> Data Masking > Channels**. If you are validating from the department level, browse to **Administration > Departments >** *Department_Name* **> Security> Data Masking > Channels**.
2. In the List pane select the channel you want to test.
3. In the Properties pane toolbar, click the **Validate** button.
4. In the Validate Pattern window, do the following:

   a. In the Sample Data provide the text you want to use for testing the pattern and Click the **Show Me** button.

   b. In the Masked Data section, you will see all the selected patterns applied to the sample data.

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



Validate Chat Pattern

Sample Data

```
American Express: 3461-421666-87940 | 346142166687940 | 3461 421666 87940
Visa 16: 4485-0713-3727-3343 | 4485071337273343 | 4485 0713 3727 3343
Master Card: 5227-6667-0186-2363 | 5227666701862363 | 5227 6667 0186 2363
Visa 13: 4222-2222-2222-2 | 4222222222222 | 4222 2222 2222 2
US Social Security Number: 555-55-5555 | 555555555 | 555 55 5555
```

Masked Data

Javascript Regular Expression

(Used to mask sensitive data in customer chats, agent chats, and agent emails.)

```
American Express: ***************** | *************** | *****************
Visa 16: ******************* | **************** | *******************
Master Card: ******************* | **************** | *******************
Visa 13: **************** | ************* | ****************
US Social Security Number: *********** | ********* | ***********
```

Java Regular Expression

(Used to mask sensitive data in auto-generated emails and inbound emails.)

```
American Express: ***************** | *************** | *****************
Visa 16: ******************* | **************** | *******************
Master Card: ******************* | **************** | *******************
Visa 13: **************** | ************* | ****************
US Social Security Number: *********** | ********* | ***********
```

Validate the patterns selected for a channel

Applying Patterns to Chat Channel

At the Partition Level

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

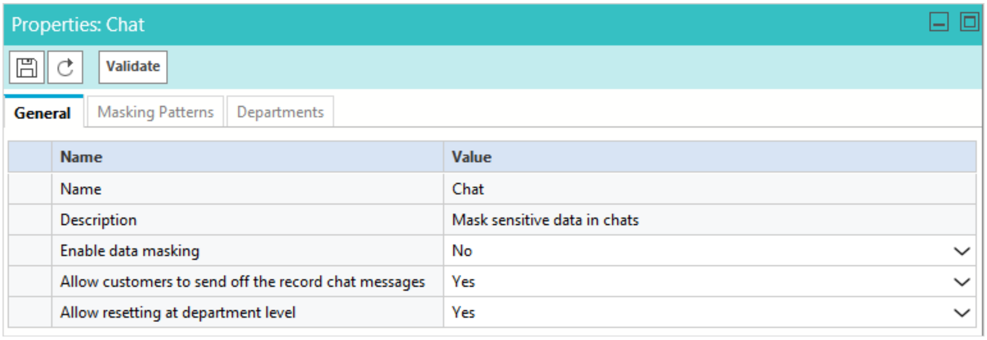
- **Manage Application Security:** Allows you to view the patterns applied to channels and to apply patterns to channels.
- **View Application Security:** Gives a read-only view of the patterns applied to channels. Users with this action cannot change any configurations.

What can the partition administrator do?

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

To apply patterns to the chat channel:

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

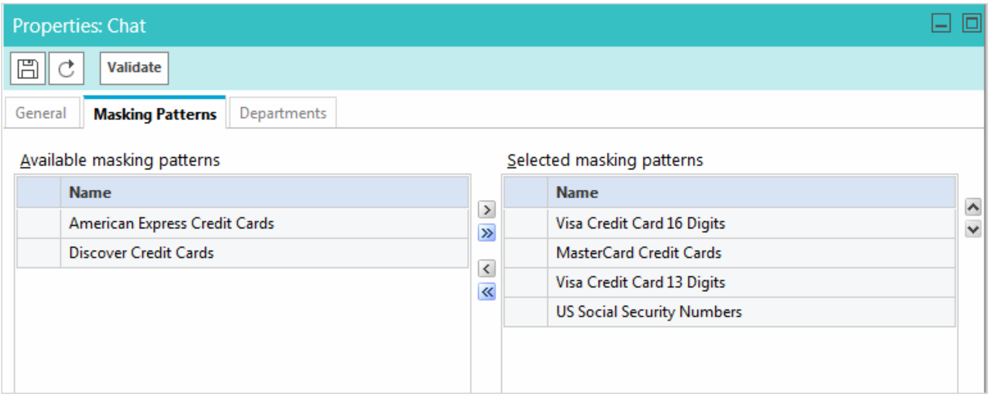


Name	Value
Name	Chat
Description	Mask sensitive data in chats
Enable data masking	No
Allow customers to send off the record chat messages	Yes
Allow resetting at department level	Yes

Set the general properties

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

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



Available masking patterns

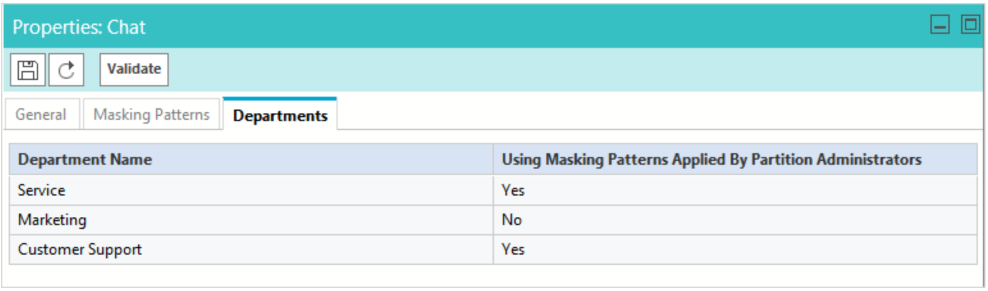
Name
American Express Credit Cards
Discover Credit Cards

Selected masking patterns

Name
Visa Credit Card 16 Digits
MasterCard Credit Cards
Visa Credit Card 13 Digits
US Social Security Numbers

Select masking patterns for chat

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



Department Name	Using Masking Patterns Applied By Partition Administrators
Service	Yes
Marketing	No
Customer Support	Yes

View the list of departments

6. Click the **Save** button.

7. After saving the changes, validate the patterns selected for the channel. For details, see "Validating Masking Patterns Applied to Channels" on page 142.

At the Department Level

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

- **Manage Department Security:** Allows you to view the patterns applied to channels and to apply patterns to channels.

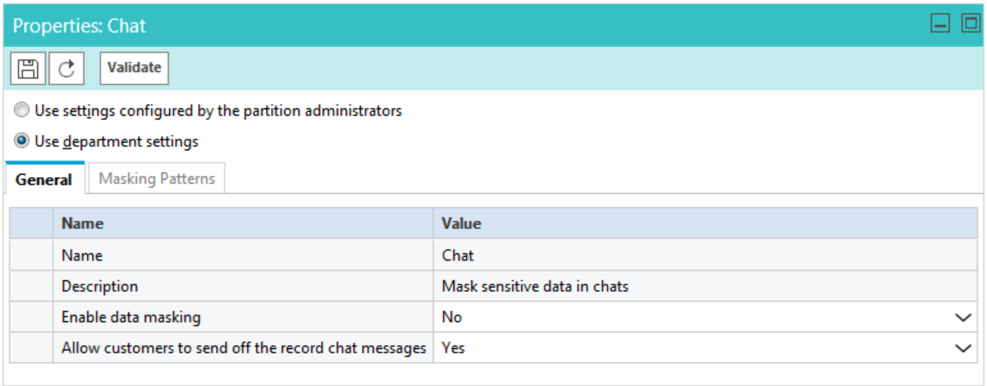
- **View Department Security:** Gives a read-only view of the patterns applied to channels. Users with this action cannot change any configurations.

How much control do department administrators get?

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

To apply patterns to the chat channel:

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

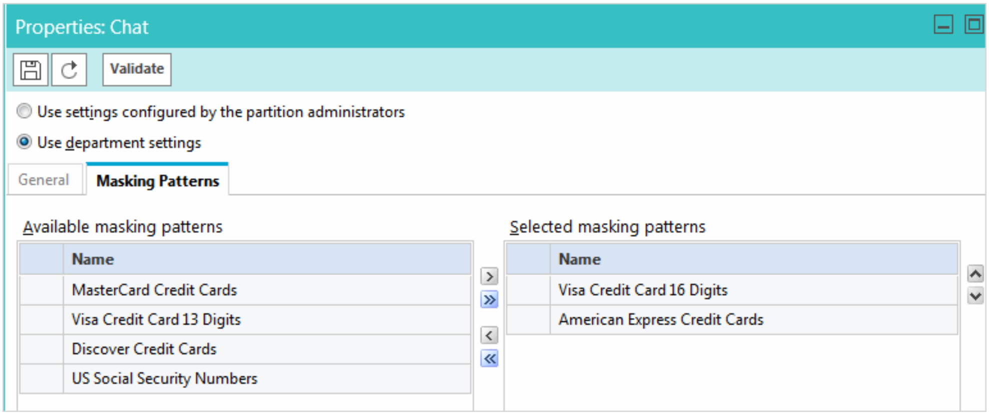


○ Use settings configured by the partition administrators
● Use department settings

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

Set the general properties

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



○ Use settings configured by the partition administrators

● Use department settings

Available masking patterns

Name
MasterCard Credit Cards
Visa Credit Card 13 Digits
Discover Credit Cards
US Social Security Numbers

Selected masking patterns

Name
Visa Credit Card 16 Digits
American Express Credit Cards

Select masking patterns for the chat channel

6. Click the **Save** button.

7. After saving the changes, validate the patterns selected for the channel by using the **Validate** button. For details, see "Validating Masking Patterns Applied to Channels" on page 142.

Applying Patterns to Email Channel

At the Partition Level

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

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

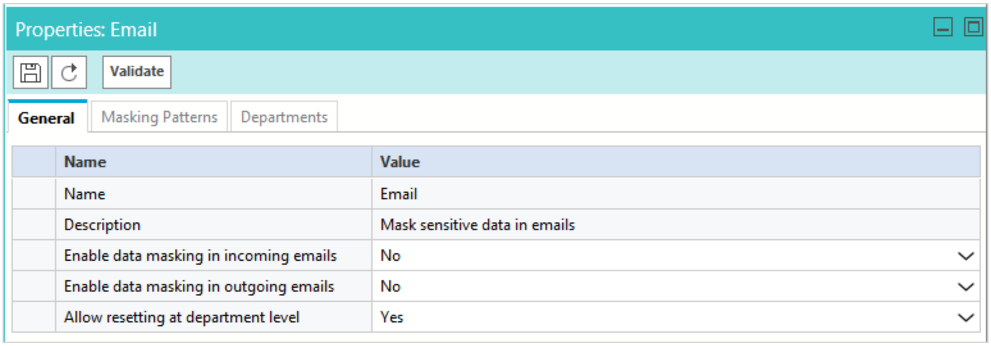
What can the partition administrator do?

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

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

To apply patterns to the email channel:

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

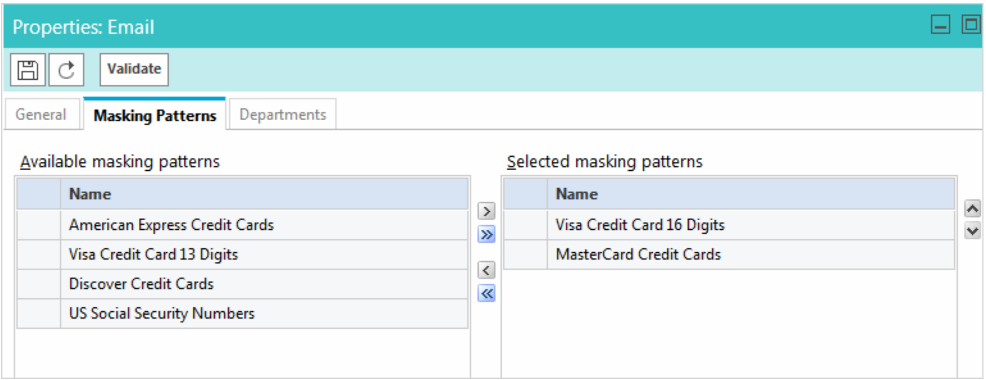


Name	Value
Name	Email
Description	Mask sensitive data in emails
Enable data masking in incoming emails	No
Enable data masking in outgoing emails	No
Allow resetting at department level	Yes

Set the general properties

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

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



Available masking patterns

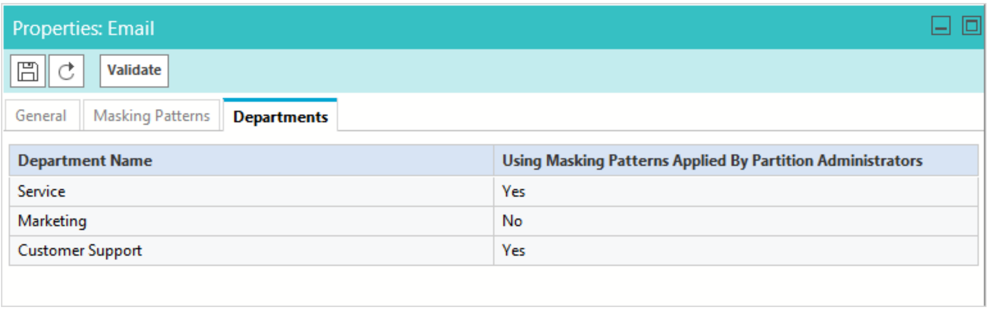
Name
American Express Credit Cards
Visa Credit Card 13 Digits
Discover Credit Cards
US Social Security Numbers

Selected masking patterns

Name
Visa Credit Card 16 Digits
MasterCard Credit Cards

Select masking patterns

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



Department Name	Using Masking Patterns Applied By Partition Administrators
Service	Yes
Marketing	No
Customer Support	Yes

View the list of departments

6. Click the **Save** 🖫 button.

7. After saving the changes, validate the patterns selected for the channel by using the **Validate** button. For details, see "Validating Masking Patterns Applied to Channels" on page 142.

At the Department Level

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

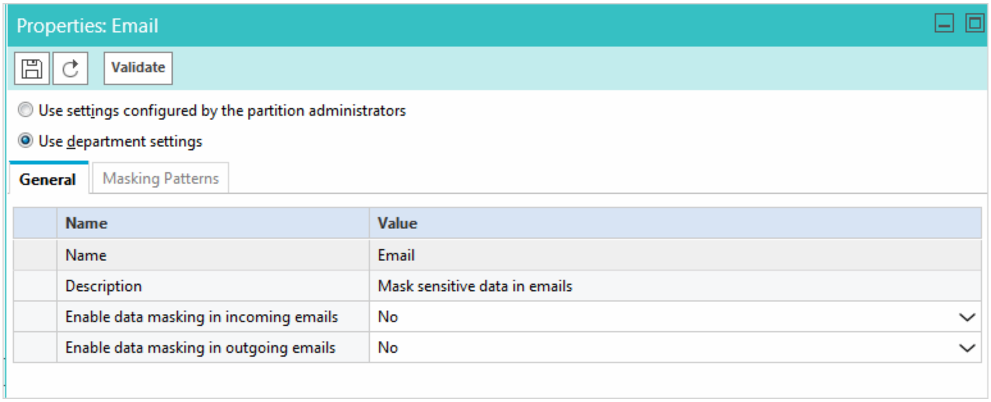
- **Manage Department Security:** Allows you to view the patterns applied to channels and to apply patterns to channels.
- **View Department Security:** Gives a read-only view of the patterns applied to channels. Users with this action cannot change any configurations.

How much control do department administrators get?

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

To apply patterns to the email channel:

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



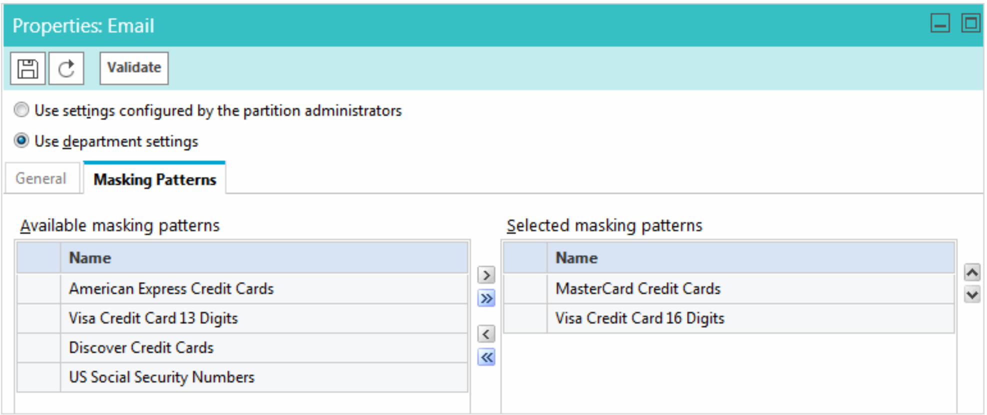
○ Use settings configured by the partition administrators

● Use department settings

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

View the general properties

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



Properties: Email

Validate

○ Use settings configured by the partition administrators

● Use department settings

General | Masking Patterns

Available masking patterns

Name
American Express Credit Cards
Visa Credit Card 13 Digits
Discover Credit Cards
US Social Security Numbers

Selected masking patterns

Name
MasterCard Credit Cards
Visa Credit Card 16 Digits

Select patterns for the email channel

6. Click the **Save** button.

7. After saving the changes, validate the patterns selected for the channel by using the **Validate** button. For details, see "Validating Masking Patterns Applied to Channels" on page 142.

6

Single Sign-On

About Single Sign-On (SSO)

SSO must be enabled to allow agents to log in to ECE through Finesse and supervisors or administrators to log in to ECE using Cisco IDS. The following options are available from the dropdown to enable SSO:

- Siteminder This method of SSO is not used in ECE.
- LDAP This method of SSO is not used in ECE.
- SAML 1.1 This method of SSO is not used in ECE.
- SAML 2.0 This method of SSO is configured for supervisors and administrators through Cisco IDS.
- Cisco IDS (page 156)

Configuring Single Sign-On (SSO)

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.
- SSO is not used to access the system partition (partition 0).
- SSO does not apply to partition administrators.
- Chat Customer Single Sign-On is not currently available in ECE.
- 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.
- An 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.
- For supervisors and administrators to log into the consoles other than the Agent Console, once SSO is enabled, you must provide a valid web server or load balancer URL in the partition settings. See “Web Server URL or Load Balancer URL” on page 47 for more information.

Preparing to Configure Single Sign-On for Cisco IDS

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

Integrating with Unified CCE

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

- For more information about integrating with Unified CCE, see "Unified CCE Integration" on page 30.
- For more information about integrating with Packaged CCE, see the *Enterprise Chat and Email Installation Guide for Packaged Contact Center Enterprise*.

Configuring ADFS

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

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

To configure public key certificate in the relying party trust:

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

Importing the SSL Certificate to Application Servers

Before configuring SSO for Cisco IDS, the SSL certificate must be imported to ECE application servers for Unified CCE installations or the ECE server for Packaged CCE installations.

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

To obtain the SSL certificate:

Important: **To obtain the necessary SSL certificate file, contact your IT department or Cisco IDS support for the preferred method of obtaining the SSL certificate prior to following these steps.**

1. On the ECE Application server, launch Internet Explorer.
2. Access `https://`*cisco-ids-1*`:8553` in the browser, where *cisco-ids-1* indicates the Fully Qualified Domain Name (FQDN) of the Primary Cisco IDS server.

3. In the page that appears, click the **Continue to this website (not recommended)** option.
4. In the address bar, click the **Certificate error** notification.
5. In the Untrusted Certificate pop-up, click the **View certificates** option.
6. In the Certificate window that appears, click the **Details** tab.
7. Click the **Copy to File...** button.
8. In the Certificate Export Wizard welcome page, click the **Next** button.
9. On the Export File Format page, select the **DER encoded binary X.509 (.CER)** option. Click **Next**.
10. Specify the path to export the certificate. For example, C:\ciscoids1.cer. Click **Next**.
11. Click **Finish**. If a secondary Cisco IDS server is in use, perform these steps for it as well.

To import the SSL certificate:

If running a distributed installation with multiple application servers, perform these steps for each application server.

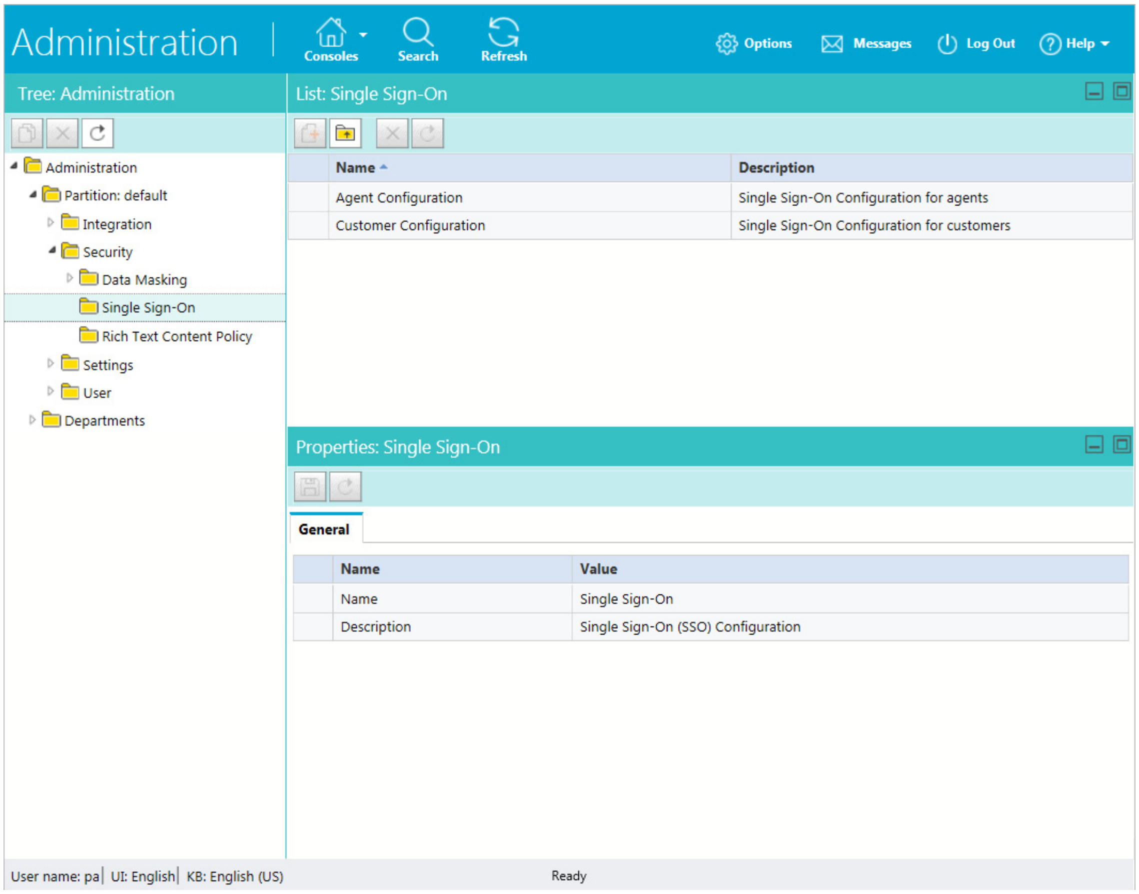
Important: **Perform these steps for both the primary and secondary Cisco IDS server.**

1. Copy the certificate file to the application server directory:
   ```
   application_server\ECE_installation_directory\Java\jdk\jre\bin
   ```
2. Open Command prompt on the application server and enter the directory where you copied the certificate file.
3. Run following command to import the certificate:
   ```
   application_server\ECE_installation_directory\Java\jdk\jre\lib\security\cacerts Java Keystore
   keytool -import -alias ciscoids -file ciscoids.cer -keystore
   ..\lib\security\cacerts
   ```
4. When prompted for the keystore password, type “**changeit**” and press ENTER on your keyboard.
5. When prompted to trust this certificate, type “**Y**” or “**Yes**” and press ENTER on your keyboard.
6. Restart the server.

Configuring Single Sign-On (SSO) for Cisco IDS

To configure SSO for Cisco IDS:

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



Name	Description
Agent Configuration	Single Sign-On Configuration for agents
Customer Configuration	Single Sign-On Configuration for customers

Name	Value
Name	Single Sign-On
Description	Single Sign-On (SSO) Configuration

Browse to single sign-on node

2. In the List pane, select **Agent Configuration**.

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

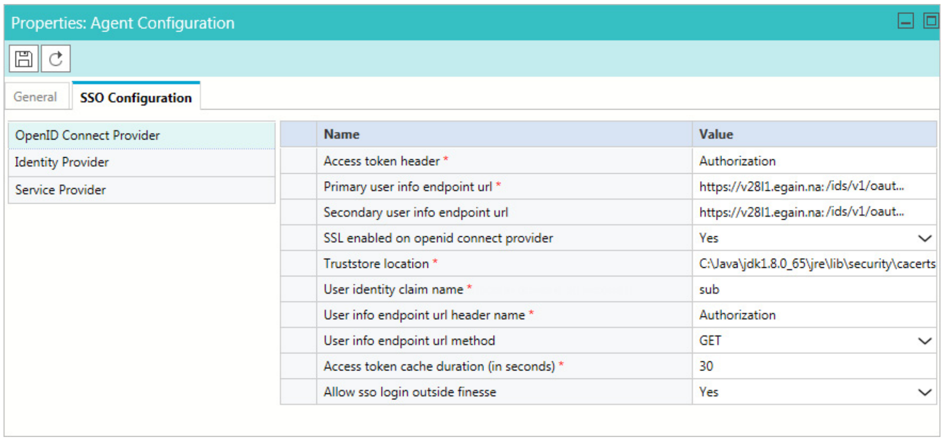
4. Click the **SSO Configuration** tab. Contact your IT department or Cisco IDS support to acquire the necessary information for the following sections, or refer to "Preparing to Configure Single Sign-On for Cisco IDS" on page 154 for more details.

5. In the Cisco IDS Provider section, the following:
   - **Access Token Header**: Name of the request header used by Finesse to pass the Bearer token to ECE.
   - **Primary User Info Endpoint URL**: The User Info Endpoint URL of the primary Cisco IDS server. This URL validates the user token/User Info API. This value can be provided by the Cisco IDS server management team. It is in format `https://`*cisco-ids-1*`:8553/ids/v1/oauth/userinfo` where *cisco-ids-1* indicates the Fully Qualified Domain Name (FQDN) of the Primary Cisco IDS server.

- **Secondary User Info Endpoint URL**: The secondary user Info Endpoint URL of the Cisco IDS server. This value can be provided by the Cisco IDS server management team. It is in format `https://`*cisco-ids-2*`:8553/ids/v1/oauth/userinfo` where *cisco-ids-2* indicates the Fully Qualified Domain Name (FQDN) of the Secondary Cisco IDS server.
- **SSL enabled on OpenID Connect Provider**: If SSL is enabled on the Cisco IDS server, select **Yes**. Otherwise, select **No**.
- **Truststore location**: The directory of the truststore on the server to where the Cisco IDS SSL certificate was imported, for example, *application_server*`\`*ECE_installation_directory*`\Java\jdk\jre\lib\security\cacerts`.

  This field is required if SSL is enabled on the Cisco IDS server. For more information, see "Importing the SSL Certificate to Application Servers" on page 154.
- **User Identity Claim Name**: The name of the claim returned by the User Info Endpoint URL, which identifies the username in Unified CCE. 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. An example of a claim name is "upn".
- **User Info Endpoint URL Header Name**: The request header used by ECE for making Bearer token validation calls to User Info Endpoint URL. This value can be provided by the Cisco IDS server management team. The default value for the header name is "Authorization".
- **User Info Endpoint URL Method**: The HTTP method used by ECE for making Bearer token validation calls to the User Info Endpoint URL. Select one of the options: **GET** or **POST**. This selection should match the IDS server's method.
- **Access Token Cache Duration (in seconds)**: The duration, in seconds, for which a Bearer token should be cached in ECE. Bearer tokens for which validation calls are successful are only stored in caches. (Minimum value: 1; maximum value 30)
- **Allow SSO login outside Finesse:** Set to **Yes** if you wish to allow users with administrator or supervisor roles to sign in to partition 1 of ECE outside of Finesse using their SSO login credentials.

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

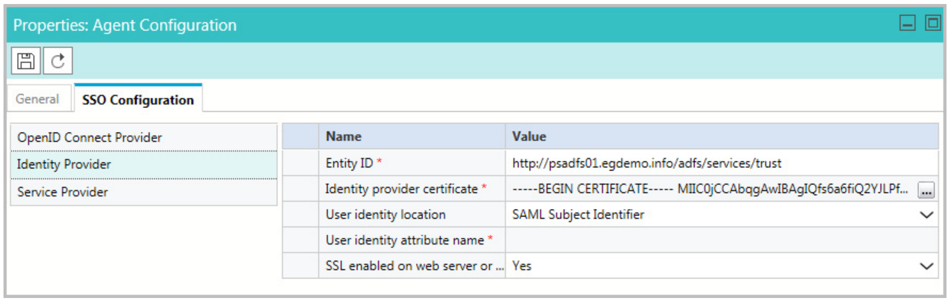


Name	Value
Access token header *	Authorization
Primary user info endpoint url *	https://v28l1.egain.na: /ids/v1/oaut...
Secondary user info endpoint url	https://v28l1.egain.na: /ids/v1/oaut...
SSL enabled on openid connect provider	Yes
Truststore location *	C:\Java\jdk1.8.0_65\jre\lib\security\cacerts
User identity claim name *	sub
User info endpoint url header name *	Authorization
User info endpoint url method	GET
Access token cache duration (in seconds) *	30
Allow sso login outside finesse	Yes

Provide the Cisco IDS details

6. If **Allow SSO login Outside of Finesse** is set to **Yes**, provide the following details in the Identity Provider section:
   - **Entity ID:** Entity ID of the ADFS server. For example, the FQDN of the Shared or Single ADFS 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**.
- **User identity attribute name:** Applicable only when User ID Location value is an SAML attribute. Leave this blank.
- **SSL enabled on web server or load-balancer:** If the Web server or load-balancer used is enabled for SSL, set the value to **Yes**. If not, set the value to **No**.



Name	Value
Entity ID *	http://psadfs01.egdemo.info/adfs/services/trust
Identity provider certificate *	-----BEGIN CERTIFICATE----- MIIC0jCCAbqgAwIBAgIQfs6a6fiQ2YJLPf...
User identity location	SAML Subject Identifier
User identity attribute name *	
SSL enabled on web server or ...	Yes

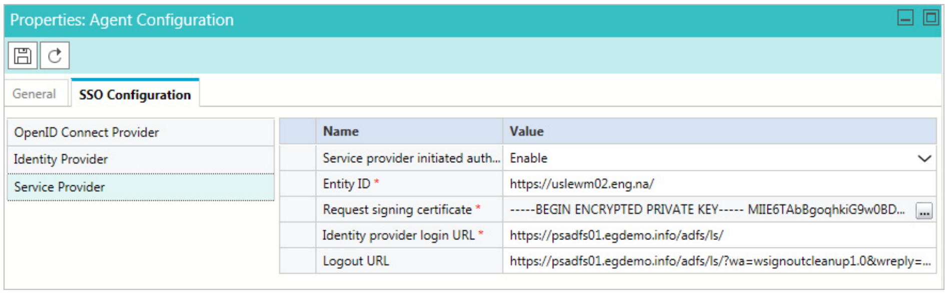
Provide the identity provider details

7. If **Allow SSO login Outside of Finesse** is set to **Yes**, provide the following the Service Provider section:
   - **Service provider initiated authentication:** Set to **Enable**.
   - **Entity ID:** The Web Server or Load Balancer FQDN of ECE.
   - **Request signing certificate:** A Java Keystore (JKS) certificate is needed to provide the necessary information. Consult your IT department to receive the JKS certificate. Click the **Assistance** ... button and provide the following information in the next window and click **OK**.
     - **Java Keystore File:** Provide the file path of your Java Keystore File. This file will be in .jks format and contains the decryption key the system needs to access files secured by SAML.
     - **Alias Name:** The unique identifier for the decryption key.
     - **Keystore password:** The password required for accessing the Java Keystore File.
     - **Key password:** The password required for accessing the Alias' decryption key.

> Important: **The request signing certificate should be converted to a public key certificate and configured in the Relying party trust created on the ADFS server. For more information, see** “Configuring ADFS” on page 154**.**

   - **Identity provider login URL:** The URL for SAML authentication.

- **Logout URL:** The URL to which users are redirected upon logging out.



Name	Value
Service provider initiated auth...	Enable
Entity ID *	https://uslewm02.eng.na/
Request signing certificate *	-----BEGIN ENCRYPTED PRIVATE KEY----- MIIE6TAbBgoqhkiG9w0BD...
Identity provider login URL *	https://psadfs01.egdemo.info/adfs/ls/
Logout URL	https://psadfs01.egdemo.info/adfs/ls/?wa=wsignoutcleanup1.0&wreply=...

Provide the service provider details

8. Click the **Save** button.
9. In the Tree pane, browse to **Administration >** *Partition_Name* **> Settings > Partition**.
10. In the List pane, select the partition settings group.

    The Properties pane refreshes to show the attributes of the group.
11. Next, in the Properties pane, go to the Attributes tab to configure values for settings. From the list, select the **Web server URL or Load Balancer URL** setting to modify. In the **Value** field provide the web server or load balancer FQDN. See “Web Server URL or Load Balancer URL” on page 47 for more information.
12. Click the **Save** button.

Signing in with Cisco IDS

To sign in with Cisco IDS:

1. After you have configured SSO for Cisco IDS, on the Finesse server, in the `ece_config.js` file, replace the following properties:
    - *Load_Balancer_or_Web_Server_Host_Name*: Replace this with ECE Web Server or Load balancer URL that supports HTTPS
    - *Context_Root*: Replace this with the context root used while installing the application.
2. Unified CCE agents configured for SSO in Unified CCE can now access the ECE gadget in Finesse without having to input their credentials. They can now simply sign in to Finesse and click the **Manage 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.
3. The other consoles can be accessed outside of Finesse by users with administrator or supervisor roles, the partition administrator, and the system administrator at the following URLs:

    `http(s)://`*Load_Balancer_URL*`/`*context_root*`/web/view/platform/common/login/root.jsp?partitionId=1`

```
http(s)://Load_Balancer_URL/context_root/web/view/platform/common/login/root.jsp?part
itionId=0
```

Troubleshooting

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

7 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 incoming emails
- Content of outgoing emails
- Knowledge article content created by authors

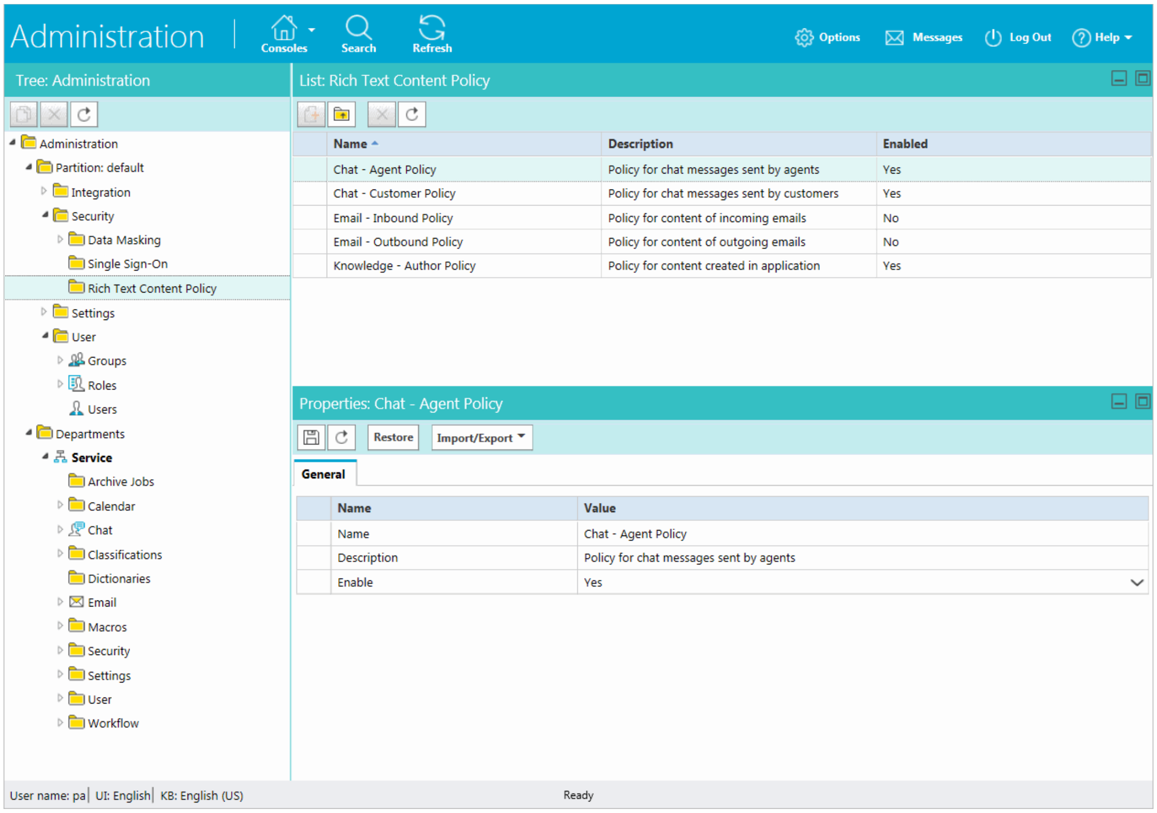
The content policy is an XML file that outlines the rules to be followed while parsing the content. It primarily addresses three things:

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

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

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

Content policies can be adjusted to only allow the use plain text as well. To learn how, see “Using a Plain Text Policy” on page 167.



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

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

Set the Rich Text Content Policies

Enabling and Disabling Rich Text Content Policies

To enable or disable rich text content policies:

1. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security > Rich Text Content Policy**.
3. In the List pane, select one of the content policies.
4. In the Properties pane, under the General tab, set the Enable field to **Yes** to enable, and **No** to disable.
5. Click the **Save** button.

Exporting and Importing Rich Text Content Policies

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

To export and import rich text content policies:

1. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Rich Text Content Policy**.
3. In the List pane, select one of the content policies.
4. In the Properties pane, click the **Import/Export** button.
5. In the dropdown menu, select **Export Policy** and save the XML file to a local directory.
6. Make the desired changes to the policy XML file and save your changes. To learn how to configure the XML file, see "Configuring the Rich Text Content Policy File" on page 164.
7. Return to the Administration Console and select the **Import Policy** option from the same dropdown menu.
8. Locate the updated XML file and import it.
9. Click the **Save** button.

Configuring the Rich Text Content Policy File

The policy XML file has four notable sections:

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

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

Adding a Common Regular Expression

To create a common regular expression:

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

```
<common-regexps>
```

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

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

Allowing a New Tag

To allow a new tag:

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

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

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

Allowing a New Attribute for a Tag

To allow a new attribute for a tag:

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

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

Adding a Rule for an Attribute Value

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

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

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

To add a list of literal values:

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

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

```
<literal value="rtl"/>
</literal-list>
</attribute>
</tag>
```

To add a list of regular expressions:

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

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

Allowing a New CSS Property

To allow a new CSS property:

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

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

Adding a Rule for a CSS Property Value

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

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

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

To add a list of literal values:

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

```
<property name="width">
```

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

To add a list of regular expressions:

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

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

Allowing Links in the Source Attribute of an iframe Tag

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

- Make the following entry in the XML file:

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

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

Using a Plain Text Policy

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

To allow plain text content only:

- Import a policy file with only the following content:

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

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

</anti-samy-rules>
```

Restoring Rich Text Content Policies

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

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

To restore rich text content policies:

1. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Rich Text Content Policy**.
3. In the List pane, select the policy you wish to restore.
4. In the Properties pane, click the **Restore** button.
5. In the window that opens, click **Yes**.

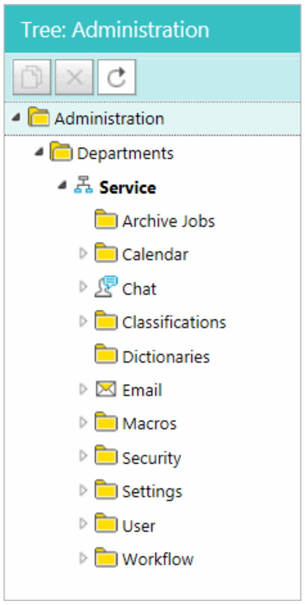
8 Departments

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

About Departments

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

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



The Administration Console tree

The following business objects are available in departments:

- Archive jobs: For more information, see "Archive" on page 194.
- Calendars: For more information, see "Business Calendars" on page 174.
- Chat: For more information, see, *Enterprise Chat and Email Administrator's Guide to Chat and Collaboration Resources.*
- Classifications: For more information, see "Classifications" on page 182.
- Dictionaries: For more information, see "Dictionaries" on page 186.
- Email infrastructure: For more information, see, *Enterprise Chat and Email Administrator's Guide to Email Resources.*
- Data Masking for emails and chat: For more information, see "Data Masking" on page 134.

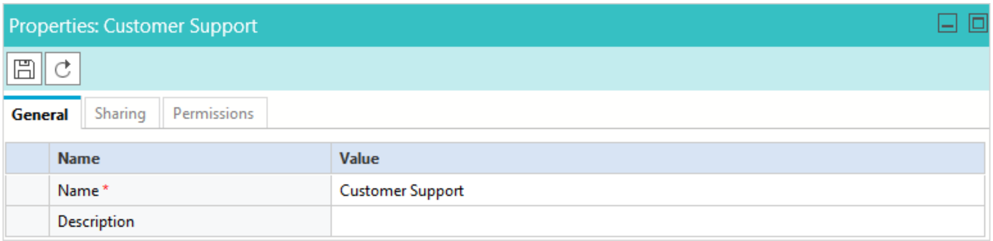
- Macros: For more information, see "Macros" on page 190.
- Settings: For more information, see "Settings" on page 36.
- Users: For more information, see "Users" on page 120.
- Workflows: For more information, see *Enterprise Chat and Email Administrator's Guide to Routing and Workflows.*

Creating Departments

Only a partition administrator can create departments.

To create a department:

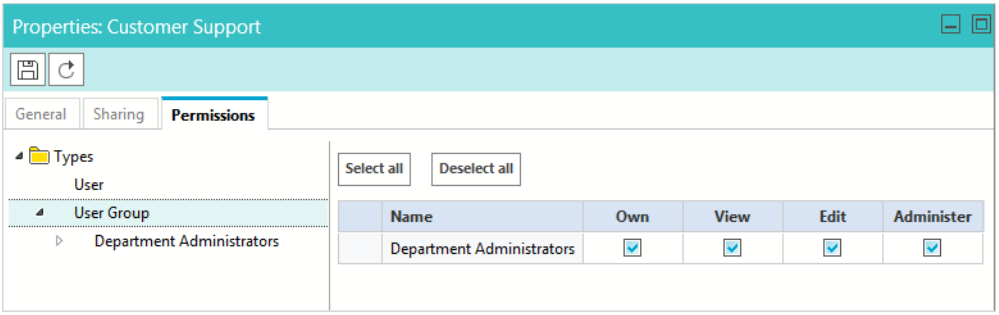
1. In the Tree pane, browse to **Administration > Departments.**
2. In the list pane toolbar, click the **New** button.
3. In the Properties pane, on the General tab, provide the name and general description for the department. The following characters are not allowed in the name: < , . ? : > $ * \ / #



Name	Value
Name *	Customer Support
Description	

Set general properties

4. The sharing section is not currently in use.
5. 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.



Name	Own	View	Edit	Administer
Department Administrators	☑	☑	☑	☑

Assign permissions

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

Configuring Activity Transfer Between Departments

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

To configure activity transfer between departments:

- Enable the **Allow transfer of activities to integrated queues in other departments** partition level setting (page 44). Mapped agents now see mapped queues (that belong to the same MRD) in their home department and in all foreign departments in the Agent Console.

Copying Departments

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

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

#	Object name	Notes
Objects in the Administration Console		
1.	Aliases	Copied as in original department with following exceptions: **Email address** is copied as *address_new_department_name* **Status** is always set as Inactive **User name** is copied as *username_new_department_name*
2.	Blocked Addresses	Copied as in original department
3.	Blocked file extensions	Copied as in original department
4.	Calendars, day labels, shift labels	Copied as in original department
5.	Classifications	Copied as in original department
6.	Chat entry points	Copied as in original department
7.	Customer Associations	Copied as in original department
8.	Data masking for email and chat channels	Not copied
9.	Delivery Exceptions	Copied as in original department
10.	Dictionaries	Copied as in original department
11.	Macros	Copied as in original department
12.	Monitors	Copied as in original department
13.	Queues	Copied as in original department
14.	Service levels	Copied as in original department

#	Object name	Notes
15.	Settings	Copied as in original department
16.	Transfer codes	Copied as in original department
17.	User groups	Copied as in original department
18.	User roles	Copied as in original department
19.	Users	Copied as in original department with following exceptions: **User name** is copied as *username_new_department_name* **Licenses** of users are not copied **Actions, Roles,** and **Permissions** are copied. Note: Permissions are disabled for the copied users until licenses are assigned to them.
20.	Workflows	Copied as in original department with following exception: The **Active** field of workflows is set to **No**.
21.	Archive Jobs	Not copied
Objects in the Knowledge Base Console		
22.	Knowledge Base	Copied as in original department with following exception: User created folders and articles within are copied and same as original department.
Objects in the Tools Console		
23.	Screen Attribute Settings	Copied as in the original department
24.	User Attribute Settings	Copied as in the original department
25.	Relationships - Customer Associations	Copied as in the original department
26.	Activity Types	Copied as in the original department

To copy a department:

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

9

Business Calendars

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

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.

Important: **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, cases, and tasks, and trigger alarms to alert supervisors.

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

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

    8 am to 12 pm: Morning shift

    12 pm to 1 pm: Lunch break

    1 pm to 5 pm: Evening shift
  - Holiday

    12 am to 11.59 pm: Holiday

Use day labels to create calendars.

Managing Shift Labels

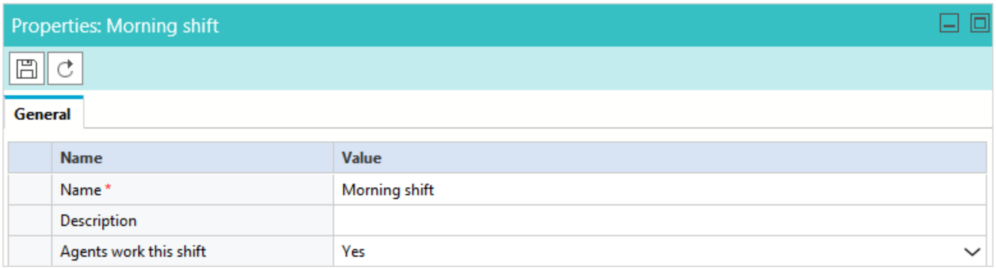
Creating Shift Labels

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

To create a shift label:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> Calendar > Shift Labels.**
2. In the List pane toolbar, click the **New** button.

   The Properties pane refreshes to show the properties of the new shift label.
3. In the Properties pane, in the General tab, provide the following details.
   - **Name:** Type a name for the shift label. Do not use a comma (,) in the name.
   - **Description:** Type a brief description.
   - **Agents work this shift:** Specify if agents work in this shift or not. By default **Yes** is selected. Select **No** if agents do not work in this shift.



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

Set general properties

4. Click the **Save** button.

Deleting Shift Labels

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

To delete a shift label:

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

Managing Day Labels

Creating Day Labels

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

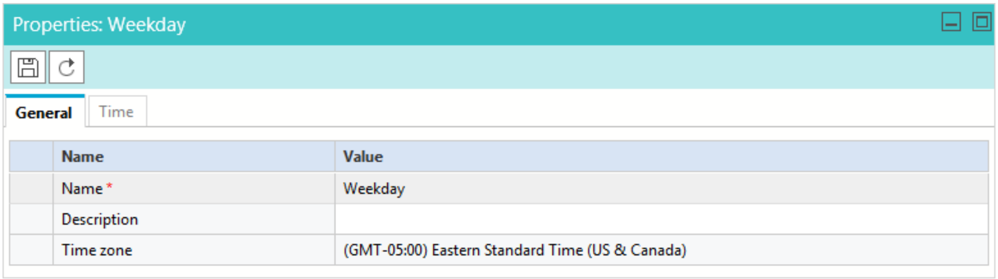
Important: **Before creating day labels, first create the shift labels.**

To create a day label:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> Calendar > Day Labels.**
2. In the List pane toolbar, click the **New** button.

   The Properties pane refreshes to show the properties of the new day label.

3. In the Properties pane, go to the General tab and provide the following details.
   - **Name:** Type a name for the day label. Do not use a comma (,) in the name.
   - **Description:** Type a brief description.
   - **Time zone:** It shows the time zone selected for the department. This field is disabled. If you want to change the time zone for your department, you can do it by changing the **Business calendar timezone** setting**.** For details on how to change this setting, see, “Setting the Time Zone” on page 178.

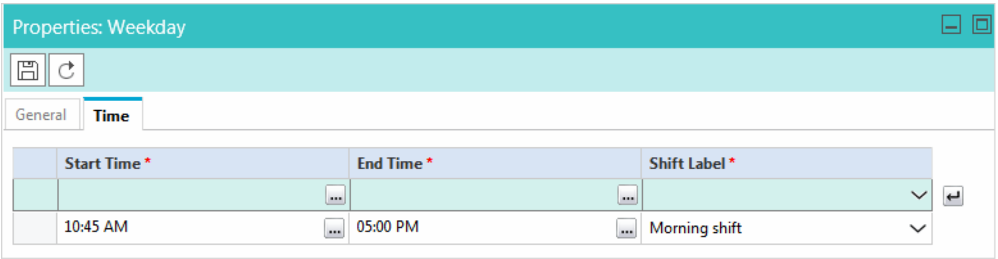


Name	Value
Name *	Weekday
Description	
Time zone	(GMT-05:00) Eastern Standard Time (US & Canada)

Set general properties

4. Next, go to the Times tab and provide the following details.
   - **Start time**: Select the start time for the day label.
   - **End time:** Select the end time for the day label.
   - **Shift label:** From the dropdown list, select the shift label to be used.

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



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

Set start times and end times for day labels

5. Click the **Save** 💾 button.

Deleting Day Labels

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

To delete a day label:

1. In the Tree pane, browse to **Administration** > **Departments** > *Department_Name* > **Calendar** > **Day Labels.**
2. In the List pane, select the day label you want to delete.
3. In the List pane toolbar, click the **Delete** ☒ button.

Managing Business Calendars

Setting the Time Zone

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

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

Important: **It is recommended that you set the time zone first and then configure the calendars.**

To change the time zone setting:

1. In the Tree pane, browse to **Administration** > **Departments** > *Department_Name* > **Settings** > **Department.**

2. In the List pane, select the department settings group.
3. In the Properties pane, go to the Attributes tab.
4. In the Attributes tab, select the **Business calendar timezone** setting**.** From the available time zones, select the time zone for your department.
5. Click the **Save** button.

Creating Business Calendars

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

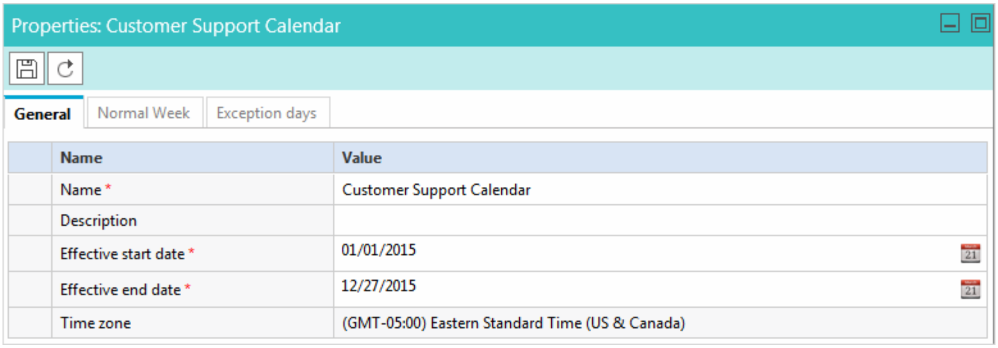
Important: **You need to create day labels before creating calendars.**

To create a calendar:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> Calendar > Calendars.**
2. In the List pane toolbar, click the **New** button.

   The Properties pane refreshes to show the properties of the new calendar.
3. In the Properties pane, go to the General tab, and provide the following details.
   - **Name:** Type a name for the calendar.
   - **Description:** Type a brief description.
   - **Effective start date:** Select the date on which the calendar becomes active. Two calendars in a department cannot have overlapping dates. Also, the start date should be greater than the current date.
   - **Effective end date:** Select the date on which the calendar becomes inactive. Two calendars in a department cannot have overlapping dates. Also, the end date should be greater than the start date.

     On the set end date, the calendar becomes inactive. Once a calendar becomes inactive, the system considers the agents work time as 24*7*365, unless some other calendar becomes active automatically.
   - **Time Zone:** It shows the time zone selected for the department. This field is disabled. If you want to change the time zone for your department, you can do it by changing the **Business calendar timezone** setting. For details on how to change this setting, see, “Setting the Time Zone” on page 178.

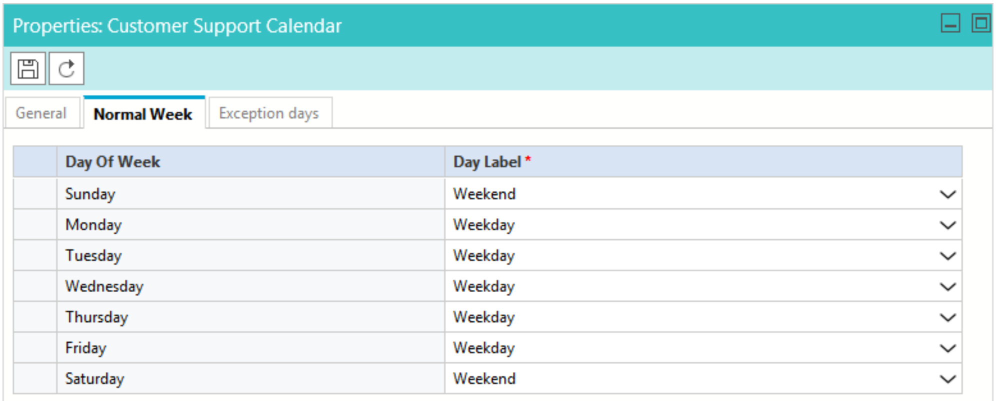


Properties: Customer Support Calendar

Name	Value
Name *	Customer Support Calendar
Description	
Effective start date *	01/01/2015
Effective end date *	12/27/2015
Time zone	(GMT-05:00) Eastern Standard Time (US & Canada)

Set general properties

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

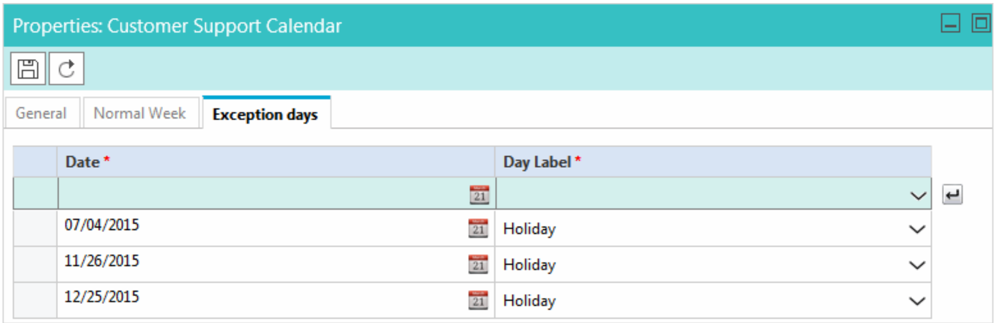


Day Of Week	Day Label *
Sunday	Weekend
Monday	Weekday
Tuesday	Weekday
Wednesday	Weekday
Thursday	Weekday
Friday	Weekday
Saturday	Weekend

Configure the calendar for a normal week

5. Lastly, go to the Exceptions tab. Specify the day labels to be used for exception days, like holidays, weekends, etc. Select the date on which there is some exception, and then select the day label to be used for that day.

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



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

Configure the calender for the exception days, like holidays

6. Click the **Save** button.

Deleting Business Calendars

To delete a calendar:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> Calendar > Calendars.**
2. In the List pane, select the calendar you want to delete.
3. In the List pane toolbar, click the **Delete** ✕ button.

Managing Daylight Saving Changes

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

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

10 Classifications

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

About Classifications

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

- Categories
- Resolution codes

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.

Managing Categories

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

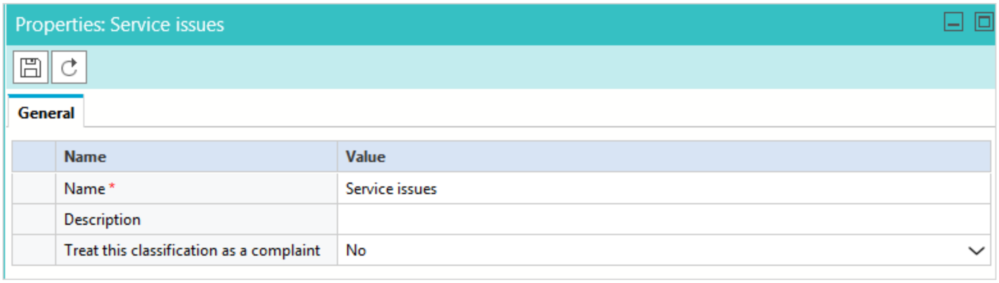
- Creating Categories on page 183
- Deleting Categories on page 184

Creating Categories

To create a category:

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

- **Treat the classification as a complaint:** Select **Yes** to create a complaint type of category.



Properties: Service issues

General

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

Set general properties

4. Click the **Save** button.

Deleting Categories

To delete a category:

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

Managing Resolution Codes

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

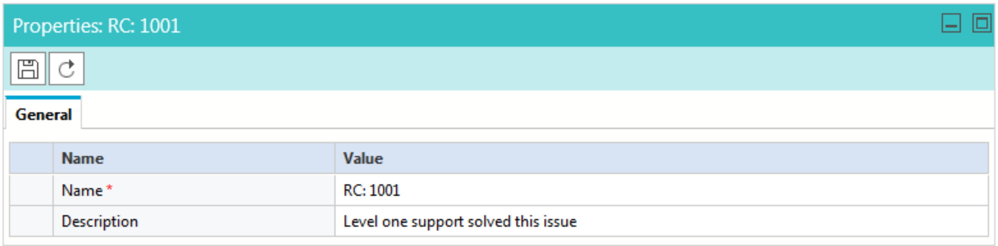
- Creating Resolution Codes on page 184
- Deleting Resolution Codes on page 185

Creating Resolution Codes

To create a resolution code:

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

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



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

Set general properties

4. Click the **Save** 🖫 button.

Deleting Resolution Codes

To delete a resolution code:

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

11

Dictionaries

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

About Dictionaries

Dictionaries refer to a list of words stored in the system for reference. Agents use dictionaries to check spellings in outgoing emails. Each department comes with 13 predefined dictionaries and one of them is configured as the default dictionary. A department can have only one default dictionary and it can be changed according to the business requirements.

Dictionaries are available in the following languages:

1. Danish
2. Dutch
3. English (UK)
4. English (US)
5. Finnish
6. French
7. German
8. Italian
9. Norwegian (Bokmal)
10. Portuguese
11. Brazilian Portuguese
12. Spanish
13. Swedish

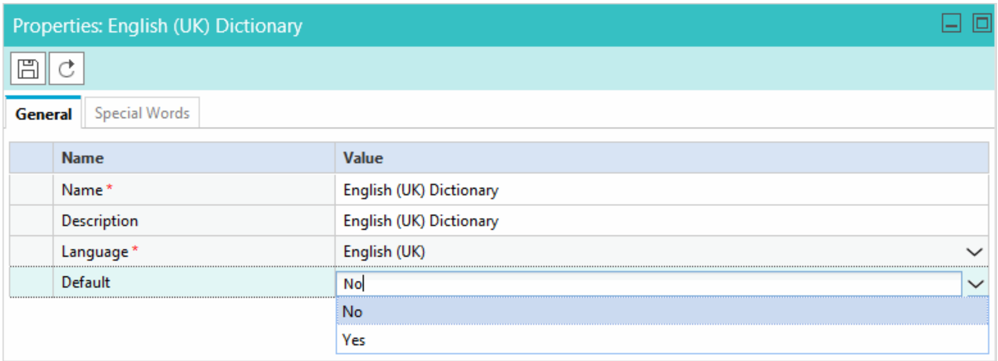
Important: **The application does not have dictionaries for the following languages: Chinese (Simplified), Chinese (Traditional), Czech, Greek, Japanese, Korean, Norwegian (Nynorsk), Portuguese (Brazilian), and Turkish.**

Choosing a Default Dictionary

To choose a default dictionary:

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

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



Properties: English (UK) Dictionary

Name	Value
Name *	English (UK) Dictionary
Description	English (UK) Dictionary
Language *	English (UK)
Default	No

Set a dictionary as the default dictionary for a department

4. Click the **Save** button.

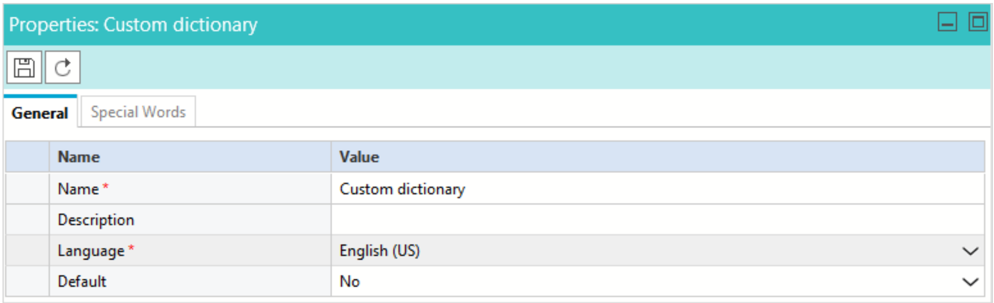
Creating Dictionaries

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

To create a new dictionary:

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

   Click the **Save** button to enable the **Default** field.
   - **Default:** Select **Yes** to make this the default dictionary of the department.



Properties: Custom dictionary

Name	Value
Name *	Custom dictionary
Description	
Language *	English (US)
Default	No

Configure the general properties

4. Click the **Save** button.

Adding Blocked Words

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

To add blocked words:

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

Approving Suggested Words

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

To approve suggested words:

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

Viewing Approved Words

To view the approved words:

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

12

Macros

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

About Macros

Macros are commands that fetch stored content. They are easy to use, and display the actual content, when expanded. Macros enable you to enter a single command to perform a series of frequently performed actions. For example, you can define a macro to contain a greeting for email replies. Instead of typing the greeting each time, you can simply use the macro. It is important to note that a macro's expansion is contextual to the object, and two macros of similar looking attribute expand differently depending upon the context object. For example, the macros "Email address of the contact point" and "Contact point data of the activity", both return the email address of the customer, but the first one returns the email address saved in the customer profile and the second one returns the email address associated with the activity in which the macro is used.

You can create two types of macros:

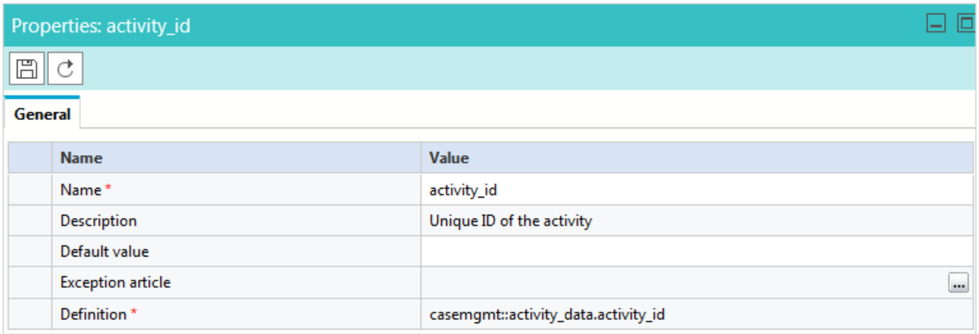
1. Business Objects macros: In Business Objects you can create macros for several objects. For example, Activity data, Customer data, User data, etc. You have to define an attribute to a macro from the list of system provided attributes. Please note that you can define only a single attribute for each macro.
2. Combination macros: In Combination Macros you can create macros with multiple descriptions. That is, you can combine multiple macros within a single macro. Multiple macros can be selected from both Business Objects and Combination macro types.

Creating Business Object Macros

To create a business object macro:

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

- **Definition:** Click the **Assistance** ⋯ button and from the Select Attribute window, select the attribute that defines this macro. Please note that for any date attributes (for example, case creation date) are displayed in the GMT timezone.



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

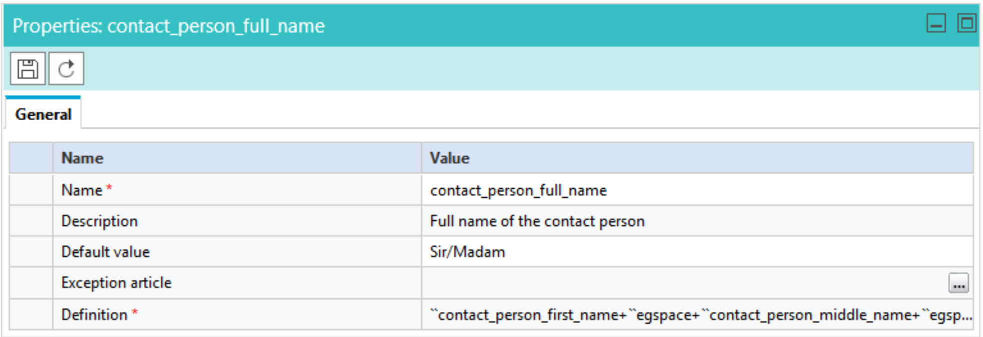
Set general properties

4. Click the **Save** 🖫 button.

Creating Combination Macros

To create a combination macro:

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



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

Set general properties

4. Click the **Save** 💾 button.

Deleting Macros

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

To delete a macro:

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

13

Archive

Important: **The Archive Jobs node is available only in installations that use the Standard Edition of Microsoft SQL. Installations using the Enterprise edition of Microsoft SQL Server database, leverage the underlying table partitioning capabilities of the Enterprise edition of the database server.**

About Archives

Data is stored in the active database. With time, the size of the data usually increases to a point where it begins to affect the performance of the system. 150 GB should be considered the maximum limit for the size of the active database, after which we recommend archiving to avoid performance issues. Hence, it is important that data that is not in use anymore is stored somewhere other than the active database.

- Archiving is a systematic process which moves data from the active database to the archive database. Periodic archiving helps to keep the size of the active database within prescribed levels, thereby improving the performance of the system.

What Can You Archive?

You can archive cases and activities that are more than eight days old. Attachments of archived activities remain on the file server and the link between archived activities and attachments is preserved even after activities are archived.

Once archived, a case or activity cannot be “unarchived.” If a customer replies to an archived case, a new case gets created.

About Archive Jobs

An archive job is a process that runs automatically at a scheduled time and archives data based on a specified criteria (such as, the age of the data and the queue to which it belongs). You can create multiple archive jobs in a department, but two jobs cannot have overlapping schedules. A job runs only when it is in active state.

When a job is run, the archiving of data happens in batches. Each archive job is broken into batches of 5000 cases. For example, if a job is scheduled to archive 22000 cases, it processes them in batches of 5000 cases. To archive 22000 cases, it will run four batches of 5000 cases and a fifth batch of 2000 cases. Breaking of a job into batches ensures that if an error occurs while archiving the data, or if the archive process is stopped and restarted, only a small piece of data has to be processed again.

Every batch completes archiving in two steps:

- First, it inserts data from the active database to the archive database.
- After successfully inserting the data in the archive database, it deletes the data from the active database.

Important: **For archive jobs to work, the Scheduler and Archive services should be running.**

Default Quarterly Archive Job

When the application is installed, a Default Quarterly Archive Job is created in the system. This job runs on Sundays and archives all closed cases and completed activities for the last 90 days. You can edit this archive job as required.

Who can Manage Archive Jobs?

Only users with appropriate actions can manage archive jobs. The actions required for managing archive jobs are:

- View archive jobs: For viewing the Archive node and archive jobs in a department
- Edit archive jobs: For editing jobs
- Create archive jobs: For creating jobs
- Delete archive jobs: For deleting jobs
- Purge archive jobs: For deleting archived data

Partition administrators have all these actions assigned to them by default, but these actions have to be given explicitly to department administrators. Since archiving is a very sensitive process, discretion should be used while assigning archiving actions to users.

Archive Criteria

While creating archive jobs, you can specify two criteria.

1. The relative age of activities and cases to be archived: You need to specify the relative age of cases and activities that should be picked up for archive. The age can be given in days, weeks, or months.

   For example: You set the job to archive closed cases and completed activities that were closed or completed one month before the date on which the archive job runs. It means the job will archive:

   - All completed activities that belong to cases that were closed one month before the job run.
   - All completed activities that do not have any case associated and were completed one month before the job run.
   - All cases that were closed one month before the job run.

   Important: **Since activities belonging to a case can be present in multiple departments, archiving checks if the first activity of a case belongs to the department in which the job is run. If it is, only then that case and its associated activities are archived.**

2. The queue to which the completed activities and closed cases belong: When you specify a queue, the job archives only the cases and activities that belong to that queue.

   Important things to note are:

   - If the last activity of a closed case belongs to a queue specified in a filter, then the case with all its constituent activities is archived.
   - If there are activities that belongs to the queue specified in the filter, with no case association, then those activities are archived.

- If the last activity in a closed case does not belong to any queue, the case and all its constituent activities do not get archived.

Planning the Schedule of Archive Jobs

When an archive job runs, it puts additional load on the system. To ensure that the productivity of agents is not affected by the archive jobs running on the system, plan the schedule of archive jobs in a way that they do not run at peak business hours.

While scheduling jobs you can specify two things. They are:

- The days of the week when an archive job should run.
- The time of the day when the job should run. In this, you can select between two options. They are:
  - Set the job to run throughout the day. For example, if your call center is closed on Saturday and Sunday, you can schedule the archive jobs to run throughout the day, on Saturday and Sunday.
  - Set the job to run between specified start and end time. For example, if your call centre runs 24/7, and has less load from 10 pm to 6 am on Monday and Tuesday, then you can schedule the archive jobs to run from 10 pm to 6 am, on Monday and Tuesday.

Two active jobs in a department cannot be scheduled for the same or overlapping time. For example, you cannot have a job scheduled from 4 pm to 6pm, and another job scheduled from 5 pm to 7 pm on the same day. However, you can have one job scheduled from 4 pm to 6pm, and another from 6pm to 8pm on the same day.

About Job Runs

A job run is a record that indicates the time at which the archive job started and ended, the status of the job, whether it is running, completed, or failed, and the number of cases and activities handled by the archive job. Every time the system runs an archive job, a new job run is created. For example, if an archive job is scheduled to run from Monday to Friday between 6 am and 9 am, and the job runs successfully every day, then there will be six job runs for the archive job. You can view all the job runs for an archive job in the History tab of the Properties pane.

A job run can have one of the following status:

- Running: The archive job is running and is in progress.
- Completed: The job run was completed when:
  - The time allotted for the job to run is over.

  Or

  - There was no more data left for archiving.
- Failed: The job encountered some problem while archiving and could not run successfully.

  Important: **If a job fails, no other scheduled job can run in the system till the failure of the job is resolved and the failed job is restarted manually.**

  An archive job can fail because of one of the following reasons:

  - Network connection is down
  - Application database or archive database is down

  - Archive database storage is full
  - Internal error in the archive process
- Stopped: The job has been stopped manually while it was running.

About Purging

As the archive jobs run, they keep moving the data from the active to the archive database, and the data size on the archive database increases. At some time the need will arise to delete the archived data. Purge is a process which helps you to systematically delete data from the archive database. Once purged, the information is lost permanently and it cannot be recovered. Data is purged job run wise and you can purge only those job runs that have completed successfully. You cannot purge a job run that is in a running state or has failed because of some error. Purge also deletes the attachments associated with the activities being purged.

> Important: **Once you start purge, it cannot be stopped, and the purged data is lost and cannot be recovered.**

When a job run is purged, it can have one of the following status:

- Purge started: The job run has been queued for purge.
- Purge completed: Purge has completed successfully.
- Purge failed: Purge has failed because of some error.

Managing Archive Jobs

Creating Archive Jobs

An archive job is a process that runs automatically at a scheduled time, and archives data based on the specified criteria (such as, the age of data and the queue to which it belongs). You can create multiple archive jobs in a department, but two jobs cannot have overlapping schedules. A job runs only when it is in active state.

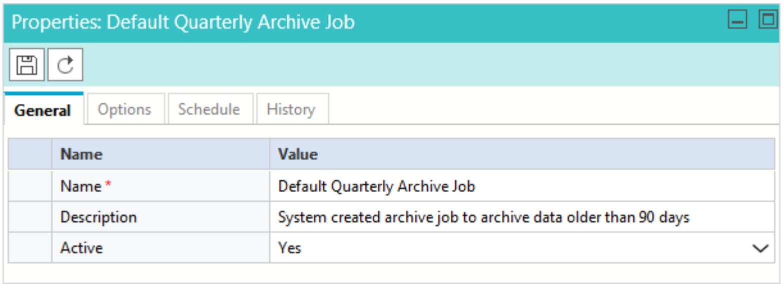
After you create a job, it runs automatically on the scheduled date and time. You cannot start a job manually. However, when a job starts running you can stop and restart it manually.

To create an archive job:

1. In the Tree pane, browse to **Administration** > **Departments** > *Department_Name* > **Archive Jobs**.
2. In the List pane toolbar, click the **New** ⊞ button.

   The Properties pane refreshes to show the attributes of the new job.
3. In the Properties pane, on the General tab, provide the following details.
   - **Name:** Type the name of the archive job. This is required information.
   - **Description:** Type a brief description.

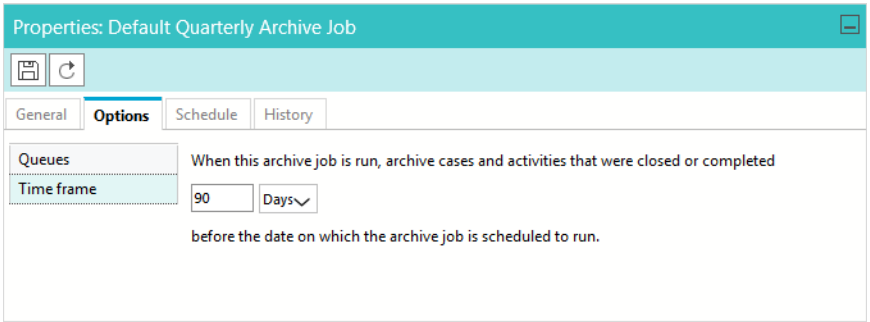
- **Active:** By default the status of the job is not active. Select **Yes** to make it active. A job can run only when it is in active state.



Name	Value
Name *	Default Quarterly Archive Job
Description	System created archive job to archive data older than 90 days
Active	Yes

Set general properties

4. Next, go to the Options tab. Here you set the criteria for the archive job.
   - In the Timeframe section, specify that when the archive job is run, archive the closed cases and completed activities that were closed or completed *n* days before the date on which the archive job runs. Select the relative time frame in days, weeks, or months. For example, if you want to archive cases and activities which were completed two months before the date on which the archive job runs, then select two months.



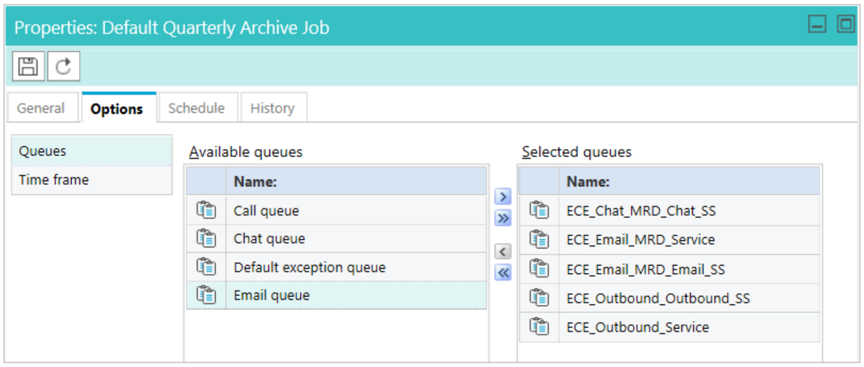
When this archive job is run, archive cases and activities that were closed or completed

90 Days

before the date on which the archive job is scheduled to run.

Set the time frame option

   - In the Queues section, select the queues on which the archive job should run.



Available queues

Name:
Call queue
Chat queue
Default exception queue
Email queue

Selected queues

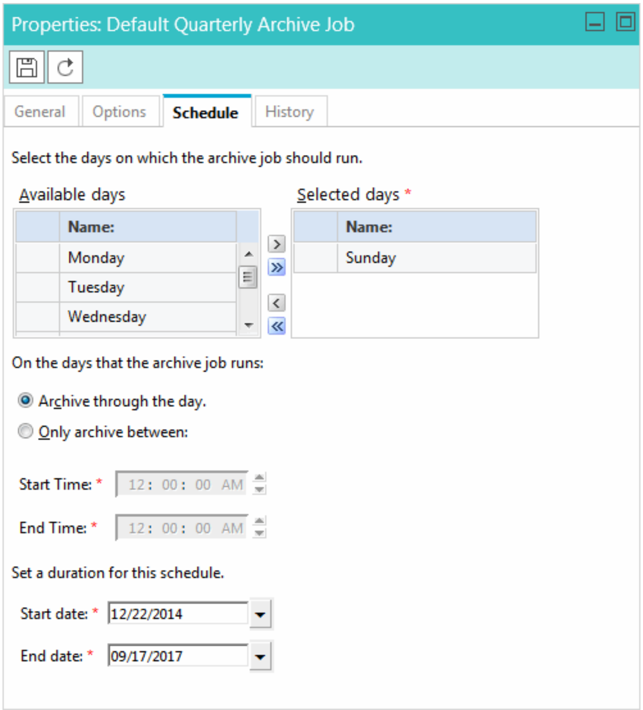
Name:
ECE_Chat_MRD_Chat_SS
ECE_Email_MRD_Service
ECE_Email_MRD_Email_SS
ECE_Outbound_Outbound_SS
ECE_Outbound_Service

Select queues

5. Next, go to the Schedule tab. Here specify the days and time when the archive job should run.
   - Select the days on which the archive job should run.
   - Specify the time of the day when the archive job should run. There are two options available.

- **Archive throughout the day:** For example, you can schedule the archive job to run on Saturday and Sunday throughout the day.
- **Archive only between the specified start and end time:** For example, you can schedule the archive job to run on Saturday and Sunday from 8 pm to 11 pm.

- Select the duration for which you want to schedule the archive job.



Select the days on which the archive job should run.

Available days

Name:
Monday
Tuesday
Wednesday

Selected days *

Name:
Sunday

On the days that the archive job runs:

● Archive through the day.

○ Only archive between:

Start Time: * 12: 00: 00 AM

End Time: * 12: 00: 00 AM

Set a duration for this schedule.

Start date: * 12/22/2014

End date: * 09/17/2017

Configure the schedule for the archive job

6. Click the **Save** button.

Important: The History tab is enabled only after you save the job.

From the History tab you can view the list of job runs. If you are creating a new job, the list will be empty. You can also stop, restart, and purge the job runs from the History tab.

Deleting Archive Jobs

Important: A job cannot be deleted if it has job runs that have not been purged. Before you can delete an archive job, you have to purge the data archived by that job.

To delete an archive job:

1. In the Tree pane, browse to **Administration** > **Departments** > *Department_Name* > **Archive Jobs**.
2. In the List pane, select the archive job you want to delete.
3. In the List pane toolbar, click the **Delete** button.

4. A message appears asking to confirm the deletion. Click **Yes** to delete the archive job.

Managing Job Runs

Viewing Job Runs

Every time an archive job runs, a record is created indicating the start and end time of the job, if the job is in running state, if it completed successfully or it failed, and the number of cases and activities archived by the job. Each record is called a Job run, and all job runs for an archive job can be viewed from the History tab.

To view a job run:

1. In the Tree pane, browse to **Administration** > **Departments** > *Department_Name* **> Archive Jobs**.
2. In the List pane, select an archive job.
3. In the Properties pane, go to History tab. Here you can see a list of job runs. You can see the following details about the job run.
    - **Start time:** Time when the job run started.
    - **End time:** Time when the job run ended.
    - **Status:** Status can be running, completed, or failed.
    - **Cases archived:** Number of cases archived.
    - **Activities archived:** Number of activities archived.

Stopping Job Runs

Important: **A job can be stopped only if it is in running state.**

To stop a job:

1. In the Tree pane, browse to **Administration** > **Departments** > *Department_Name* > **Archive Jobs**.
2. In the List pane, select an archive job.
3. In the Properties pane, go to the History tab and select the job run you want to stop.
4. Click the **Stop** button.

Restarting Job Runs

You will need to restart a job if:

- You stopped the job manually: If you restart a job within its scheduled time, it will run till the end of the schedule. If the restart happens outside the scheduled time, then it will only complete the batch it was archiving at the time you stopped the job.

- The job failed while running: In case of a failure, if the job is restarted within the scheduled time, it runs till the end of the schedule. And, if the restart happens outside the schedule time, it will only complete the batch it was archiving at the time of failure.

Important: **If a job run fails and its schedule expires, such a job run can also be restarted. On restart it will only complete the batch it was archiving at the time of failure.**

To restart a job:

1. In the Tree pane, browse to **Administration** > **Departments** > *Department_Name* > **Archive Jobs**.
2. In the List pane, select an archive job.
3. In the Properties pane, go to the History tab and select the job run you want to restart.
4. Click the **Restart** button.

Purging Archived Data

As archive jobs run, they keep moving the data from the active to the archive database, and the data size on the archive database increases. At sometime the need will arise to delete the archived data. Purge is a process which helps you to systematically delete data from the archive database. Once purged, the information is lost permanently and it cannot be recovered. The data can be purged job run wise, and you can purge only those job runs that have completed successfully. You cannot purge a job run that is in a running state or has failed because of some error. Purge also deletes the attachments associated with the activities being purged.

Important: **Once you set up a job run for purge, it cannot be stopped, and the purged data is lost and cannot be recovered.**

When a job run is purged, it can have one of the following status.

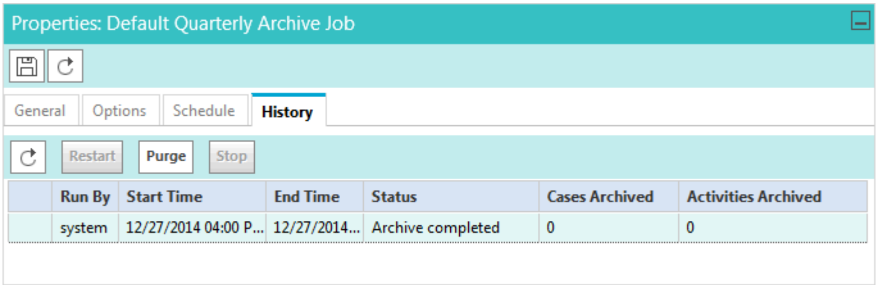
- Purge started: The job run has been queued for purge
- Purge completed: Purge has completed successfully
- Purge failed: Purge failed because of some errors

Important: **Purge of the archived data does not start immediately. Data is purged at the purge interval defined at the time of installing the application and it cannot be changed.**

To purge archived data:

1. In the Tree pane, browse to **Administration** > **Departments** > *Department_Name* > **Archive Jobs**.
2. In the List pane, select an archive job.
3. In the Properties pane, go to the History tab and select the job run you want to purge.

4. Click the **Purge** button.



	Run By	Start Time	End Time	Status	Cases Archived	Activities Archived
	system	12/27/2014 04:00 P...	12/27/2014...	Archive completed	0	0

Purge the archived data

The status of the job run changes to Purge started, and it shows the name of the user who started the purge and the time at which the purge started.