eGain SOLVE

Fall 2019

Administrator's Guide to Administration Console

easy with eGain

eGain® Administrator's Guide to Administration Console, December 19, 2019

License Agreement

Proprietary Information; Government Use

Trademarks

Third-Party Copyrights

Contact information

- Email for documentation feedback and requests: publications@egain.com

Contents

Preface

Welcome to **eGain Solve™**, the leading cloud solution for omnichannel customer engagement. Powered by a unified platform for omnichannel interactions, knowledge, Artificial Intelligence (AI), and full-spectrum analytics, the applications suite solves the following business challenges:

- Deliver superior experiences for the digital and omnichannel customer
- Make millennial advisors as good as the best ones through AI and knowledge-guided service interactions and processes
- Make innovation in digital CX easy with rich, out-of-the-box solution capabilities, complemented by risk-free consumption model and agile services

About this Guide

eGain 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.

Document Conventions

This guide uses the following typographical conventions.

Convention	Indicates
Italic	Emphasis, or the title of a published document.
Bold	An item in the user interface, such as a window, button, or tab.
`Monospace`	A file name or command.
Script	A variable, which is a placeholder for user-specific text provided by the user. Or, text that must be typed by the user.

Document conventions

Other Learning Resources

Various learning tools are available within the product, as well as on the product CD and our website. You can also request formal end-user or technical training from eGain Education Services.

Online Help

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

Use	To view
Help button	All topics in the online help; the **Help** button appears in the console toolbar on every screen, as well as on most windows.
F1 keypad button	Context-sensitive information about the item selected on the screen.

Document Set

The document set can be found in the `Documentation` folder on the eGain Application CD. It contains the following documents:

- *eGain 17 Release Notes*
- *eGain 17 System Requirements (Windows)*
- *eGain Browser Settings Guide*

Installation Guides

- *eGain Installation Guide*
- *eGain Solve for Cisco Installation Guide for Cloud Deployments*

Upgrade Guides

- *eGain Upgrade Guide*
- *eGain Solve for Cisco Upgrade Guide for Cloud Deployments*

Configuration Guides

- *Configuration Guide for Unified CCE*

Companion Guides

- *eGain Solve for Cisco Companion Guide*

User's Guides for Interaction Consoles

- *eGain Agent's Guide*
- *eGain Social Media Manager's Guide*

User's Guides for Authoring Consoles

- *eGain Knowledge Manager's Guide*
- *eGain Knowledge Manager's Guide to Portals*

- *eGain Author’s Guide to Knowledge Base*
- *eGain Author’s Guide to Guided Help*

User’s Guides for Management Consoles

- *eGain Supervisor’s Guide*
- *eGain Administrator’s Guide to Administration Console*
- *eGain Administrator’s Guide to Chat and Collaboration Resources*
- *eGain Administrator’s Guide to Email Resources*
- *eGain Administrator’s Guide to Routing and Workflows*
- *eGain Administrator’s Guide to Offers Console*
- *eGain Administrator’s Guide to Data Adapters*
- *eGain Administrator's Guide to Reports Console*
- *eGain Administrator’s Guide to System Console*
- *eGain Administrator’s Guide to Tools Console*

eGain Education Services

Training programs are available for agents, managers, and administrators, both at eGain offices or customer sites. These programs can be tailored to meet your specific needs. For more information about course schedules and enrollment, email register@eGain.com or visit http://www.egain.com/products/egain_university.

Contact Information

If you have a current support agreement, you can submit a webform inquiry, or contact eGain Support by email, phone, or fax.

Channel	Details
Web	www.egain.com
Email	publications@egain.com
Voice	US: 408-636-4500; UK: 01635-800087
Fax	US: 408-636-4400; UK: 01635-41624

We are interested in hearing your comments about this document—particularly if it fell short of your needs or expectations. Please email all feedback to publications@egain.com. If you are reporting an error, include the chapter title and page number.

1

Console Basics

- Important Administration Tasks
- Key Terms and Concepts
- Sharing of Business Objects
- Accessing the Application
- Elements of the User Interface

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

Important Administration Tasks

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

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

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
  - Advisor Desktop
  - Knowledge Base Console
  - Reports Console
  - Supervision Console
  - Social Console
  - System Console
  - Offers 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

Customer information can be shared across all departments. Other resources such as agents and activities can also be shared between departments. Sharing of such resources is one-directional, which means that even if Department A shares its agents with Department B, Department B could decide not to share its agents with Department A.

Settings

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

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

For more information, see "Settings" on page 39.

Users

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

Users can be created at three levels:

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

Two users are created during the installation:

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

For more information, see "Users" on page 132.

User Roles

A role is a set of permissible actions for various business resources. An agent's role, for instance, would include actions such as "Edit customer," and "Add notes." You can 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 132.

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 132.

Email Infrastructure

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

The following objects can be configured for emails:

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

For more information, see *eGain Administrator's Guide to Email Resources.*

Chat and Collaboration Infrastructure

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

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

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

For more information, see *eGain Administrator's Guide to Chat and Collaboration Resources.*

Data Masking for Email and Chat

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

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

Data masking is available for emails and chats. For more information, see "Data Masking" on page 197.

Data Adapters

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

The following objects should be configured for data adapters:

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

For more information, see *eGain Administrator's Guide to Data Adapters.*

Workflows

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

- Alarm workflows
- General workflows
- Inbound workflows
- Outbound workflows

For more information, see *eGain Administrator's Guide to Routing and Workflows.*

Queues

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

For more information, see *eGain 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 *eGain 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 268.

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 275.

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 287.

Macros

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

You can create business object macros for:

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

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

For more information, see “Macros” on page 291.

Personalization

Navigating an expansive knowledge base with countless articles can become a challenge. Website visitors and agents alike may have difficulty locating the articles they need on knowledge portals with massive libraries of articles, even with specially tuned search tools. To assist users with knowledge searches, tags can be applied to articles as a form of metadata.

The Personalization section is where administrators can create the following:

- Tag Categories
- Tag Groups
- Tags
- User Profiles
- Publish Views

For more information, see *eGain Knowledge Manager’s Guide.*

Guided Help Profiles

Profiles allow the user to separate the logical parts of the case base and thus restrict and control access to the case bases. A profile is required for any user to view data within the case base, so by default, the system profile is generally used and assigned to most users and consequently most case bases are built with case base objects that are defined to use the system profile, thus allowing all areas of the case base to be accessed by all users.

For more information, see “Guided Help Profiles” on page 281.

Products

Products allow you to efficiently manage, and organize the list of company’s products. You can create a catalogue of all your products, and also attach files or web pages, and articles from the knowledge base, thereby, providing more information regarding those products. This is helpful for agents, as they can use it to associate products with customers. This adds to the details of a customer, thereby enabling the agent to know and serve the customer better.

For more information, see “Products” on page 295.

Secure Messaging

Secure Messaging allows you to create secure message centers for online customers. Secure message centers are highly secure web portals, meant for exchanging sensitive information with customers. Agents working on outgoing messages can mark them as secure. These messages are not sent directly to the recipient’s primary email, but are instead sent to the customer’s secure inbox. They can then access the message sent by the agent by logging in to the secure message center.

For more information, see *eGain Administrator’s Guide to Email Resources*.

Solve

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

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 Advisor Desktop: 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 196.
- Business calendars
- Queues, service levels, and workflows
- Chat infrastructure
- Email infrastructure
- Data masking
- Data adapters
- Profiles
- Classifications
- Dictionaries
- Macros
- Personalization
- Products
- Secure Messaging

KB Console

- KB Articles
  - Not shared
  - Exception: Foreign users can view and create articles in the departments they are shared with.
- Portals
  - Not shared
  - Exception: Foreign users can view and create portals in the departments they are shared with.
- Case Bases
  - Not shared
  - Exception: Foreign users can view and create case bases 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.

Advisor Desktop

- Not shared
- Exceptions:
  - Customers: If customer departmentalization is not enabled (see "Customer Departmentalization" on page 66), 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).
  - If two departments are shared, users from one department can transfer activities to another department. For details, see "Sharing Department Resources" on page 264.
  - Foreign users can work on activities from departments they are shared with. And, while working on these activities they can access the data links, KB, and classifications of the foreign department.

Accessing the Application

Users of varying roles, licenses, and permissions can access different consoles in the Solve application. To help facilitate the different types of users attempting to access their own side of the application, a landing page with direct links to the different tools and desktops of Solve is provided. It is recommended to bookmark the landing page to make accessing the different consoles of the application easier.

The landing page can be accessed via the web server or load balancer URL, for example: `http://`*Web_server.company.com*`/`*partition_name* in your browser, where *Web_server.company.com* is the fully qualified domain name of your web server and *partition_name* is the virtual directory created for this partition. If you have configured the web server to use SSL, or if your system is an eGain Cloud installation, then the URL is `https://`*Web_Server.company.com*`/`*partition_name*. For example, `https://v17.egain.com/default`. This URL is established and configured during the installation process. For more information, see the Logging in to the Application section of the *eGain 17 Installation and Configuration Guide*.

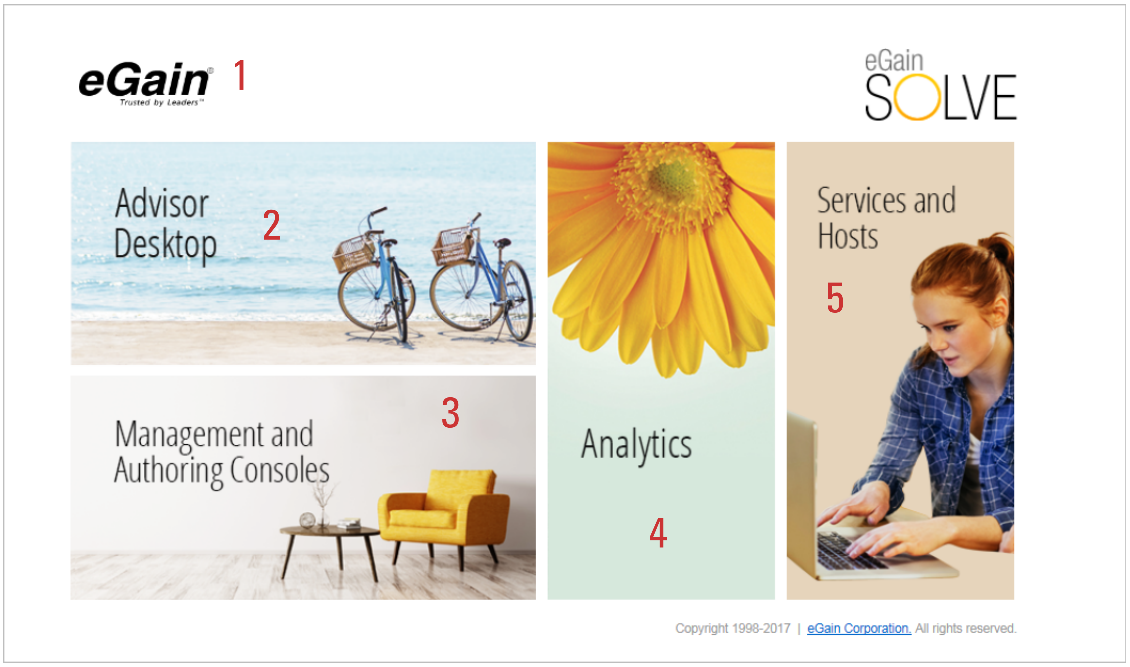
Important: **Once single sign-on has been configured on a system, agents should use the single sign-on URLs to access the application. For more information about configuring SSO, see “Agent Single Sign-On” on page 218.**

The landing page is provided at the time of installation and contains the following areas.

1. **Company Logo:** An image in the top corner of the landing page to help provide context to new users accessing the application. This image can changed in the Landing page settings at the partition level. For more information, see “Landing Page Settings” on page 47.
2. **Advisor Desktop:** The Advisor Desktop is a service console and is designed specifically for use by customer service agents to handle service interactions and tasks. This console can be accessed from the landing page on Chrome, Firefox, and Internet Explorer.
3. **Management and Authoring Consoles:** The consoles available here make up a majority of the Solve application. The types of tasks that can be performed here range from authoring articles, to creating offers, to running monitors as a supervisor, to general administrative tasks like creating users. The following consoles can be access from the **Management and Authoring Consoles** button:
   - Administration
   - Knowledge Base
   - Offers
   - Reports
   - Social
   - Supervision
   - System
   - Tools
4. **eGain Analytics:** eGain Analytics is a powerful 'measure and manage' platform that gives business users visibility and control of customer contact operations across multiple channels and touchpoints. Analytics must be installed for this button to appear and the URL to the Analytics login page must be configured in the Landing page settings.
   - For details about installing and configuring Analytics, see *eGain Analytics Installation and Configuration Guide*.

- For details about configuring the Analytics button on the landing page, see “Landing Page Settings” on page 47.

5. **Services and Hosts:** This provides access to the administrative consoles on the system partition. Access to this partition and its tools is restrict to system administrators.


eGain
Trusted by Leaders
1
eGain SOLVE
Advisor Desktop
2
Management and Authoring Consoles
3
Analytics
4
Services and Hosts
5
Copyright 1998-2017 | eGain Corporation. All rights reserved.

Important: **Management and Authoring Consoles and Services and Hosts buttons are only enabled on Internet Explorer.**

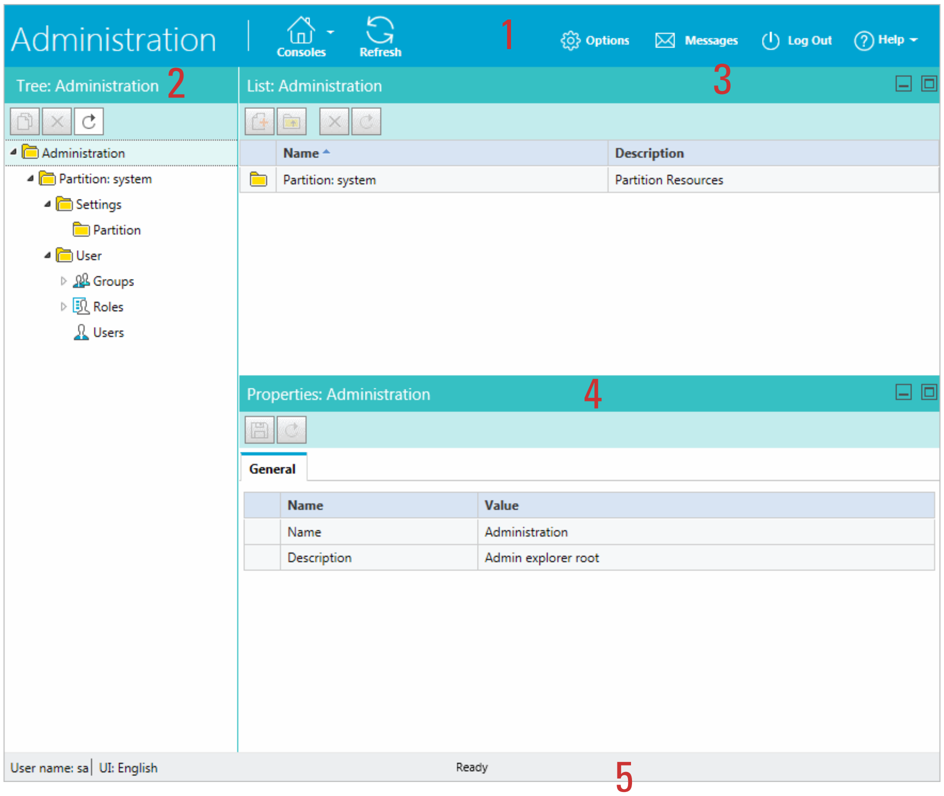
Elements of the User Interface

The console user interface has five functional areas:

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

   To expand all first and second level nodes with a single click, shift + click the plus [+] button next to the topmost node. The contents of all first and second level nodes are displayed in the Tree pane.
3. **List pane:** The List pane displays first-level contents of the folder selected in the Tree pane. You can view the name, description, date of creation, and so on, of the displayed items. In this pane, you can create items or select existing ones to modify or delete them.
4. **Properties pane:** The Properties pane displays the contents of the business object selected in the List pane. In this pane, you can edit the properties of the selected item.

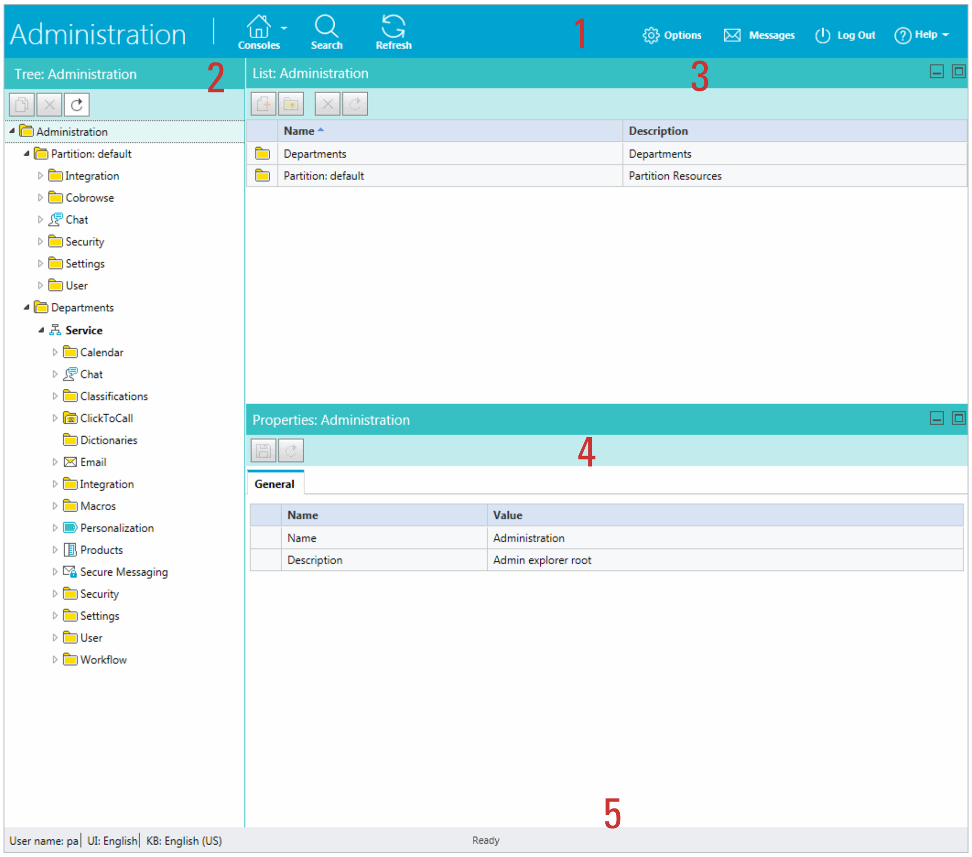
5. **Status bar:** The status bar is present at the bottom of every screen. It displays the following information:
    - The user name with which the user has logged in the system.
    - The language currently in use.
    - The status of the system (**Loading, Ready,** and so on).



Name	Description
Partition: system	Partition Resources

Name	Value
Name	Administration
Description	Admin explorer root

Elements of the Administration Console available in the system partition

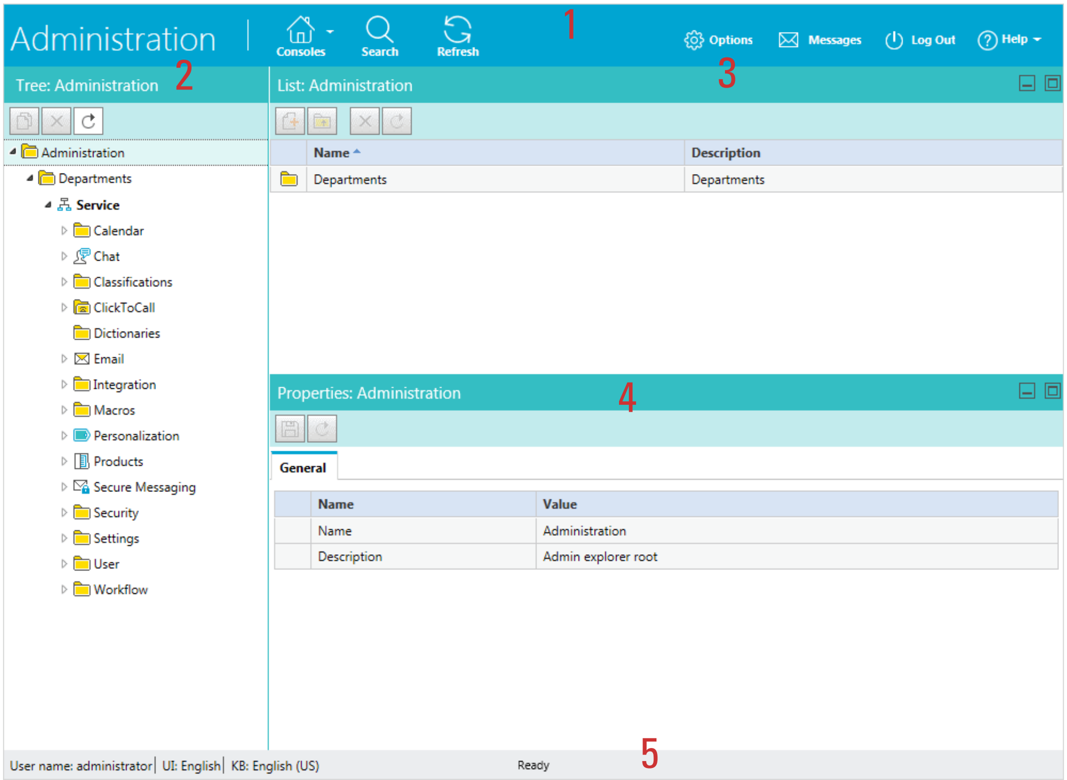


Name	Description
Departments	Departments
Partition: default	Partition Resources

Name	Value
Name	Administration
Description	Admin explorer root

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

Elements of the Administration Console available in the business partition



Name	Description
Departments	Departments

Name	Value
Name	Administration
Description	Admin explorer root

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

Elements of the Administration Console available in a department

2

Settings

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

About Settings

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

Important: **If your system has been integrated with Cisco Unified CCE, the settings available for configuration may vary. For more details, see the *eGain for Cisco Unified CCE Companion Guide*.**

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. Cobrowse settings
   e. Common settings
   f. CTI settings
   g. Dispatcher settings
   h. Retriever settings
   i. General settings
   j. Knowledge base settings
   k. Monitoring settings
   l. Offers settings
   m. OneTag settings
   n. Workflow Engine settings
   o. Security settings
   p. Social 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. Click to call settings

e. Cobrowse Settings

f. Common settings

g. Email blocked file extension settings

h. General settings

i. Knowledge base settings

j. Monitoring settings

k. Queue settings

l. Security settings

m. Social settings

n. Spell checker settings

o. 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 70)
- From: address for notifications from services (page 70)
- Default SMTP server settings (page 70)

At the Department Level

Configure the following setting for each department.

- From email address for alarm (page 74)

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 66)
- Inactive time out (page 59)
- Session time out (page 59)

At the Department Level

- Business calendar timezone (page 63)

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.

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 eGain deployments, make sure that you use a unique installation name for all your eGain installations. This installation name is appended to the article IDs. Changing the value of this setting will impact all the article IDs and the sitemaps generated for the portals.

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

Web Server URL or Load Balancer URL

This URL is used for the following:

- URLs in the report notifications
- Single Sign-On configurations (page 219)
- Self-service portals
- SEO portals

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

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

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: —

Landing Page Settings

Use this setting to configure the small company image that appears on the user landing page and to assign the URL to eGain Analytics. To view or configure the settings, click the **Assistance** button in the **Value** field of the setting. For more information about how to use the landing page, see "Accessing the Application" on page 33.

Analytics URL

In this field, provide the URL to the Analytics login page. When a user clicks the Analytics button on the landing page, they are redirected to the URL provided here.

- Type: Partition settings group
- Subtype: Landing page settings
- Data type: String
- Default value: —

Logo URL

In this field, provide the URL to the company logo image you wish to display in the top left corner of the landing page. The image should use a 2x1 aspect ratio and must not exceed 2 MB.

- Type: Partition settings group
- Subtype: Landing page settings
- Data type: String
- Default value: —

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: 09/22/2019 (shows current date)
- Value options:

    - 09/22/2019
    - Sep/22/2019
    - September 22 2019
    - 2019-09-22
    - 22/09/2019
    - 22-09-2019
    - 22 Sep 2019
    - Sep 22, 2019
    - 22.09.2019
- Can be reset at lower level: Yes

Date and Time Format

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

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

- Can be reset at lower level: Yes

Enable Internal Chat

Agents can collaborate with one another using the built-in internal chat feature in the Advisor Desktop. Agents can chat with individual members of their department, or in group chats. This feature can be enabled and disabled.

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

Enable Scratchpad

Scratchpad is an area of the Advisor Desktop where agents can write notes and save them for future reference. This area appears in a tab on the right side of the desktop. This feature can be enabled and disabled.

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

License Expiration Alerts

Use this setting to enable the system to send alerts to administrators in the event that user license are about to expire. To view or configure the settings, click the **Assistance** button in the **Value** field of the setting.

Alert Administrators When Licenses Are About to Expire

Enable or disable alerts for administrators when licenses approach the expiration date.

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

Advance Notice Time Frame (Days)

Set the amount of days prior to the expiration of a license for which an alert must be sent.

- Type: Partition settings group
- Subtype: License expiration alerts settings
- Data type: Integer
- Default value: 60
- Minimum value: —
- Maximum value: —

Security Settings for Cookies

Use these settings to secure the cookies created by the application for user consoles, knowledge portals, and customer websites, which are enabled for OneTag and Offers. 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, Advisor Desktop, Administration Console, and so on.) and the knowledge portals. When this setting is enabled, you must configure SSL for accessing the application. For details, see the *eGain Installation Guide*. If SSL is not configured, users will not be able to access the application and the knowledge portals. 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

You need to enable this setting if you are using offers, cobrowse, or OneTag. Enable this setting to secure all the cookies created by the application for the customer websites. If this setting is enabled and the customer website is not secure, offers, cobrowse, and OneTag will not work.

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 the eGain Social product, or for portals that have been optimized for search engines–for connections from the application and services servers to the Internet must configure the proxy settings.

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

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

Use Server

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

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

Server Hostname

Provide the fully qualified domain name of the proxy server.

- Type: Partition settings group

- Subtype: Common
- Data type: String
- Default value: —
- Minimum value: —
- Maximum value: —

Server Port

Provide the port number of the proxy server.

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

Authentication

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

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

Username

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

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

Password

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

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

Logger Settings

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

Maximum Backups of Log Files

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

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

Default Size in MB

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

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

Default Log Level

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

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

Encrypt Log Files

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

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

User Account Settings

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

Password Complexity Policy

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

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

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

Login Name Minimum Length

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

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

Login Password Case Sensitive

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

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

Password Life Time

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

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

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

Password Life Time Unit

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

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

Allow Users to Change Password

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

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

Unsuccessful Attempts Time Frame

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

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

- Can be reset at lower level: No

Unsuccessful Attempts Time Unit

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

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

Maximum Number of Unsuccessful Timed Attempts

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

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

Maximum Number of Unsuccessful Attempts

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

- Type: Department setting group
- Subtype: Security
- Data type: Integer
- Default value: 0
- Minimum value: 0
- 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 Profile Photo for Agents

Use this setting to enable or disable the ability for agents to upload and update their profile picture in the Advisor Desktop.

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

Allow Local Login for Partition Administrators

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. This option is only available to users in partition 1 with the “administer partition” permission. Once enabled, partition administrators may use the following URL to log in: `http(s)://`*`HOST_NAME`*`/context_root/web/view/platform/common/login/root.jsp?partitionId=1&localLogin=true`.

Users outside this partition, or without this permission, will not be able to log in to the application with this URL.

- 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

PCI Compliance Settings

Display a Warning Message to Agents for PCI Compliance

Use this setting to define if the agents should be displayed the PCI Compliance message every time they log in to the Advisor Desktop. The message displayed to the agents is “If you see any credit card account numbers or CVV codes in customer correspondence, please delete them.”

Important: **As an alternative to this setting, you might consider instead using the Data Masking capabilities (page 197) available in the application. This will help ensure that no sensitive data is exchanged between customers and agents.**

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

CTI Settings

Enable CTI Integration with the Agent Console

This enables CTI integration with the Advisor Desktop. It will also allow agents to manage availability for Phone from the Advisor Desktop.

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

Enables Phone Process and Instance Nodes in the System Console

This enables Phone process and instance nodes in the System Console. Nodes are only visible if the Enable CTI Integration with the Advisor Desktop setting is set to **Yes**.

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

Enable Call Control Buttons in the Agent Console

This enables call control buttons in the Advisor Desktop. Call buttons are only visible if the Enable CTI Integration with the Advisor Desktop setting is set to **Yes**.

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

Display Phone Field on Login Page for Single Sign-On

This enables the user to use the phone and login in to the eGain application at the same time.

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

Chat - Make Agents Unavailable When Network Connection Fails

Make agents unavailable for chat when network connection fails between the Solve application and the CTI application.

- Type: Partition setting group
- Subtype: CTI setting

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

Enable External Phone Book

This enables external phone book tab for transfers, conferencing, and custom implementations.

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

Enable Number Pad

This enables number pad for dialing the phone numbers, transfers, conferencing, and entering IVR Data.

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

Amazon Connect URL

Provide the CCP URL to help integrate the application with Amazon Connect.

- Type: Partition setting group
- Subtype: CTI setting
- Data type: String
- Default value: No
- Can be reset at lower level: No

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.

Exception Email Settings

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

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

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 Advisor Desktop, and while configuring workflows from Administration Console. If a system generated email (auto-acknowledgements, auto-replies and so on.) exceeds this size, the email will not be sent and a notification is sent to the email address configured in the "To: address for notification from Services" setting.

- 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 Advisor Desktop, and while configuring workflows from Administration Console. If a system generated email (auto-acknowledgements, auto-replies and so on.) exceeds this size, the email will not be sent and a notification is sent to the email address configured in the "To: address for notification from Services" setting.

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

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

To: Address for Notifications from Services

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

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

From: Address for Notifications from Services

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

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

Notification Mails Auto BCC

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

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

Default SMTP Server Settings

For various objects in the system, you can configure notifications to be sent to administrators. Some of the objects for which you can configure notifications are, Monitors (in the Supervision Console), Reports (in the

Reports Console), Alarm workflows (in the Administration Console), Abandoned chats (in the Administration Console). The address to which these notifications are sent, is specified in the properties of the object and the from email address is specified in the “From: address for notifications from services” setting.

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

Server Type

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

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

Use SMTP

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

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

Server Name

In this setting provide the name of the server.

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

User Name (ESMTP)

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

- Type: Partition settings group
- Subtype: Default SMTP Server

- Data type: String
- Default value: —
- Minimum value: 0
- Maximum value: 255

Password

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

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

Connection Type

Select the authentication connection type for the server to use.

- Type: Partition settings group
- Subtype: Default SMTP Server
- Data type: Enumeration
- Default value: Plain text
- Value options: Plain text, SSL, TLS

Port

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

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

Blocked Attachments Settings

Email - Criteria for Blocking Attachments

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

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

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

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 *eGain_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 database 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

Mail User Max Load

This setting determines the maximum email activities that can be assigned to agents by workflows or other agents. When an agent reaches the maximum number, workflows cannot assign new activities to the agent and other agents cannot transfer activities to the agent, but the agent can pull activities. All open email activities in the agent's inbox qualify for this setting. It can take any numeric value. A value of -1 denotes that infinite number of emails can be assigned to the agent.

- Type: Department settings group, User settings group
- Subtype: Activity
- Data type: Integer
- Default value: -1
- Minimum value: -1
- Maximum value: 100000
- Can be reset at lower level: Yes

Social User Max Load

This setting determines the maximum social activities that can be assigned to a user at a given moment. When an agent reaches the maximum number, workflows cannot assign new activities to the agent, but the agent can pull activities and other agents can transfer activities to the agent.

- Type: Department settings group
- Subtype: Social
- Data type: Integer
- Default value: -1
- Minimum value: -1
- Maximum value: 100000
- Can be reset at lower level: Yes

Chat - User Max Load

This setting determines the maximum chat activities that can be assigned to a user at a given moment. When an agent reaches the maximum number, new chats cannot be assigned to the agent.

- Type: Department settings group
- Subtype: Activity
- Data type: Integer
- Default value: 4

- Minimum value: 1
- Maximum value: 10
- Can be reset at lower level: Yes

Chat - Override User Max Load Setting for Pull

Use this setting to allow agents to pull chat activities from queues after the agents have reached the maximum value defined in the “Chat user max load” setting.

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

Max Load for All Other Activities

This setting determines the maximum activities, other than emails and chats, that can be assigned to agents by workflows. When a user reaches the maximum number, workflows cannot assign new activities to the agent but, the agent can pull activities and other agents can transfer activities to the agent.

- Type: Department settings group, User settings group
- Subtype: Activity
- Data type: Integer
- Default value: -1
- Minimum value: -1
- Maximum value: 100000
- Can be reset at lower level: Yes

Personalized Activity Assignment Settings

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 and social 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.

This feature works in conjunction with the “Ignore User Max Load for Personalized Activity Assignment” setting. When the Ignore User Max Load for Personalized Activity Assignment setting is enabled, the personalized activity assignment will happen even though the user has reached the maximum load for emails.

When the setting is disabled, the Personalized Activity Assignment setting takes affect only when the user has not reached the maximum allowed load (value specified in the setting "Mail user max load" if it is an email activity or "Social user max load" setting if it is a social activity).

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 and social activities.

- 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 and social activities (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 Personalized Activity Assignment Only to Users with Permissions on Queue

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

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

Ignore User Max Load for Personalized Activity Assignment

Use this setting to override the user max load setting if an email or social activity that qualifies for personalized activity assignment. When this setting is disabled, the Personalized Activity Assignment setting takes affect only when the user has not reached the maximum allowed load (value specified in the setting “Mail user max load” if it is an email activity or “Social user max load” if it is a social activity).

- Type: Department settings group
- Subtype: Activity
- 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 Advisor Desktop. When the agent clicks the **Pull** button in the Advisor Desktop, 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 Advisor Desktop.

- 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 Advisor Desktop.

- 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

Automatically Save Pull Activity Queue

Use this setting to automatically decide the queues from which an agent is assigned activities when he clicks the **Pull Next** button. When the setting is enabled the agent is not allowed to select the queues from the Preferences window in the Advisor Desktop. All the queues on which the agent has pull permission are selected automatically.

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

Criteria for Push Based Assignment

This setting determines the criteria for assigning activities from queues to agents.

- Type: Department settings group
- Subtype: Activity
- Data type: Enumeration
- Default value: Most overdue
- Value options: Most overdue, Due Soonest, Highest Priority, Newest, Oldest
- Can be reset at lower level: No

Push Based Assignment Criteria for Social

This setting determines the criteria for assigning social activities from queues to agents.

- Type: Department settings group
- Subtype: Activity
- Data type: Enumeration
- Default value: Most overdue
- Value options: Most overdue, Due Soonest, Highest Priority, Newest, Oldest
- Can be reset at lower level: No

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 settings 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: 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: 30
- Maximum value: 6000
- Can be reset at lower level: Yes

Number of Activities to be Monitored for Service Level

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

- Type: Department settings group
- Subtype: Monitoring
- Data type: Integer
- Default value: 10
- Minimum value: 1
- Maximum value: 1000

- Can be reset at lower level: No

Chat - SLA for Response Time (Seconds)

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

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

Chat - Daily Service Level Sample Set Definition

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

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

Chat - Daily Service Level Timezone

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

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

(GMT-12:00) Eniwetok, Kwajalein

(GMT-11:00) Midway Island, Samoa

(GMT-10:00) Hawaii

(GMT-09:00) Alaska-Standard

(GMT-08:00) Alaska-Daylight

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

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

(GMT-07:00) Arizona

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

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

(GMT-06:00) Central America

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

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

(GMT-06:00) Mexico City-Standard

(GMT-05:00) Mexico City-Daylight

(GMT-06:00) Saskatchewan

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

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

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

(GMT-05:00) Indiana (East)

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

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

(GMT-04:00) Caracas, La Paz

(GMT-04:00) Santiago-Standard

(GMT-03:00) Santiago-Daylight

(GMT-03:30) Newfoundland-Standard

(GMT-02:30) Newfoundland-Daylight

(GMT-03:00) Brasilia-Standard

(GMT-02:00) Brasilia-Daylight

(GMT-03:00) Buenos Aires, Georgetown

(GMT-03:00) Greenland-Standard

(GMT-02:00) Greenland-Daylight

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

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

(GMT-01:00) Azores-Standard

(GMT) Azores-Daylight

(GMT-01:00) Cape Verde Is.

(GMT) 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

Activity Handling Settings

Agent Guidance Notifications

Define different types of agent guidance notifications. Here you can adjust the style, color, and duration of the notifications that appears in the advisor desktop.

- Type: Department settings group
- Subtype: Common
- Data type: String
- Default value: —
- Value options: There are default notifications available for configuration. Additional notifications can be added. Default notifications include:
  - **Before Due Date:** When an advisor selects an activity in the Inbox and its due date is within next 4 hours, a notification bubble appears in the bottom right corner.
  - **After Due Date:** When an advisor selects an activity in the inbox and it is past due, a notification bubble appears in the bottom right corner.
  - **Newest Customer Note:** When an advisor selects an activity in the inbox and there are multiple notes attached to the customer for this activity, the latest note appears in the bottom right corner.
  - **Salesforce Case:** When the agent tabs out of the custom field (salesforce_case_id) in the Reply pane, if the entered text matches a caseId in salesforce, the subject of the case appears in the bottom right corner.

    Note: SFDC integration needs to be enabled and a custom attribute named “salesforce_case_id” on activity data and needs to be added in Reply pane screen.
  - **Latest Transfer Note:** When the advisor selects an activity in the inbox and there is a note attached to the activity from the last agent who transferred it to the current agent, the latest note appears in the bottom right corner.

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. The following alerts are displayed: If the agent’s focus is in the Main Inbox of the Advisor Desktop, the **Refresh** button blinks; If the Advisor Desktop 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: No alert is displayed to agents.
  - Always: An alert is displayed every time an activity is assigned to the agent.
  - When the agent has no open activity: The alert is displayed only when the agent has no activities in the inbox.
- Can be reset at lower level: Yes

Allow Agent to Associate a New Outbound Activity with a Queue

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

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

Send Agent an Email When Activity Is Assigned

Use this setting to decide if an email notification should be sent to an agent's business email address 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

Require Activity Note on Transfer

Use this setting to decide if agents are required to add a note to the activity before transferring it to another agent or queue.

- Type: Department settings group
- Subtype: Activity
- Data type: Enumeration
- Default value: No
- Value options: Yes, No
- 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 Advisor Desktop. This information is available in the Activity 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

Show CC Field

With this setting you can make the **CC** field available in the Reply pane of the Advisor Desktop. If you do not want agents to be able use the **CC** field, then along with configuring this setting, make sure that the **Edit CC field** action is not assigned to the agents.

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

Show BCC Field

With this setting you can make the **BCC** field available in the Reply pane of the Advisor Desktop. If you do not want agents to be able use the **BCC** field, then along with configuring this setting, make sure that the **Edit BCC field** action is not assigned to the agents.

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

Allow Agents to Associate a New Outbound Activity With a Queue

Use this setting to allow agents to associate an activity with a queue while composing an outbound email activity. You would want to set the value of this setting to **Yes** when you have configured the Solve feature for the queues and you want the agents to be able to use this feature for composed activities as well. While composing emails, agents are prompted to associate the email with a queue. Agents are displayed the list of queues on which they have pull permissions.

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

Service Chat and Phone Activities at the Same Time

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

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

Chat - MeadCo Download on Agent Console

Use this setting to decide if an agent should be prompted to download MeadCo when he logs in to the Advisor Desktop for the first time from a user desktop.

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

Calltrack Activity Settings

Allow Classifications to be Added as Text on Reply Pane for Phone Type Activities

Use this setting to automatically add the names of categories and resolution codes assigned to an activity in the call log. This setting is for calltrack activities only.

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

Allow Related Activity Details to be Added as Text on Reply Pane for Phone Type Activities

Use this setting to automatically add a note (#Created activity#) to the call log when a new activity related to the calltrack activity is created. Only the activities meeting the following criteria are added - activities created during the call; activities associated with the current case. This setting is for calltrack activities only.

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

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 Advisor Desktop.

- Type: Department settings group, User settings group
- Subtype: Activity
- Data type: Long
- Default value: 10
- Minimum value: 1
- Maximum value: 75
- 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 Advisor Desktop.

- 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 Advisor Desktop. 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 Advisor Desktop. 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

Mail - Agent Availability Choice Enabled

Use this setting to allow agents to change their availability for email activities in the Advisor Desktop.

- Type: Department settings group
- Subtype: General
- Data type: Enumeration
- Default value: Yes
- Value options:
  - Yes: Agents can change their availability.
  - No: Agents become available automatically when they login and become unavailable when they logout.
- 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 Advisor Desktop. 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 Advisor Desktop. 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 - Agent Availability Choice Enabled

Use this setting to allow agents to change their availability in the Chat Inbox in Advisor Desktop.

- Type: Department settings group
- Subtype: General
- Data type: Enumeration
- Default value: Yes
- Value options:
  - Yes: Agents can change their availability.
  - No: Agents become available automatically when they login and become unavailable when they logout.
- Can be reset at lower level: No

Chat Supervisor Inbox Settings

Chat - My Monitor - Max Join Load

This setting determines the maximum number of chats a supervisor can join from the “My monitors” node in the Advisor Desktop.

- Type: Department settings group
- Subtype: Activity
- Data type: Integer
- Default value: 4
- Minimum value: 1
- Maximum value: 10
- Can be reset at lower level: No

Chat - My Monitor - Activity Refresh Interval (Seconds)

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

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

Spelling and Blocked Words Settings

Preferred Dictionary of the User

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

- Type: Department settings group, 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, and so on. 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, and so on.

- Type: Department settings group

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

Auto Blockcheck

Use this setting to check the content of emails, tasks, etc for blocked words. This setting is not used for chat activities. For chat, use the Chat - Auto Blockcheck setting. The list of blocked words is set from the Dictionaries node in the Administration Console. For details, see "Adding Blocked Words" on page 290.

- 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 290.

- 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, and so on.

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

Ignore Words that Contain Numbers

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

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

Ignore Web Addresses and File Names

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

- Type: Department settings group, 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 pane of the Advisor Desktop.

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

Maximum Number of Records to Display for NAS Search

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

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

Always Show Prompt Window for My Searches

Use this setting to define whether you want the search window to come up and allow agents to edit values for a saved search. This setting is meant for users who do not configure their saved searches with the ~~prompt option for values.

- Type: Department settings group, User settings group
- Subtype: Common
- Data type: Enumeration
- Default value: No
- Value options:
  - **Yes:** The saved search is not run automatically. The system displays the search criteria that is defined in the My Search, and allows agents to change the values before running the search.

    - **No:** Runs the search and displays the search results without providing users with the opportunity to change the predefined values.
- Can be reset at lower level: Yes

Knowledge Base Settings

Update External Attachment Service Update Interval in Minutes

Use this setting to determine the regular time interval at which the KB Import Service synchronizes the content of the external attachments of articles with the content of the files in the external location.

- Type: Partition settings group
- Subtype: Knowledge base
- Data type: Long
- Default value: 6
- Minimum: 6
- Maximum: 1440

Popular Articles Display Count

Use this setting to specify the number of articles that are displayed in the "Most popular articles" folder in the Agent and KB Consoles.

- Type: Partition settings group
- Subtype: Knowledge base
- Data type: Integer
- Default value: 10
- Minimum: 1
- Maximum: 100

Popular Articles Evaluation Period in Days

Use this setting to determine the number of days for which the article usage is evaluated before it is added to the "Most popular articles" folder.

- Type: Partition settings group
- Subtype: Knowledge base
- Data type: Integer
- Default value: 10

- Minimum: 1
- Maximum: 30

Popular Articles Update Interval in Hours

Use this setting to determine the time period after which the system updates the list of popular articles displayed in the “Most popular articles” folder.

- Type: Partition settings group
- Subtype: Knowledge base
- Data type: Long
- Default value: 1
- Minimum: 1
- Maximum: 24

New Articles Timespan (Days)

This setting determines the time period for which a new article is displayed in the “Recently added articles” folder in the Agent and KB Consoles.

- Type: Partition settings group
- Subtype: Knowledge base
- Data type: Long
- Default value: 30
- Minimum: 1
- Maximum: 365

Updated Articles Timespan (Days)

This setting determines the time period for which an updated article is displayed in the “Recently updated articles” folder in the Agent and KB Consoles.

- Type: Partition settings group
- Subtype: Knowledge base
- Data type: Long
- Default value: 30
- Minimum: 1
- Maximum: 365

Article Rating Service Delay in Seconds

Use this setting to specify the time interval (in seconds) after which the system recalculates the ratings of the articles.

- Type: Partition settings group
- Subtype: Knowledge base
- Data type: Long
- Default value: 30
- Minimum: 30
- Maximum: 3600

Time to Expire in Days

Use this setting to specify the number of days for which an article should be displayed in the “Articles about to expire” folder before it expires.

- Type: Partition settings group
- Subtype: Knowledge base
- Data type: Integer
- Default value: 5
- Minimum: 1
- Maximum: 30

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), Polish, Portuguese, Portuguese (Brazilian), Romanian, Russian, 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

Select Article Type and Article Template on Create

Enable this setting to prompt authors to select the article type and template when they create new articles. When this setting is enabled, users see the Select Article window and they have to select an article type and article template to be used for the article they are creating. Authors can always change the article type and template after they have created an article.

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

Default Article Type and Article Template for Creating Articles

Use this setting to define the default article type and template that should be used for creating new articles. If the article type or template used in this setting is deleted from the system, new articles are created using the **General** article type and **Blank document** article template. When the “Select Article Type and Article Template on Create” setting is enabled, authors can set and change the default values from the Select Article window.

- Type: Department settings group, User settings group
- Subtype: Knowledge Base
- Data type: String
- Default value: General || Blank Document
- Value options: The secondary window displays the list of article types and templates created in the department.
- Can be reset at lower level: Yes

Default Portal for Previewing Articles

Authors who have been assigned a Knowledge+AI license can preview their articles in a Portal using the Preview in Portal feature. A default portal can be assigned for authors in a department to use in previewing their articles in a portal.

When the application is first installed, the master portal serves as the default portal. The default portal is the portal used while configuring solutions for each queue. Any portal in the department can be designated the default portal. By default, the master portal is assigned as the default portal for previewing articles.

- Type: Department settings group, User settings group
- Subtype: Knowledge Base
- Data type: String
- Default value: Master portal
- Value options: The secondary window displays the list of article types and templates created in the department.
- Can be reset at lower level: Yes

Display Short Form IDs of KB Objects in Portals and APIs

When this setting is enabled, the short form IDs of articles are displayed in the self-service portals and by the APIs.

- Type: Partition settings group
- Subtype: Knowledge Base
- Data type: Enumeration
- Default value: No (in updated systems) Yes (in new installations of eGain Solve)
- Value options: Yes, No

Default Portal for Previewing Articles

Select a default portal for previewing articles during the authoring process. Authors can also set and change the default portal from the preview window.

- Type: Department settings group, User settings group
- Subtype: Knowledge Base
- Data type: String
- Default value: —
- Value options: The secondary window displays the list of portals available in the department.
- Can be reset at lower level: Yes

Timeout Settings for Knowledge Agent and Web Portal Sessions

Set the amount of time before a user is logged out of a portal after becoming inactive.

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

Inactivity Timeout for Knowledge Agents (Minutes)

Set the amount of time before an agent is logged out of a knowledge agent portal after becoming inactive.

- Type: Partition settings group
- Subtype: Knowledge Base
- Data type: String
- Default value: 60
- Minimum: 5
- Maximum: 480
- Can be reset at lower level: No

Inactivity Timeout for Web Self-Service Users (Minutes)

Set the amount of time before a user is logged out of a self-service portal after becoming inactive.

- Type: Partition settings group
- Subtype: Knowledge Base
- Data type: String
- Default value: 20
- Minimum: 5
- Maximum: 120
- Can be reset at lower level: No

eGain Knowledge System

Use this setting to identify another Solve system as the source of knowledge for a Solve configuration for digital channels, such as chat or email. The URL for the knowledge system must be provided here in order to configure queues to use external knowledge bases for Solve. For more information about configuring Solve for queues, see *eGain Administrator’s Guide to Routing and Workflows*.

- Type: Department settings group
- Subtype: Knowledge Base
- Data type: String
- Default value: —
- Minimum: —

- Maximum: —
- Can be reset at lower level: No

KB Approval Process Settings

These settings need to be configured only if you are using Knowledge Promotion and have configured the Knowledge Approval Process to send suggestions from the production system to the remote authoring system. These settings are configured on the production system.

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

Before you begin, you need to get the Remote authoring server user ID, Remote authoring server exception folder ID, Remote authoring server department ID from the authoring system. For details about doing this task, see the *eGain Author's Guide to Knowledge Portals.*

Send Suggestions to Remote Authoring Server

Enable this setting if you are enabling the Knowledge Approval Process across the production and remote authoring system.

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

Remote Authoring Server User ID

Provide the ID of the user on the authoring system. All articles suggested from Production Installations will use this user as the suggester of the article.

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

Remote Authoring Server Exception Folder ID

Provide the ID of a KB Folder on the authoring system. If users on Production Installations attempt to create a suggestion in a folder that is not promoted, or is not present in the Development Installation, suggestions will be created in this folder instead.

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

Remote Authoring Server Department ID

Provide the ID of the department to which the exception KB folder belongs.

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

Web Search Settings for Knowledge Portals

Configure the web search settings if you want to run searches on the web and include the search results from web in your portal searches. The web search adapter uses the Google custom search API. To configure these settings you need a Gmail account, which you will then use to generate the API key and to configure your Custom Search Engine.

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

URL

The value of this setting is automatically set to **https://www.googleapis.com/customsearch/v1** and should not be changed without consulting eGain.

- Type: Department settings group
- Subtype: Knowledge Base
- Data type: String
- Default value: https://www.googleapis.com/customsearch/v1

API Key

Provide the API key for the Google search API. Go to http://code.google.com/apis/console to generate an API key. To learn how to generate the API key, use the API console help pages provided by Google in their support section.

While generating the API key, in the Credentials section, in the IPS field provide a comma separated list of external IPs of the application servers.

- Type: Department settings group
- Subtype: Knowledge Base
- Data type: String

Engine ID

Create a custom search engine and provide the Engine ID in this setting. Follow the instructions available at: http://www.google.com/cse/ While generating the engine ID, in the Basics tab, in the Sites to search field, select the Search the entire web but emphasize included sites option.

- Type: Department settings group
- Subtype: Knowledge Base
- Data type: String

Chat Settings

Chat Auto-Pushback Settings

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

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

Enable Auto-Pushback of Chats

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

- Type: Partition settings group
- Subtype: Chat
- Data type: Enumeration
- Default value: Yes

- Value options: Yes, No

Expiry Time for Auto-Pushback for Chats (Minutes)

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

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

Make Agent Unavailable on Auto-Pushback of Chats

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

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

Chat Agent Session Settings

Chat - Agent Chat Message Maximum Length

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

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

Show Smiley in Agent Chat Toolbar

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

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

Chat - Display Timestamp in Agent Chat Console

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

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

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

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

- Type: Department settings group
- Subtype: Common

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

Chat - Enable Sound Alert

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

Video Chat - Invitation Timeout Period

The time period, in seconds, for which the video chat link offered by the agent is active in the Customer Chat Console. Agent Availability is reserved for that video chat during this time. The system cannot assign new chats to the agent and the agent cannot pull new chats from queues.

- Type: Department settings group
- Subtype: General
- Data type: Integer
- Default value: 60
- Minimum value: 5
- Maximum value: 600
- Can be reset at lower level: No

Chat - Reason for Transfer

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

- Type: Department settings group
- Subtype: Activity
- Data type: Enumeration
- Default value: Optional

- Value options:
  - Optional
  - Required
- Can be reset at lower level: No

Chat - Require Activity Note on Transfer

Use this setting to decide if agents are required to add a note to the chat activity before transferring it to another agent or queue.

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

Chat - Restore Agent Console when a Message Arrives

Use this setting to decide if the Advisor Desktop should be restored to the top window of an agent's screen when a chat message arrives in the agent's inbox. This includes instances in which the window with the Advisor Desktop is not the window the agent is actively viewing, as well as instances in which the window with the Advisor Desktop is minimized to the taskbar.

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

Enable Conversation Stream

Use this setting to enable conversation view for chats in advisor desktop. The Conversation stream provides a visible record of all previous chats for retuning customers. When an agent enters a conversation with a returning customer, all previous chat conversations are displayed in the Chat window directly above the current conversation. Conversation view is enabled by default.

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

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

Chat Customer Session Settings

Important: **The settings described in this section are used only for templates that are upgraded to eGain Solve from previous versions of eGain Service.**

Chat - Customer Chat Message Maximum Length

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

- 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

Chat - Display Timestamp in Customer Chat Console

Use this setting to decide if the timestamp should be displayed with the chat messages in the Customer Console.

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

Chat - MeadCo Download on Customer Console

Use this setting to decide if a customer should be prompted to download MeadCo when the chat window is opened for the first time from a customer desktop.

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

- value options: Enable, Disable
- Can be reset at lower level: No

Offers Settings

Offers Managers with the “Edit Offer Settings” action can configure these settings from the Offers Console as well. Changes made from the Offers Console are reflected in the Administration Console, and vice versa.

Important: **These settings are valid only in installations that include Offers.**

Offer Expiration Period (Seconds)

The time period, in seconds, after which an offer automatically expires and is removed from the web page if the user has neither accepted nor rejected it. An expired offer is considered to have been ignored.

- Type: Partition settings group
- Subtype: Offers
- Data type: Integer
- Default value: 60
- Minimum value: 10
- Maximum value: 14400 (4 Hours)

Interval for Re-offering Ignored Offers (Seconds)

The time period, set in seconds, after which an ignored offer may be presented again in the same user session, in case the user becomes eligible for the offer again. The user can be on the same page where he had ignored the offer earlier, or can be on another web page of the website where the same offer is enabled. This setting applies to offers that have the **Re-Offer on Ignore** option enabled.

- Type: Partition settings group
- Subtype: Offers
- Data type: Integer
- Default value: 300
- Minimum value: —
- Maximum value: 86400 (24 Hours)

Interval for Re-offering Accepted Offers (Seconds)

The time period, set in seconds, after which an accepted offer may be presented again in the same user session, in case the user becomes eligible for the offer again. The user can be on the same page where he had accepted the offer earlier, or can be on another web page of the website where the same offer is enabled. For Agent Offers which are accepted, the interval for re-offering is counted from the time the previous offer was accepted, not the time that the previous chat or call ended. This setting applies to offers that have the **Re-Offer on Accept** option enabled.

- Type: Partition settings group
- Subtype: Offers
- Data type: Integer
- Default value: 300
- Minimum value: —
- Maximum value: 86400 (24 Hours)

Interval for Checking Eligibility of an Offer That Was Not Presented (Seconds)

The time period, set in seconds, after which a website visitor is checked for eligibility for an automatic chat offer, in case the offer is not presented to the user when he last became eligible. An automatic chat offer is not presented if agents are not available or the chat queue depth is met at the time when the visitor becomes eligible.

- Type: Partition settings group
- Subtype: Offers
- Data type: Integer
- Default value: 120
- Minimum value: 10
- Maximum value: —

Maximum Time on Webpage (Minutes)

The maximum time, set in minutes, a visitor can remain on a webpage before the application stops checking for offer eligibility. This applies to a single webpage, and not for the entire visit to the website. For example, if the maximum time is set to 30 minutes and a visitor remains on the same page for more than 30 minutes, the application will not check for offer eligibility for the remainder of time the visitor is on the page, even if she performs the actions necessary to become eligible for an offer. If the same visitor then moves to another webpage on the same website, the timer starts over.

- Type: Partition settings group
- Subtype: Offers
- Data type: Integer
- Default value: 120

- Minimum value: 1
- Maximum value: 360

Limit Number of Offers Per Visit

Use this setting to limit the number of offers that will be presented to a visitor during a single visit to the website. If you enable this setting, make sure you configure the **Maximum number of offers per visit** setting to define the limit.

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

Maximum Number of Offers Per Visit

Configure this setting if you have enabled the **Limit number of offers per visit** setting. In this setting define the maximum offers to be presented per visit. Once this number is met, the visitor is not presented with another offer for the rest of that visit. Note that at the offer level the Offer Manager can configure an offer to be excluded from this limit.

- Type: Partition settings group
- Subtype: Offers
- Data type: Integer
- Default value: -1
- Minimum value: -1
- Maximum value: —

Maximum Size Allowed for Offers Template Zip File (in Kilobytes)

Use this setting to define the maximum allowed size, in kilobytes, of an offer template zip file that can be uploaded from the Offers Console.

- Type: Partition settings group
- Subtype: Offers
- Data type: Integer
- Default value: 250
- Minimum value: 250
- Maximum value: 25600

Click to Call Settings

Select the service provider for ClickToCall. If Amazon Connect is the selected service provider, you must also provide the Access Key ID, Secret Access Key, and Contact Flow Arn. If Asterisk is selected, you must provide the Asterisk Context and the SIP peer or friend group.

- Type: Department settings group
- Subtype: ClickToCall
- Data type: String
- Default value: eGainClick2Call
- Value options: Asterisk; Amazon Connect
- Can be reset at lower level: No

Asterisk Context

Context of the Asterisk Telephony Server which is used by eGain ClickToCall when connecting a website visitor with the call center.

- Type: Department settings group
- Subtype: ClickToCall
- Data type: String
- Default value: eGainClick2Call
- Value options: —
- Can be reset at lower level: No

SIP Peer or Friend Group

The Session Initiation Protocol (SIP) peer or friend group that is associated with the Asterisk Telephony Server context used by eGain ClickToCall when connecting a website visitor with the call center.

- Type: Department settings group
- Subtype: ClickToCall
- Data type: String
- Default value: voiptalk
- Value options: —
- Can be reset at lower level: No

Social Settings

Important: **These settings are valid only in installations that include Social.**

Social Test Mode Settings

The test mode for social allows you to test your Facebook and Twitter adapters and configurations before you start posting content to these social sites.

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

Enable Social Test Mode

By default the test mode for Social is turned on and all messages posted to Twitter and Facebook are posted to the test accounts configured in the “Test user for Twitter” and “Test user for Facebook” settings. If no values are set for the test user settings, all the responses and messages posted to Facebook and Twitter are sent to the Exception Queue.

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

Test User for Twitter

Provide the Twitter ID to which you want to post the test data. If no value is set for this setting and the social test mode is turned on, all the responses and messages posted to Twitter are sent to the Exception Queue.

- Type: Partition settings group
- Subtype: Social
- Data type: String
- Default value: —
- Value options: —

Test User for Facebook

Provide the Facebook ID to which you want to post the test data. If no value is set for this setting and the social test mode is turned on, all the responses and messages posted to Facebook are sent to the Exception Queue.

- Type: Partition settings group
- Subtype: Social

- Data type: String
- Default value: —
- Value options: —

Social Response Settings

Number of New Social Activities to Post

The maximum number of new social activities that are processed by the Social Dispatcher Service in each cycle.

- Type: Partition settings group
- Subtype: Social Response
- Data type: Integer
- Default value: 100
- Minimum value: 1
- Maximum value: 1000

Number of Retry Social Activities to Post

The maximum number of retry social activities, which failed to be sent in previous attempts, that are processed by the Social Dispatcher Service in each cycle.

- Type: Partition settings group
- Subtype: Social Response
- Data type: Integer
- Default value: 10
- Minimum value: 1
- Maximum value: 100

Frequency to Post Social Activities

Use this setting to define the time interval (in minutes) at which the Social Response Service processes batches of social activities and post messages to the social networks.

- Type: Partition settings group
- Subtype: Social Response
- Data type: Integer
- Default value: 5
- Minimum value: 1
- Maximum value: 1440

Number of Parallel Post Processes for Social Activities

The number of parallel threads that should be used to dispatch social activities. If you have a large number of activities to dispatch, you should consider increasing the value of this setting.

- Type: Partition settings group
- Subtype: Social Response
- Data type: Integer
- Default value: 1
- Minimum value: 1
- Maximum value: 10

Social Search Settings

Expiry Duration for Social Media Hits

Specify the number of days after which the search results should be marked for deletion. The result is deleted from the Social Inbox at the time interval specified in the **Frequency of deletion of expired social activities** setting.

- Type: Partition settings group
- Subtype: Social Search
- Data type: Integer
- Default value: 7
- Minimum value: 1
- Maximum value: 21

Frequency of Deletion of Expired Social Activities

The time interval, in hours, after which the expired search results should be automatically deleted from the Social Inbox. The expiry time for the results is defined in the **Expiry duration for social media hits** setting.

- Type: Partition settings group
- Subtype: Social Search
- Data type: Integer
- Default value: 24
- Minimum value: 1
- Maximum value: 240

Expiry Duration for Follow up Activities

When you post a response, or publish a message to a social network, you can choose to follow-up your message. Specify the number of days after which the system should stop following up on the post. After this time, the system automatically closes the case associated with the activity. If there are any other activities, such as, emails, associated with the case, then the case is not closed.

- Type: Partition settings group
- Subtype: Social Search
- Data type: Integer
- Default value: 7
- Minimum value: 1
- Maximum value: 60

Frequency of Deletion of Expired Social Follow up Activities

The time interval, in hours, after which the system deletes all expired search results.

- Type: Partition settings group
- Subtype: Social Search
- Data type: Integer
- Default value: 24
- Minimum value: 1
- Maximum value: 240

Frequency to Retrieve Social Media Hits

Use this setting to define the time interval (in minutes) at which the Social Search Service will run and search for social media hits that match the search terms configured in the Social Console.

- Type: Partition settings group
- Subtype: Social Search
- Data type: Integer
- Default value: 30
- Minimum value: 1440
- Maximum value: 1

Common Settings

The following settings can also be configured from the Social Console.

Chat Entry Point

Provide the link for the chat entry point that should be available to agents and social managers for adding to social responses.

- Type: Department settings group
- Subtype: Social
- Data type: String
- Default value: —
- Value options: —
- Can be reset at lower level: No

Self Service Portal

Provide the link for the self-service portal that should be available to agents and social managers for adding to social responses.

- Type: Department settings group
- Subtype: Social
- Data type: String
- Default value: —
- Value options: —
- Can be reset at lower level: No

External URL

Provide the link for any website that should be available to agents and social managers for adding to social responses.

- Type: Department settings group
- Subtype: Social
- Data type: String
- Default value: —
- Value options: —
- Can be reset at lower level: No

Number of Results to Display Per Page

Specify the number of search results to be displayed per page in the Social Console.

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

Cobrowse Settings

Web Cache Service Settings

While in a cobrowse session, the agent browser does not have an active session with the actual website. As a result, the websites which have authenticated static contents (CSS, images) are not rendered correctly on the agent side. The Web Cache feature downloads such static contents from the customer browser and send them to the application server where the contents are stored and cached. The agent browser then downloads these static contents from the application server while in a cobrowse session. Use these settings to enable the Web Cache feature and to define the white list of domains as well as resources pattern for the authenticated static resources (image and CSS).

For example, if the whitelisted domains are a.comp.com, b.ecomp.com and the resources defined are /secured/images,/secured/css, the feature will apply to URLs that contain \secured\images and \secured\css but not to the URLs that contain \public\images

The following URLs will qualify:

- http://a.comp.com/secured/css/style.css
- http://b.comp.com/secured/css/products/style.css
- http://a.comp.com/secured/images/products/kb.png
- http://b.comp.com/secured/images/logo.png

And, the following URLs will not qualify:

- http://a.comp.com/public/css/default.css
- http://b.comp.com/public/css/products/default.css
- http://a.comp.com/public/images/products/deature.png
- http://b.comp.com/public/images/comp.png

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

Use Web Cache Service Settings

You must enable this setting if you are going to cobrowse web pages where access to images and CSS files is authenticated. If the setting is not enabled, then agents will not be able to see the images available on the customer side and the formatting of page will be distorted. As a result, the agent and customer browsers will look different. By default this setting is disabled. Set **Yes** to enable the feature.

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

Web Cache Service Domain

Provide a comma separated list of the domains which contain the static content that is authenticated.

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

Web Cache Service Resources

Provide a comma separated list of the resources in the web domain which contain the static content and is authenticated.

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

Use Memory Cache

By default, the application stores all the images and CSS fetched from the list of white-listed domains in the database. On every request, the stored information is fetched from the database. When you enable the memory cache setting, all the static content stored in the database is cached in the application server memory to avoid database calls. You should enable this setting only if the size of static content (images and CSS files) is less than 500 KB.

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

Cobrowse Session Settings

Cobrowse Session Timeout (Minutes)

The cobrowse session timeout interval is the time duration after which the cobrowse session is terminated if any of the following conditions are met — the customer browser is closed, the customer browser is idle (no activity is happening from the customer browser), or the customer navigates to a non-cobrowsable page.

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

List All Active Cobrowse Sessions

This setting governs whether to display the list of all active cobrowse sessions in the Cobrowse pane in the Advisor Desktop. If the value is set to **No**, active cobrowse sessions are not listed in the Cobrowse section. If an agent knows the cobrowse session ID, for example, when he is on phone with a customer, and customer shares the ID, the agent can type the ID in the **Filter** field. The matching session is listed and then the agent can join that session.

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

Start Session on Same Page

Use this setting to determine if the cobrowse session starts on the page that was used to launch the chat session.

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

OneTag Settings

OneTag Data Storage URL

This setting displays the URL for the OneTag Data Storage system. The value of this setting should not be changed.

- Type: Partition settings group
- Subtype: OneTag
- Data type: String
- Default value: http://analytics-egain.com/data
- Value options: —
- Max URL length: 500

OneTag Data Access Details

Provide the OneTag data access details. You should get this information from your eGain account manager. To set the value, click the **Assistance** button in the value field. In the OneTag Data Access Details window, provide the account ID and the Access Token and press Enter. If needed, add details for more accounts. When you are done click the **OK** button to close the window.

- Type: Partition settings group
- Subtype: OneTag
- Data type: String
- Default value: —
- Value options: *Account ID:Access Token*

Retries for Navigation Request to OneTag Server

Use this setting to define the number of times the application attempts to connect to the OneTag server.

Important: **The value of this setting must be changed only under the guidance of the eGain Support team.**

- Type: Partition settings group
- Subtype: OneTag
- Data type: Integer
- Default value: 2
- Minimum value: 0
- Maximum value: 2

Timeout for Navigation Request to OneTag Server

Specify the time after which the application stops trying to connect to the OneTag server.

Important: **The value of this setting must be changed only under the guidance of the eGain Support team.**

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

3 Users

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

Important: **If your system has been integrated with Cisco Unified CCE, the process of creating and configuring users can vary from what is discussed in this guide. For more details, see the** *eGain for Cisco Unified CCE Companion Guide***.**

About Users, Groups, Roles, and Actions

Users

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

Users 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, 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.

The following users are created during the installation:

- **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.
- **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.

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

Users	Licences	Roles	Explicit Actions	Permissions
Administrator	▸ eGain MailPlus: For managing emails ▸ eGain ChatPlus: For managing chat	Administrator		▸ Users: Own, View, Edit, and Delete ▸ User Group: Own group, View group, Edit group, Delete group, Own user, View user, ▸ Edit user, and Delete user ▸ Routing Queues: Own, View, Edit, and Delete ▸ Usage Links: Own, View, Edit, and Delete ▸ KB Folder: View Folder ▸ Reports: View, Run, Edit, Delete, Schedule
Agent	▸ eGain MailPlus: For working on email activities and Solve ▸ eGain ChatPlus: For working on chat activities and Solve ▸ eGain CallTrackPlus: For working on CallTrack activities and Solve ▸ eGain CobrowsePlus: For working on Cobrowse activities ▸ eGain Knowledge+AI: For accessing self-service portals and guided help on self-service portals	Agent	—	▸ KB Folders: View folder, Suggest article ▸ Users: View, Transfer activities, and Pull activities ▸ User Groups: View, Transfer activities, and Pull activities ▸ Routing queues: View, Transfer activities, and Pull activities ▸ Data usage links: View and Execute

Users	Licences	Roles	Explicit Actions	Permissions
Author	- eGain Platform or - eGain Knowledge+AI: to be able to preview articles in a portal and author guided help.	Author	- Portal - Import - Portal - Launch all Knowledge Promotions - Portal - Launch a Knowledge Promotion - Portal - Generate Sitemap - Knowledge Base - Export Related Questions - Knowledge Base - Export Translations - Knowledge Base - Import Translations - KB Folders: Reset Lock - Article Template: View, Create, Edit, Delete - Article Type Folder: View, Create, Edit, Delete - Knowledge Workflow: View, Create, Edit, Delete - Manage Stage: View, Create, Edit, Delete - Usage Links - View - Usage Links - Execute	- Permission on KB folders. - Permissions on queues for bookmarking articles for queues. - Permissions on data usage links to be able to add links in the KB content and be able to execute them.
Knowledge Base Manager	- eGain Platform or - eGain Knowledge+AI: to be able to preview articles in a portal and author guided help.	Knowledge Base Manager	- Portal - Import - Portal - Launch all Knowledge Promotions - Portal - Launch a Knowledge Promotion - Portal - Generate Sitemap - Knowledge Base - Export Related Questions - Knowledge Base - Export Translations - Knowledge Base - Import Translations - KB Folders: Reset Lock - Usage Links - View - Usage Links - Execute	- Permission on KB folders. - Permissions on queues for bookmarking articles for queues. - Permissions on data usage links to be able to add links in the KB content and be able to execute them.

Users	Licences	Roles	Explicit Actions	Permissions
Social manager	- eGain Platform or - eGain MailPlus			No permissions are needed to work in the Social Console.
Offers manager	- eGain Platform		- Preference Group - Edit	No permissions are needed to manage offers from the Offers Console.
Supervisor	- eGain Platform or - eGain MailPlus: For email supervisory loops - eGain ChatPlus: For viewing chat monitors.	Supervisor	—	No permissions are need for performing supervision tasks from the Supervision Console.

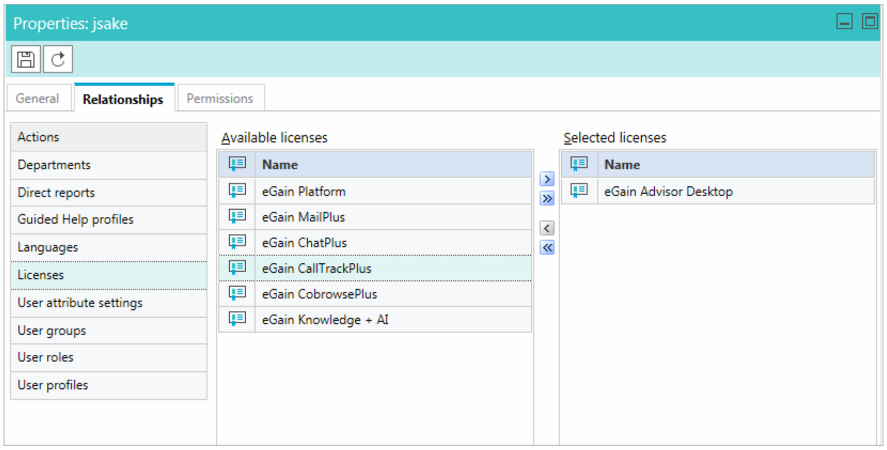
User Groups

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.

Licenses

Licenses are essential for users of the application. Every user in the application must have the necessary licenses to sign in and utilize various functions within the application. Some licenses can be assigned to individual users, but no licenses can be assigned to user groups. If you have configured your application for auto-provisioning through SAML 2.0 single sign-on, the application can assign licenses to users as they are registered in the system. For more information, see "User Auto-Provisioning" on page 228.

The assignment of the correct licenses to users is paramount. If users have not been assigned the correct licenses, they may be able to sign in to the application, but unable to perform their required tasks. For example, a user that is assigned the Author role, requires only the Platform license to access the application and begin authoring articles. However, if a user is assigned the Agent role, one of the other licenses (MailPlus, ChatPlus, etc) must be assigned to allow the user to access the Advisor Desktop and work on various types of activities.



Available licenses

Name
eGain Platform
eGain MailPlus
eGain ChatPlus
eGain CallTrackPlus
eGain CobrowsePlus
eGain Knowledge + AI

Selected licenses

Name
eGain Advisor Desktop

The licenses that appear here are user-based

Types of Licenses

Licenses operate under the following policies:

- **Concurrent:** Concurrent licenses can be assigned to an unlimited number of users. Concurrent licenses are consumed when users with those licenses log in and are released when the users log out. The consumption of those licenses by users at the same time is based on the total number of units purchased.

  For example, if 100 agents have been assigned the MailPlus license, but only 50 concurrent licenses have been purchased, then only 50 of those agents can be logged in at one time. If an offline agent with this license wants to access the application, one of the users currently logged in with that license must log out.

  For more information about license consumption, see "License Consumption and Release" on page 139.

- **Named:** Named licenses belong to the users to whom they are assigned, as in, users assigned a Named license are not affected by other users with the same license. Named licenses are consumed when they are assigned to users and are released only when the licenses have been unassigned.

  For example, if you have 100 agents and only 50 Named MailPlus licenses, then only 50 of those agents can be assigned the licenses at one time. If a new agent needs to work on mail activities, a MailPlus license must be unassigned from one of the other agents and re-assigned to the new agent.

There are other licenses that are nonuser-based licenses for specific functions within the application. All deployments have nonuser-based licenses. These licenses cannot be assigned to users are used to enable various features of the application, such as Content Offers or Messaging. For more information about viewing the licenses in an installation, see "Viewing Licenses" on page 140.

Most licenses provide access to more than one product and are consolidated into combo licenses, such as MailPlus, ChatPlus, etc. These allow users to utilize different tools and navigate through the various consoles of the application without restraint. Since these combo licenses include products that may overlap with other combo licenses (i.e. ChatPlus and MailPlus), it is recommended to reduce redundancy and assign as few licenses as necessary per user. Consult the table below for a list of licenses in the application.

Important: **The eGain Platform license should not be assigned to users with other combo licenses already assigned as the total number of eGain Platform licenses is limited and the combo licenses provide the same level of access.**

The following table lists the licenses that can be provided with the application. The licenses may vary with your installation.

License	Included Products (combo licences)	User-based or Nonuser-based	Available Policy Type	Additional Details
Platform	▸ N/A	User-based	▸ Concurrent or ▸ Named	▸ The basic platform license. Every user attempting to access the application must be assigned this license or a combo license that includes the Platform product. ▸ The total number of Platform licenses provided with an application is limited. Therefore, it is recommended that combo licenses be used in most cases; Platform licenses should only be assigned to administrators or users who do not need to access to multiple products within the application.
Knowledge+AI	▸ Platform ▸ Data Adapters ▸ Agent and Self-Service Portals ▸ Agent Guided Help	User-based	▸ Concurrent or ▸ Named	▸ The Knowledge+AI license is required to access Guided Help on the self-service portal. ▸ Authors do not require this license to author and publish articles. ▸ Required for authors to preview articles in a portal.
MailPlus	▸ Platform ▸ Data Adapters ▸ Mail ▸ Agent Portal access in Advisor Desktop ▸ Social	User-based	▸ Concurrent or ▸ Named	▸ Social media managers must have either this license or Advisor Desktop.
ChatPlus	▸ Platform ▸ Data Adapters ▸ Chat ▸ Video Chat ▸ Agent Portal access in Advisor Desktop ▸ Agent Offers	User-based	▸ Concurrent or ▸ Named	
CallTrackPlus	▸ Platform ▸ Data Adapters ▸ CallTrack ▸ Agent Portal access in Advisor Desktop	User-based	▸ Concurrent or ▸ Named	

License	Included Products (combo licences)	User-based or Nonuser-based	Available Policy Type	Additional Details
CobrowsePlus	Platform Data Adapters Cobrowse Agent Portal access in Advisor Desktop	User-based	Named	
SelfService+AI	Customer Portals Customer Guided Help	Nonuser-based	Concurrent	This license is consumed when a customer accesses the self-service portal or guided help.
Content Offers	N/A	Nonuser-based	Other	
Hot Leads	N/A	Nonuser-based	Other	
Social Monitoring	N/A	Nonuser-based	Other	
ClickToCall	N/A	Nonuser-based	Other	
Advanced Workflow	N/A	Nonuser-based	Other	
Messaging	N/A	Nonuser-based	Other	
Document Search	N/A	Nonuser-based	Other	

License Consumption and Release

The following section only applies to the consumption and release of concurrent licenses.

Concurrent licenses are consumed upon logging in to the application through one of its channels and are released upon logging out. If there are not concurrent licenses available when a user is attempting to log in, the user is unable to log in to the various channels of the application. The application defines the channels through which users can log in as:

- **Advisor Desktop**: This channel applies to signing in to the Advisor Desktop. Only one active login via this channel is permitted per user.
- **All Other Consoles**: This channel applies to signing in to other consoles like the KB or Administration Consoles.
- **Self-Service Portals & APIs**: This channel applies to signing in to the application through web services APIs. This includes self service portal authentication, but does not apply to portal access through the Advisor Desktop or through the preview in portal function in the KB Console. Five active logins via this channel are permitted per user. For more information about the use of APIs, see *eGain Knowledge Access API Reference Guide* and *eGain Knowledge Authoring and Interaction API Reference Guide*.

Since users may require access to a single channel multiple times, or multiple channels at once, there is some flexibility when it comes to consuming concurrent licenses. Assuming a user has all the necessary licenses, that user may have one active login of each channel in the same instance. If the user is actively logged in to the Advisor Desktop, that user can log in to one of the other consoles and the self-service portal before consuming additional licenses. If no additional licenses are available, the user is unable to create new logins until the consumed licenses have been released.

For example, an agent with the Advisor Desktop concurrent license, who is also a knowledge author, is answering emails in the Advisor Desktop and using the Solve feature to access the knowledge portal. An error in one of the articles needs to be fixed, so the agent opens the KB Console to author and fix the article without closing the Advisor Desktop. Once he is done editing the article and publishes it, the agent checks the portal in his browser to view the changes. In this single instance, the consumption of the license has given the agent access to all three channels.

When a user logs out, the licenses that were consumed for the login are released. Once the licenses are released, they are available again for consumption. If a user with a set of licenses has logged in to multiple channels, that set of licenses is not released until that user signs out of each of those channels. If the user has created additional logins beyond the initial three channels, a new login session is created and a second set of let of licenses is consumed. Thus, to release each set of licenses, the user must log out of the channels to which each license set applies.

For example, if the same user as before is logged in to the Advisor Desktop, the KB Console, and the self-service portal, the license set is not released until the user has logged out of all three channels, regardless of the order in which the logout is performed. If that same user is logged in to all three channels and creates an additional login on the self-service portal, another set of licenses is consumed. In order for the first set of licenses to be released, the user must log out of the Advisor Desktop, the KB Console, and the first portal session. The second set of licenses will be released if the user logs out of the second portal session.

Upon logging in to the application, the application attempts to consume all concurrent licenses assigned to the user. Under specific circumstances in which the total number of available concurrent licenses is does not match the total number of users logging into the various channels, an exception is made and not all licenses are consumed.

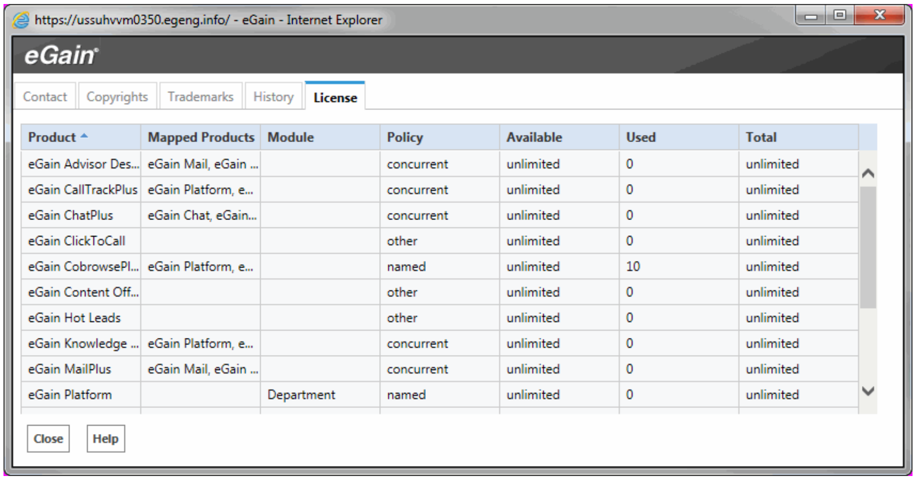
Viewing Licenses

The list of licenses available in your installation can be viewed at any time.

To view the licenses in your installation:

1. Access the About window. This can be achieved by performing the following:
   - **If not signed into the application:** Click the **About** option on the login screen.
   - **If signed into the application:** Navigate to the Help dropdown in the Console Toolbar and click the **About eGain** option. This can be done in any of the user consoles.

2. Click the **License** tab to view all the licenses available in your installation.



https://ussuhvvm0350.egeng.info/ - eGain - Internet Explorer
eGain
Contact
Copyrights
Trademarks
History
License
Close
Help

Product	Mapped Products	Module	Policy	Available	Used	Total
eGain Advisor Des...	eGain Mail, eGain ...		concurrent	unlimited	0	unlimited
eGain CallTrackPlus	eGain Platform, e...		concurrent	unlimited	0	unlimited
eGain ChatPlus	eGain Chat, eGain...		concurrent	unlimited	0	unlimited
eGain ClickToCall			other	unlimited	0	unlimited
eGain CobrowsePl...	eGain Platform, e...		named	unlimited	10	unlimited
eGain Content Off...			other	unlimited	0	unlimited
eGain Hot Leads			other	unlimited	0	unlimited
eGain Knowledge ...	eGain Platform, e...		concurrent	unlimited	0	unlimited
eGain MailPlus	eGain Mail, eGain ...		concurrent	unlimited	0	unlimited
eGain Platform		Department	named	unlimited	0	unlimited

Licenses installed with the application

User Roles

A role is a set of permissible actions for various business resources. An agent's role, for instance, would include actions such as "Edit customer" and "Add notes." You can 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 and templates for roles. You can use the default roles, and if required, create your own user roles using role templates. 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. To know more about the role of a partition administrator, see "Partition Administrator" on page 144.

  A department administrator is created by the partition administrator, and has the authority to create all the resources for the department he administers. This includes: setting rules for incoming and outgoing activities through workflows, creating classifications, dictionaries, users, and assigning permissions to the users to perform various tasks.

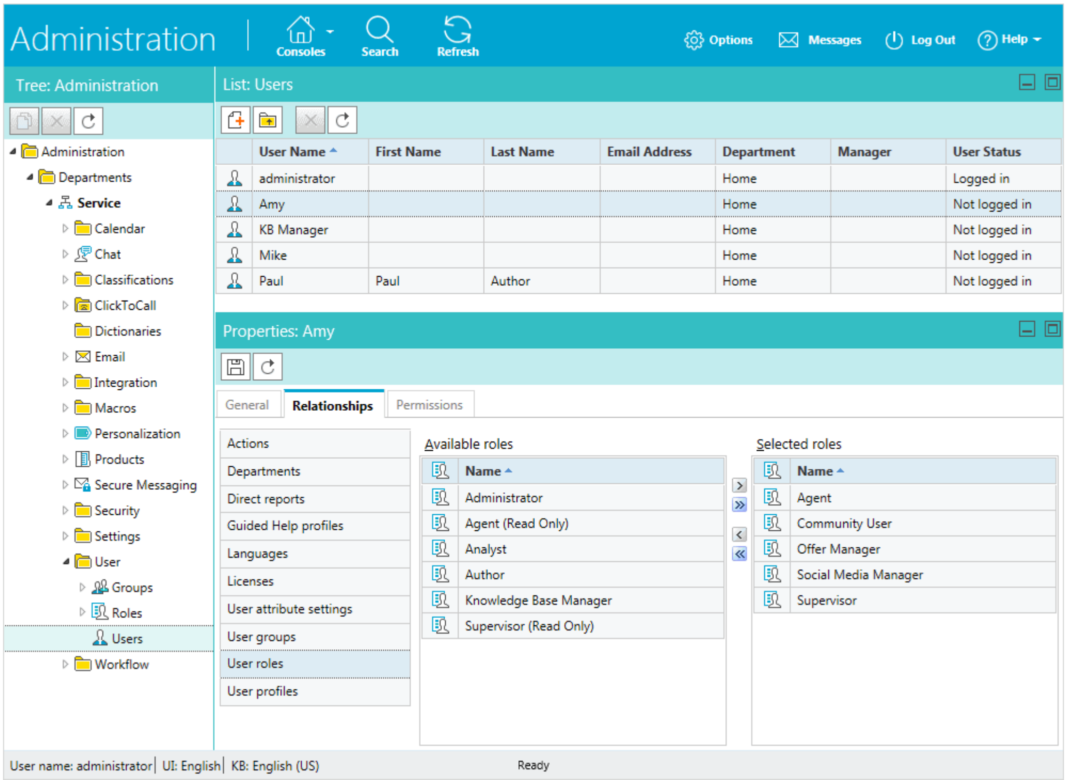
- **Agent:** An agent is a person who handles customer queries, who is directly in contact with the customer. He has access to the Advisor Desktop. Agents are created by the administrator of the department.

- **Agent (Read Only):** An agent (read only) has access to the Advisor Desktop, 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.

- **Analyst:** An analyst is a person who reviews and interprets the data retrieved and displayed in eGain Analytics.

- **Author:** An author is the writer of all the articles that agents can use as replies for customer queries. An author has access to the Knowledge Base Console, which is a store house for all company articles.

- **Knowledge Base Manager:** A knowledge base manager can do all the tasks that a user with the author role can do. In addition to that, he can manage article types and templates and configure knowledge workflows from the Knowledge Base Console.
- **Offer Manager:** An offer manager has access to the Offers Console. He can create offers and configure pages where offers should be presented. He can also monitor the success of offers by viewing dashboards and analytics data.
- **Social Media Manager:** A social media manager has access to the Social Console. He configures adapters, search terms, monitor the social activity from the Social Inbox, and creates activities and cases for the search results.
- **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.



User Name	First Name	Last Name	Email Address	Department	Manager	User Status
administrator				Home		Logged in
Amy				Home		Not logged in
KB Manager				Home		Not logged in
Mike				Home		Not logged in
Paul	Paul	Author		Home		Not logged in

Available roles

Name
Administrator
Agent (Read Only)
Analyst
Author
Knowledge Base Manager
Supervisor (Read Only)

Selected roles

Name
Agent
Community User
Offer Manager
Social Media Manager
Supervisor

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

Selecting user roles

Actions

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

Permissions

Permissions allow you to give users access to particular business objects, such as KB folders, queues, data access links, 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.

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 might 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
Advisor Desktop	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
Role	Create, View, Edit, Delete
Access Links	Create, View, Edit, Delete
Usage links	Create, Own, View, Edit, Delete, Execute
System Attribute Profiles	View, Edit
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
Customer	Create, View, Edit, Delete, Change
Contact Person	Create, Edit, Delete
Contact Details	Create, Edit, Delete
Association	Create, View, Edit, Delete
Inbox Folder	Create, Delete
Notes	View, Delete
Resolution Codes	Create, View, Edit, Delete
Customer Associations	Create, View, Edit, Delete
Macro	Create, View, Edit, Delete
Product Catalog	Create, View, Edit, Delete

Resource Name	Actions Permitted
Business Objects	Create, View, Edit, Delete
Case	Edit, Close, Unarchive
Monitors	Create, Edit, Delete, Run
Reports	Create, Delete, View, Run, Edit, Schedule
Queue	Create, Own, View, Edit, Delete
Workflow	Create, View, Edit, Delete
Settings	Create, View, Edit, Delete
Shift Label	Create, View, Edit, Delete
Day Label	Create, View, Edit, Delete
Calendar	Create, View, Edit, Delete
Dictionary	Create, View, Edit, Delete
Search Console	View
Global Search	Create, Edit, Delete
Service Levels	Create, Read, Edit, Delete
Personal Search	Create
Alias	Create, View, Edit, Delete
Blocked Addresses	Create, View, Edit, Delete
Delivery Exceptions	Create, View, Edit, Delete
Blocked File Extensions	Create, View, Edit, Delete
Email	Send Email, Resubmit supervised emails, Reject emails for supervision, Send and Complete Email, Edit Reply Type, Edit From field, Edit Reply To field, Edit To field, Edit CC field, Edit BCC field, Accept emails for supervision
Blocked Attachment	Restore
Incoming Attachment	Delete
Profiles	Create, View, Edit, Delete
Profiles Management	View
Personalization	View, Manage

Actions assigned to the Administrator role

Agent

The following actions have to be explicitly assigned to agents, if you want them to be able to do the associated tasks.

Resource name	Actions permitted
Search Result	Change Sentiment [this action allows agents to change the sentiment of social activities.]

Explicit actions for agents

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

Resource Name	Actions Permitted
Advisor Desktop	View
User	View
Usage links	View, Execute
Category	View
Customer	Create, View, Edit, Delete, Change
Contact Person	Create, Edit, Delete
Contact Details	Create, Edit, Delete
Association	Create, View, Edit, Delete
Inbox Folder	Create, Delete
Notes	View, Add, Delete
Resolution Codes	View
Folder	View
Article	Suggest
Personal Folders	Manage
Macro	View
Product Catalog	View
Activity	Edit Subject, Create, Print, Complete, Unpin, Pull Selected Activities, Edit, Pull Next Activities, Transfer Activities, Add Footer, Add Greeting, Add Attachment, Add Header, Assign Classification, Add Signature, Pin
Case	Edit, Print, Close
Queue	View
Personal Dictionary	Create
Personal Search	Create
Email	Send Email, Resubmit supervised emails, Reject emails for supervision, Send and Complete Email, Edit Reply Type, Edit From field, Edit Reply To field, Edit To field, Edit CC field, Edit BCC field, Accept emails for supervision
Blocked Attachment	Restore
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.
	Print	Enables the **Print** button in the following toolbars: ▸ The Main Inbox toolbar ▸ The toolbar in the Activity pane ▸ The toolbar in the Case pane ▸ The Search Console toolbar, while searching for activities **Note:** In the Print window (which opens on clicking the **Print** button), only the **Summary of activities assigned to me** and **Currently selected activity contents** options are enabled. The **Currently selected case contents** is enabled only when the **Print Case** action is assigned to an agent.
	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 **Add** and **Save** buttons in the Classify section of the Activity pane, so that agents can assign categories and resolution codes to activities.

Resource Name	Actions Permitted	Description
Case	Edit	Allows an agent to edit the case details. Enables the **Save** button in the Case pane. 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 Case pane.
	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 Case pane.
	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 Case pane.
Calltrack	Send email with transcript of phone call	-
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 Chat** 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 Inbox. 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 Customer pane.
	Delete	Allows an agent to delete a customer associated with an activity. It enables the **Delete** button in the Customer pane.
	Change Customer	Allows an agent to change the customer associated with an activity. Displays the **Change customer** button in the Customer pane.
	Create Contact Person	Allows an agent to create a contact person for group and corporate customers. It enables the **New** button in the Customer pane 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 Customer pane 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 Customer pane 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 Contact details of the Customer pane.
	Edit Contact Details	Allows an agent to edit the contact details of a customer. It enables the **Save** button in the Customer pane 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 Customer pane 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 Customer pane 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 Customer pane 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 Customer pane 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.
Filter Folder (Inbox 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.

Resource Name	Actions Permitted	Description
	Delete	Enables the **Delete** button in the Inbox Tree pane toolbar. Using this button, agents can delete search folders and personal folders from their inbox.
KB Folder	Suggest Article	Allows an agent to suggest articles to the Knowledge Base. Agents can suggest articles to only those folders, on which they have the **Suggest Article** permission. All agents have permissions to suggest 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 choose not to give **Suggest Article** permission on those folders. It also allows the agent to suggest articles from the reply pane.
	View Folder	Allows agents to view Knowledge content in the Knowledge pane. This action is assigned to all agents with the **Platform** license and it cannot be removed. But, the view access to articles in a folder can be controlled by permissions. 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 to the following types of Knowledge Base articles: personal articles, pending suggestions, and suggestions. It enables the **Notes** button.
Macro	View	Allows agents to view and use macros in emails, chats, tasks, phone logs, 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 Notes section, which can be accessed from the following panes: ‣ Activity Pane ‣ Case Pane ‣ Customer Pane
	Add	Allows an agent to add notes to cases, activities, customers, and customer associations. It displays the **Add notes** option in the Notes section, which can be accessed from the following panes: ‣ Activity Pane ‣ Case Pane ‣ Customer Pane 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 section, which can be accessed from the following panes: ‣ Activity Pane ‣ Case Pane ‣ Customer Pane
	Delete	Allows an agent to delete the notes associated with cases, activities, customers, and customer associations. It enables the **Delete button** in the Notes Notes section, which can be accessed from the following panes: ‣ Activity Pane ‣ Case Pane ‣ Customer Pane
Release	Search	
	Make Suggestions	

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
Search Console	View Search Console	Allows agents to access the Search Console and run searches for objects in the system, such as cases, activities, or customers.
System Resource	View Advisor Desktop	Allows an agent to access the Advisor Desktop.
Usage links	Execute	This action can be assigned only to agents with the eGain MailPlus or eGain ChatPlus licenses. It enables the **Execute** and **Add Results to Reply** buttons in the Links pane. These buttons are enabled only if the agent has **Execute** permission on at least one usage link.
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
Advisor Desktop	View
User	View
Usage links	View, Execute
Category	View
Customer	View
Inbox Folder	Create, Delete
Notes	View
Resolution Codes	View
Folder	View
Article	Suggest
Macro	View
Product Catalog	View
Activity	Print
Case	Print
Search Console	View
Queue	View

Actions assigned to the Agent (read only) role

Knowledge Base Manager Role

The various actions assigned to the Knowledge Base Manager role are listed in the following table.

Resource Name	Actions Permitted
System Resource	View Agent
System Resource	View Reports
System Resource	View Knowledge Console
User	View
Categories	View
Notes	View, Add, Delete
Resolution	View
KB Folder	Create Folder, Own Folder, View Folder, Edit Folder, Delete Folder, Add Notes, Delete Notes
KB Folder	Create Article, Edit Article, Print Article, Delete Article, Suggest Article, Import Article, Associate Article With Topics
KB Folder	Manage Suggestions
KB Folder	Manage Personal Folders, View Personal Folder
KB Folder	Manage Bookmarks
KB Folder	Create Lists, Delete Lists, Edit Lists
Article Template	View, Create, Edit, Delete
Article Type Folder	View, Create, Edit, Delete
Knowledge Workflow	View, Create, Edit, Delete
Manage Stage	View, Create, Edit, Delete
Macro	View, Create, Delete, Edit
Portals	View, Create, Edit, Copy, Delete
Manage Approval process	Manage Approval Process
Release	Manage Approval Process, Search, Manage Suggestions, Make Suggestions, Manage Release, Author, Create, Export Casebase, Make Suggestions, Import Casebase
Report	View, Run, Edit, Delete, Create, Schedule
Text Editor	Edit HTML source for articles
Topic	Copy, View, Delete, Edit, Create, Cut
Locations	View
Channels	View
Expertise	View

Resource Name	Actions Permitted
Profiles	View
Search Console	View
Saved Search	Create, Delete, Edit
Messaging	Create Message, Delete Message

Actions assigned to the Knowledge Base Manager role

The following actions have to be explicitly assigned to authors, if you want them to be able to do the associated tasks.

Resource Name	Actions Permitted
Portals	Replication, Replication Launch All
Knowledge Base	Import Translations, Export Translation, Export Related Questions
KB Folders	Reset Lock

Explicit actions for he Knowledge Base Manager role

Author

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

Resource Name	Actions Permitted
System Resource	View Agent
System Resource	View Reports
System Resource	View Knowledge Console
User	View
Categories	View
Notes	View, Add, Delete
Resolution	View
KB Folder	Create Folder, Own Folder, View Folder, Edit Folder, Delete Folder, Add Notes, Delete Notes
KB Folder	Create Article, Edit Article, Print Article, Delete Article, Suggest Article, Import Article
KB Folder	Manage Suggestions
KB Folder	Manage Personal Folders, View Personal Folder
KB Folder	Manage Bookmarks
KB Folder	Create Lists, Delete Lists, Edit Lists
Macro	View, Create, Delete, Edit
Portals	View, Create, Edit, Copy, Delete
Manage Approval process	Manage Approval Process
Release	Manage Approval Process, Search, Manage Suggestions, Make Suggestions, Manage Release, Author, Create, Export Casebase, Make Suggestions, Import Casebase
Report	View, Run, Edit, Delete, Create, Schedule
Text Editor	Edit HTML source for articles
Topic	Copy, View, Delete, Edit, Create, Cut
Locations	View
Channels	View
Expertise	View
Profiles	View
Search Console	View
Saved Search	Create, Delete, Edit
Messaging	Create Message, Delete Message

Actions assigned to the Author role

The following actions have to be explicitly assigned to authors, if you want them to be able to do the associated tasks.

Resource Name	Actions Permitted
Portals	Replication, Replication Launch All
Knowledge Base	Import Translations, Export Translation, Export Related Questions
KB Folders	Reset Lock
Article Template	View, Create, Edit, Delete
Article Type Folder	View, Create, Edit, Delete
Knowledge Workflow	View, Create, Edit, Delete
Manage Stage	View, Create, Edit, Delete

Explicit actions for Author role

Analyst

The various actions assigned to the Analyst role are listed in the following table. Note that Analysts will primarily be using eGain Analytics, which is where most of their actions are permissions are configured.

Resource Name	Actions Permitted
KB Folder	Create Folder, View Folder,
KB Folder	Create Article
KB Folder	Manage Suggestions

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 Advisor Desktop, Supervision Console, and Reports Console.

Object	Actions permitted
System Resource	View Agent, View Reports, View Supervision **Note:** These actions provide access to the Advisor Desktop, 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, Pull Next Activities, Pull Selected Activities,Add Greetings, Add Header, Add Attachment, Add Folder, Add Signature, Assign Classification
Calltrack	Send email with transcript of Phone call, Discard call log transcript email
Case	Edit, Print, Close Case, Change Case, Create Case
Categories	View
Chat	Complete Chat Activity, Pull Next Chat Activity, Leave Chat Activity, Transfer Chat Activities, Monitor Chat Activity, Whisper **Note:** The following action enables the supervisor to monitor chats from the **My Monitor** node in the Advisor Desktop: Monitor Chat Activity
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, View Personal Folder, Suggest Article, Delete Notes, Create Agent Personal Folders, Add Notes, Manage Personal Folders
Messaging	Create Message, Delete Message These actions also apply to use in the Advisor Desktop, allowing users to use the Ask option when right-clicking on highlighted text in the Reply pane.
Macros	View
Notes	View, Add, Delete
Personal Dictionary	Personal Dictionary

Object	Actions permitted
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
Usage links	View, Execute
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 (Not in use)	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
Advisor Desktop	View
Reporting Console	View
User	View
Usage links	View, Execute
Customer	View
Association	View
Inbox Folder	Create, Delete
Notes	View
Resolution Codes	View
Folder	View
Article	Suggest
Macro	View
Product Catalog	View
Activity	Print
Case	Print
Monitor	Create, Edit, Delete, Run
Reports	View, Run
Queue	View

Actions assigned to the Supervisor (read only) role

Offer Manager Role

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

Resource Name	Actions Permitted
System Resource	View Offers Console
Offer	Manage Offer Templates

Actions assigned to the Offer Manager role

The following actions have to be explicitly assigned to offer managers, if you want them to be able to do the associated tasks.

Resource Name	Actions Permitted
Preference Group	Edit [this action allows offer managers to change the offers related settings from the Options window in the Offers Console.]

Explicit actions for the Offer Manager role

Social Media Manager Role

The various actions assigned to the Social Media Manager role are listed in the following table.

Resource Name	Actions Permitted
System Resource	View Social Console
Activity	Publish
Preference Group	Edit [This action allows users to edit social settings from the Social Console]
Social Adapters	View, Edit, Create, Delete

Actions assigned to the Social Media Manager role

Managing User Roles

This section talks about:

- Creating User Roles on page 162
- Creating User Subroles on page 165
- Copying User Roles on page 166
- Restoring User Roles on page 166
- Deleting User Roles and Subroles on page 167

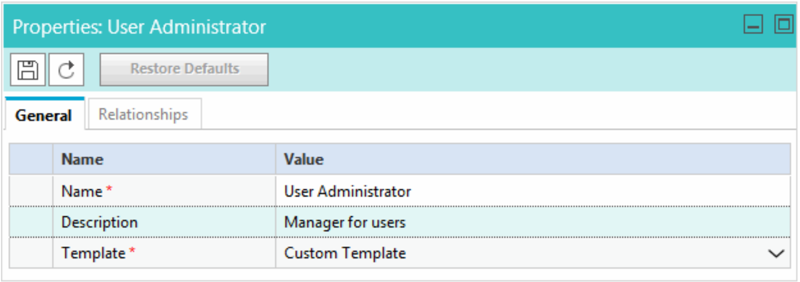
Creating User Roles

To create a user role:

1. In the Tree pane, browse to the **Users** node. Based on where you want to create a user role, do one of the following:
   - If you are a system administrator, go to the system partition and browse to **Administrator > Partition:** *Context_Root_Name* **> User > Roles.**
   - If you are a partition administrator, go to the business partition and browse to **Administrator > Partition:** *Partition_Name* **> User > Roles.**

- If you are a department administrator, browse to **Administration > Departments >** *Department_Name* **> User > Roles.**

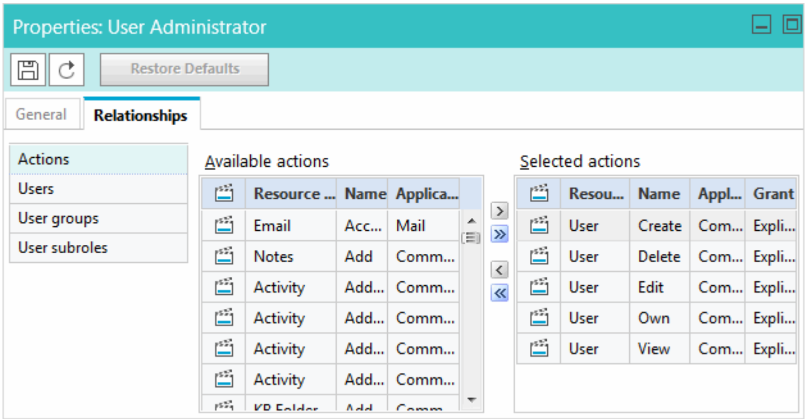
2. In the List pane toolbar, click the **New** button.
3. In the Properties pane, on the General tab, set the following:
   - **Name:** Provide a name for the role
   - **Description:** Provide a brief description.
   - **Template:** From the dropdown list, select an available template or select **Custom Template** to start with a blank role. The template cannot be changed once you save the role.



Name	Value
Name *	User Administrator
Description	Manager for users
Template *	Custom Template

Set general properties

4. Click the **Save** button. This enables the Relationships tab.
5. Next, go to the Relationships tab and do the following.
   a. In the Actions section, select the actions for the role.
      - When you start with a custom template, the role does not have any actions associated with it. While selecting the actions for the role, make sure you select all the actions that are required to do a task. For example, if you want a user with this role to be able to manage resolution codes, then make sure you assign all the four actions, Resolution - Create, View, Edit, and Delete, to the role.
      - If you started with an pre-configured template, like the Agent Template, the Actions section will show the list of actions associated with the template. You can customize the role by adding or removing actions. If you feel you want to go back to the original list of actions, you can restore the role to its default state (page 166).



Available actions

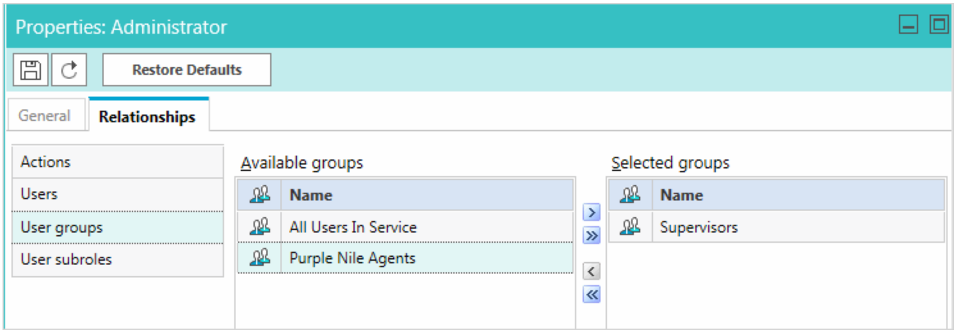
Resource ...	Name	Applica...
Email	Acc...	Mail
Notes	Add	Comm...
Activity	Add...	Comm...
Activity	Add...	Comm...
Activity	Add...	Comm...
Activity	Add...	Comm...
KB Folder	Add	Comm...

Selected actions

Resou...	Name	Appl...	Grant
User	Create	Com...	Expli...
User	Delete	Com...	Expli...
User	Edit	Com...	Expli...
User	Own	Com...	Expli...
User	View	Com...	Expli...

Select actions

b. Go to the User groups section, and assign the role to user groups. You can also choose to assign roles to users individually; however, it is recommended that you assign roles to user groups. It helps you manage your users better.

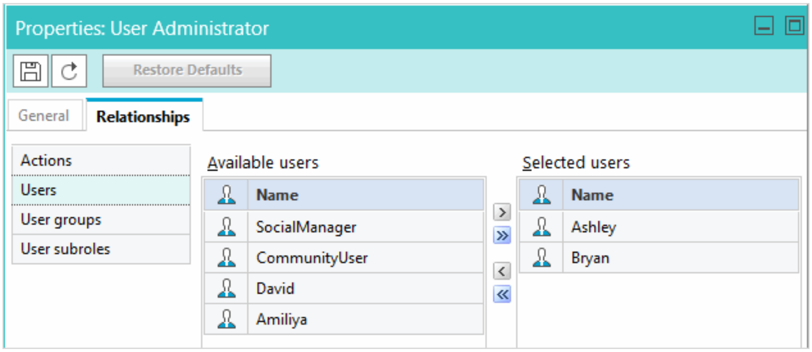


Available groups
Name
All Users In Service
Purple Nile Agents

Selected groups
Name
Supervisors

Assign the role to user groups

c. Next go to the Users section, and assign the role to users.

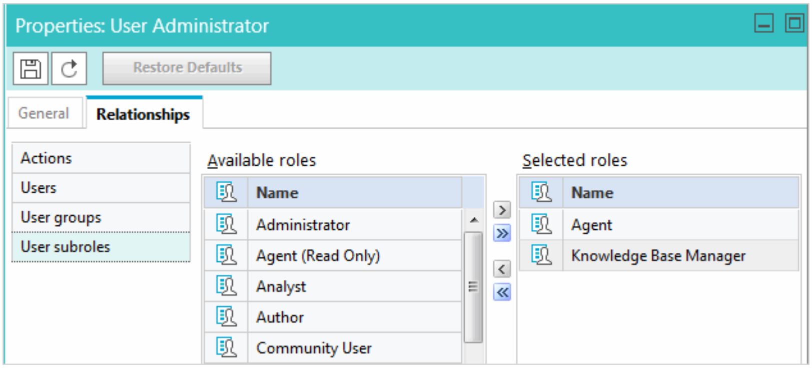


Available users
Name
SocialManager
CommunityUser
David
Amiliya

Selected users
Name
Ashley
Bryan

Assign the role to users

d. Now go to the User subroles section, and select the roles you want to associate with this role as subroles. You can even set default roles as subroles. To know more about subroles, see "Creating User Subroles" on page 165.



Available roles
Name
Administrator
Agent (Read Only)
Analyst
Author
Community User

Selected roles
Name
Agent
Knowledge Base Manager

Select user subroles

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

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

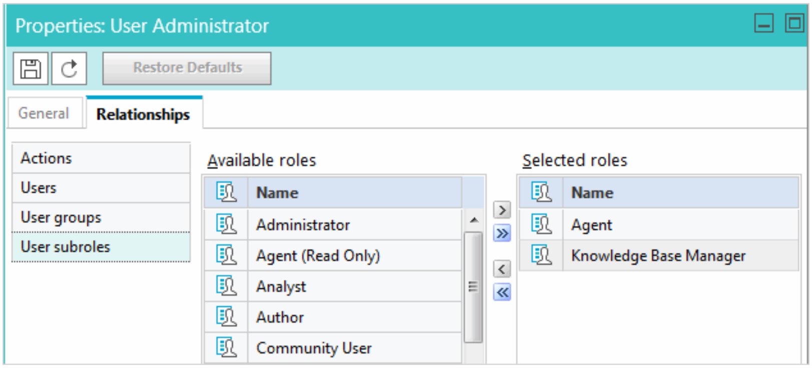
Creating User Subroles

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

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

To create a subrole:

1. In the Tree pane, browse to the **Users** node. Based on where you want to create a user subrole, do one of the following:
   - If you are a system administrator, go to the system partition and browse to **Administrator > Partition:** *Context_Root_Name* **> User > Roles.**
   - If you are a partition administrator, go to the business partition and browse to **Administrator > Partition:** *Partition_Name* **> User > Roles.**
   - If you are a department administrator, browse to **Administration > Departments >** *Department_Name* **> User > Roles.**
2. Select the role for which you want to create a subrole.
   - If you want to use an existing role as a subrole, go to Relationships tab and in the User subroles section, select from the available roles.



Available roles: Name
Administrator
Agent (Read Only)
Analyst
Author
Community User

Selected roles: Name
Agent
Knowledge Base Manager

Select subroles

   - If you want to create a new subrole, follow steps 2 to 5 in "Creating User Roles" on page 162. When you create a role under an existing role, it automatically becomes the subrole of the role.

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

Copying User Roles

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

To copy a role:

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

Restoring User Roles

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

To restore a role:

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

Deleting User Roles and Subroles

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

The system provided roles cannot be deleted. These roles are:

- In the system partition: System Administrator
- In the business partition: Partition Administrator
- In a department: Administrator, Agent, Agent (read only), Supervisor, Supervisor (read only), Author, Offer Manager, Social Media Manager

To delete a user role or subrole:

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

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

Managing User Groups

This section talks about:

- Creating User Groups in System Partition on page 167
- Creating User Groups in Business Partition on page 170
- Creating User Groups in Departments on page 172
- Creating User Subgroups on page 175
- Deleting User Groups on page 176

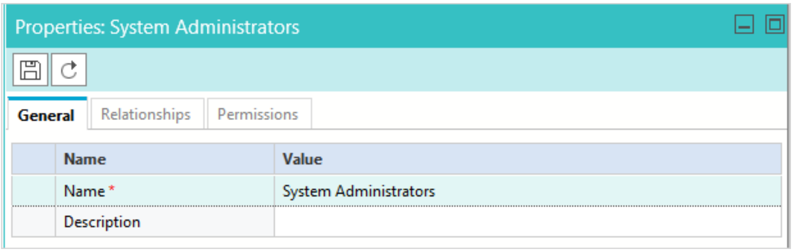
Creating User Groups in System Partition

To create a group of system administrators:

1. Log in to the system partition (zero partition) and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Context_Root_Name* **> User > Groups.**

3. In the List pane toolbar, click the **New** button.

4. In the Properties pane, on the General tab, provide the name and description for the user group.



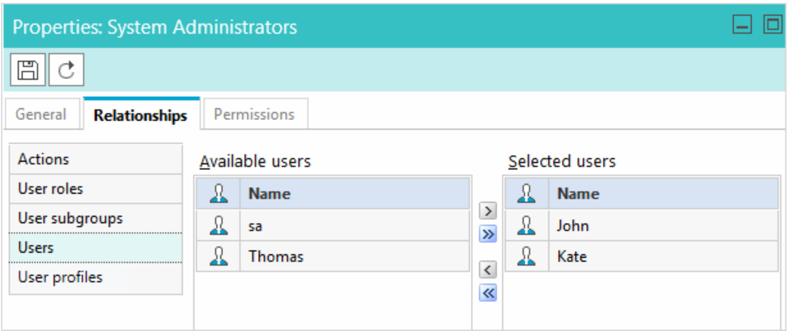
Name	Value
Name *	System Administrators
Description	

Set general properties

5. Click the **Save** button. The Relationships and Permissions tabs are enabled only after you click **Save**.

6. In the Relationships tab, do the following.

   a. Go to the Users tab and select the users who should be part of this user group.



Available users

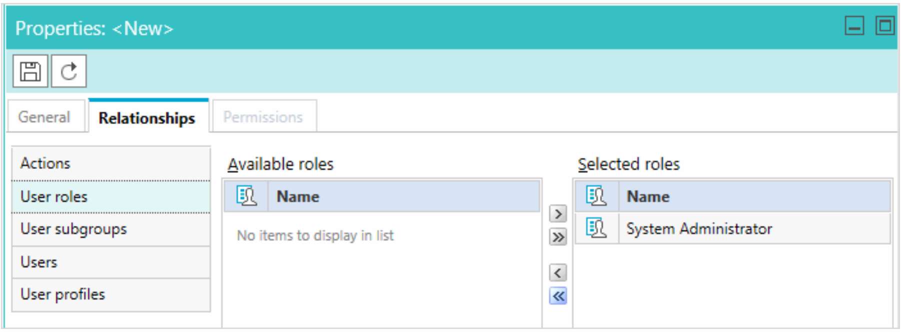
Name
sa
Thomas

Selected users

Name
John
Kate

Select users

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



Available roles

Name
No items to display in list

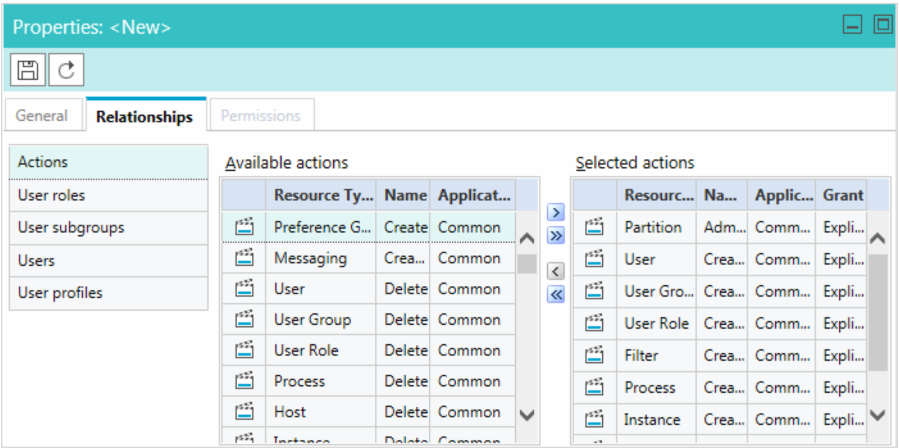
Selected roles

Name
System Administrator

Select user roles

   c. Next, go to the Actions tab, and view the list of actions assigned to the user group. Here you can also assign additional actions to the user group. From the Grant field in the Selected actions section, you can identify how actions are assigned to the user. The actions assigned as part of the role show the name of the role, and actions assigned explicitly show the value “Explicit”.

It is highly recommended that you do not assign actions directly to user groups. You should always create a user role, with the actions, and assign the role to the user. This makes user management easier. For more details on creating user roles, see "Creating User Roles" on page 162.



Available actions

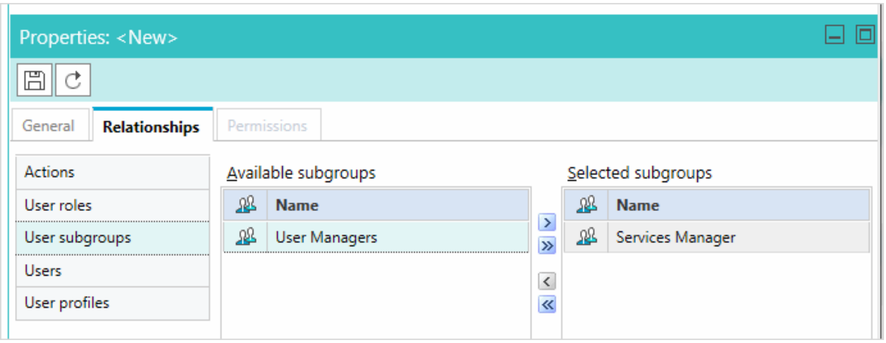
Resource Ty...	Name	Applicat...
Preference G...	Create	Common
Messaging	Crea...	Common
User	Delete	Common
User Group	Delete	Common
User Role	Delete	Common
Process	Delete	Common
Host	Delete	Common
Instance	Delete	Common

Selected actions

Resourc...	Na...	Applic...	Grant
Partition	Adm...	Comm...	Expli...
User	Crea...	Comm...	Expli...
User Gro...	Crea...	Comm...	Expli...
User Role	Crea...	Comm...	Expli...
Filter	Crea...	Comm...	Expli...
Process	Crea...	Comm...	Expli...
Instance	Crea...	Comm...	Expli...

Select actions

d. Next, go to the User subgroups section and select sub groups for the group. For more details on subgroups, see "Creating User Subgroups" on page 175.



Available subgroups

Name
User Managers

Selected subgroups

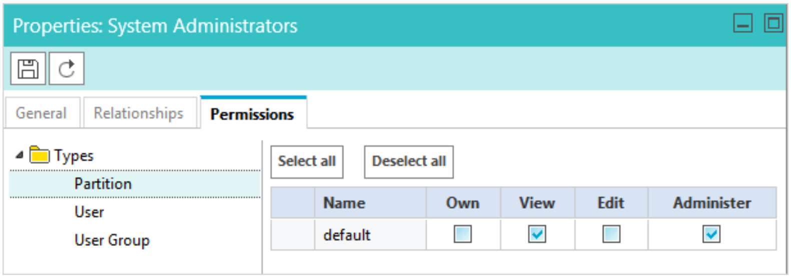
Name
Services Manager

Select user subgroups

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

8. 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



Name	Own	View	Edit	Administer
default	□	☑	□	☑

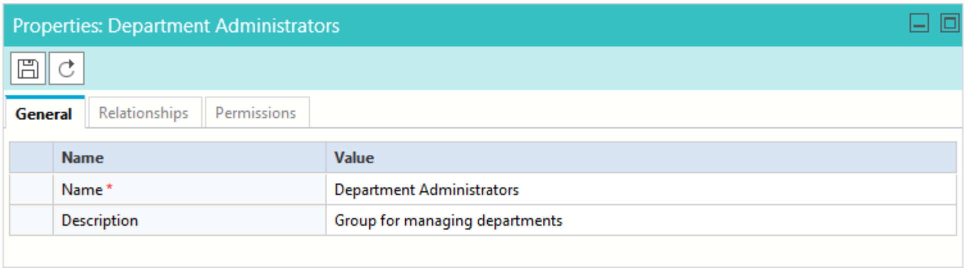
Assign permissions

9. Click the **Save** 🖫 button.

Creating User Groups in Business Partition

To create a group of partition administrators:

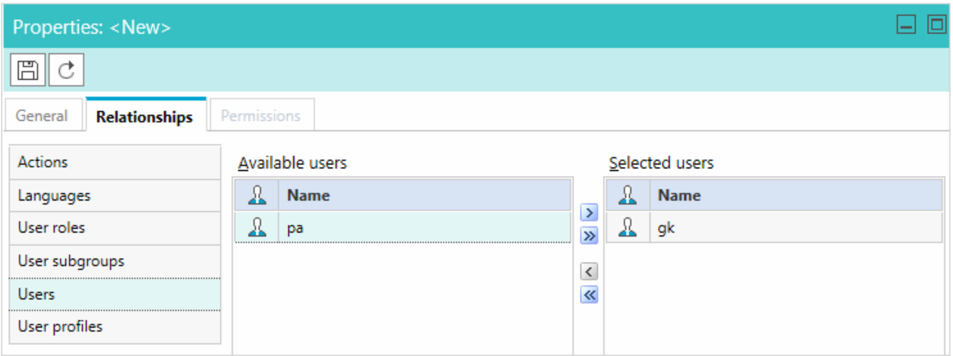
1. Log in to the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> User > Groups.**
3. In the List pane toolbar, click the **New** button.
4. In the Properties pane, on the General tab, provide the name and description for the user group.



Name	Value
Name *	Department Administrators
Description	Group for managing departments

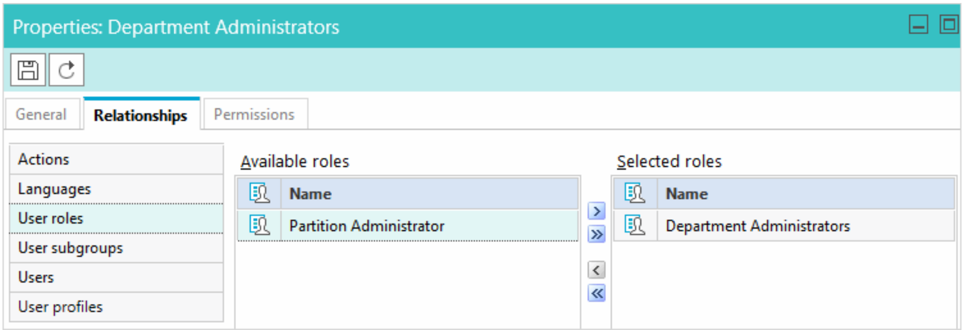
Set general properties

5. Click the **Save** 🖫 button. The Relationships and Permissions tabs are enabled only after you click **Save**.
6. In the Relationships tab, do the following.
   a. Go to the Users tab and select the users who should be part of this user group.



Select users

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



Available roles:

Name
Partition Administrator

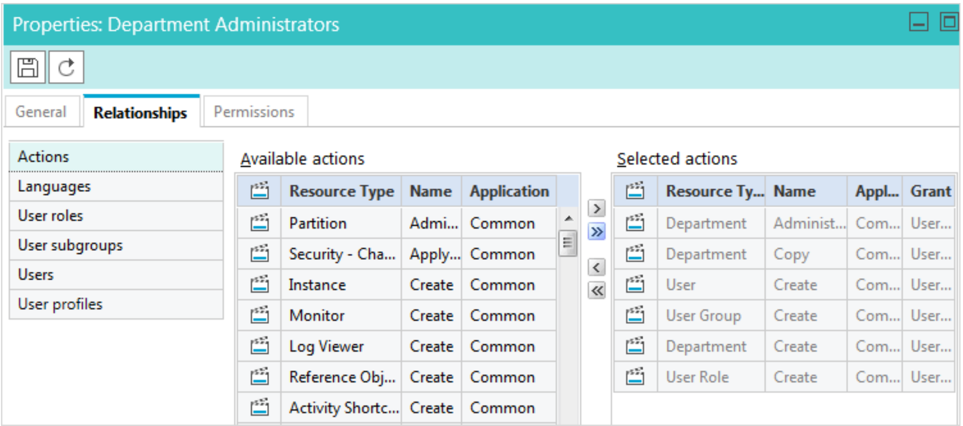
Selected roles:

Name
Department Administrators

Select user roles

c. Next, go to the Actions tab, and view the list of actions assigned to the user group. Here you can also assign additional actions to the user group. You can identify how actions are assigned from the Grant field in the Selected actions section. The actions assigned as part of the role show the name of the role, and actions assigned explicitly show the value "Explicit".

It is highly recommended that you do not assign actions directly to user groups. You should always create a user role, with the actions, and assign the role to the user. This makes user management easier. For more details on creating user roles, see "Creating User Roles" on page 162.



Available actions:

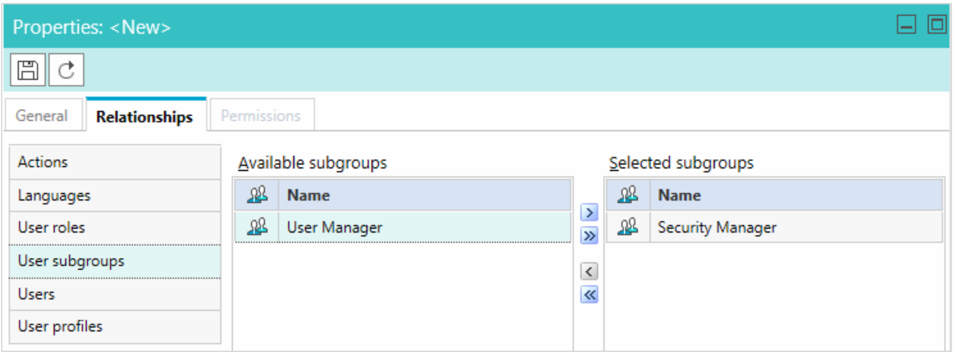
Resource Type	Name	Application
Partition	Admi...	Common
Security - Cha...	Apply...	Common
Instance	Create	Common
Monitor	Create	Common
Log Viewer	Create	Common
Reference Obj...	Create	Common
Activity Shortc...	Create	Common

Selected actions:

Resource Ty...	Name	Appl...	Grant
Department	Administ...	Com...	User...
Department	Copy	Com...	User...
User	Create	Com...	User...
User Group	Create	Com...	User...
Department	Create	Com...	User...
User Role	Create	Com...	User...

Select actions

d. Next, go to the User subgroups section and select subgroups for the group. For more details on subgroups, see "Creating User Subgroups" on page 175.



Available subgroups:

Name
User Manager

Selected subgroups:

Name
Security Manager

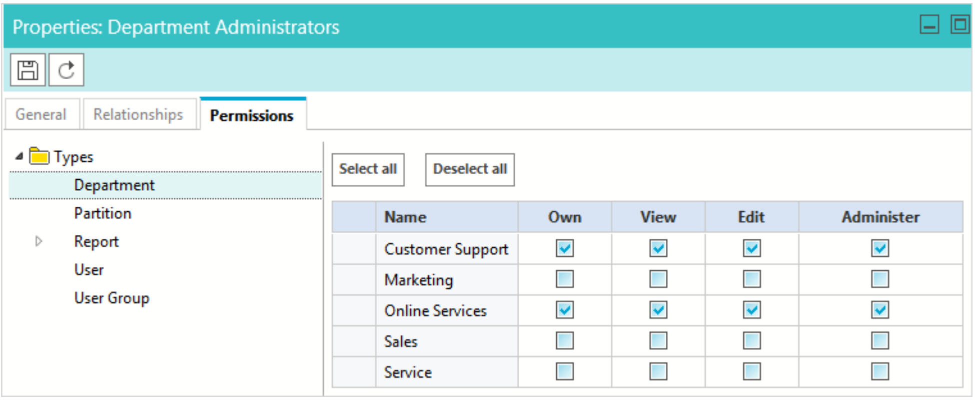
Select user subgroup

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

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

8. 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	□	□	□	□

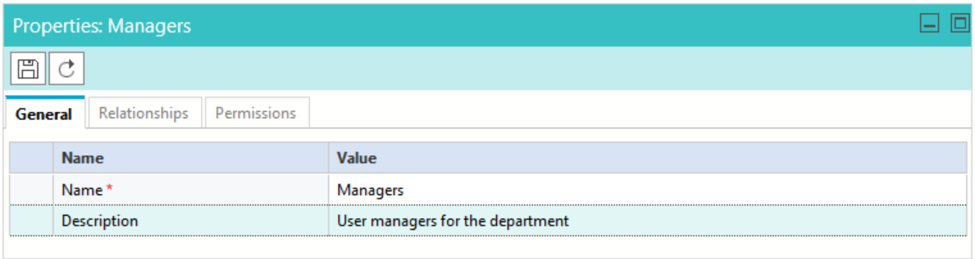
Assign permissions

9. Click the **Save** button.

Creating User Groups in Departments

To create a group of department users:

1. Log in to the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> User > Groups.**
3. In the List pane toolbar, click the **New** button.
4. In the Properties pane, on the General tab, provide the name and description for the user group.



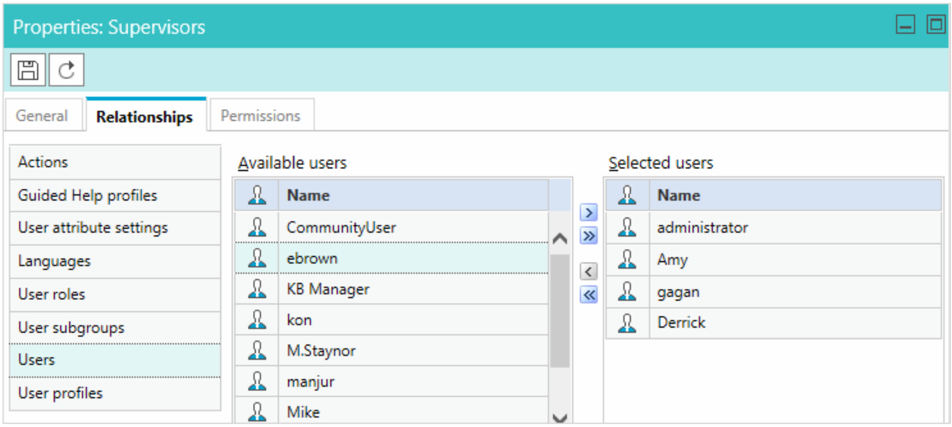
Name	Value
Name *	Managers
Description	User managers for the department

Set general properties

5. Click the **Save** button. The Relationships and Permissions tabs are enabled only after you click **Save**.

6. In the Relationships tab, do the following.

   a. Go to the Users tab and select the users who should be part of this user group.

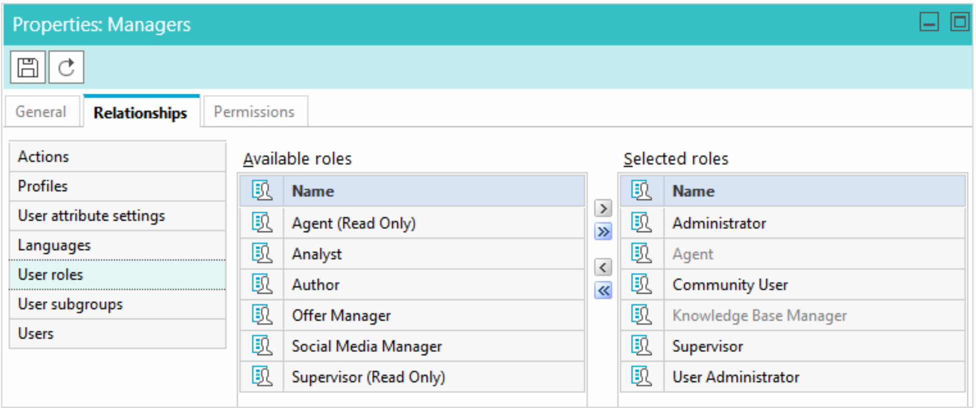


Available users
Name
CommunityUser
ebrown
KB Manager
kon
M.Staynor
manjur
Mike

Selected users
Name
administrator
Amy
gagan
Derrick

Select users

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



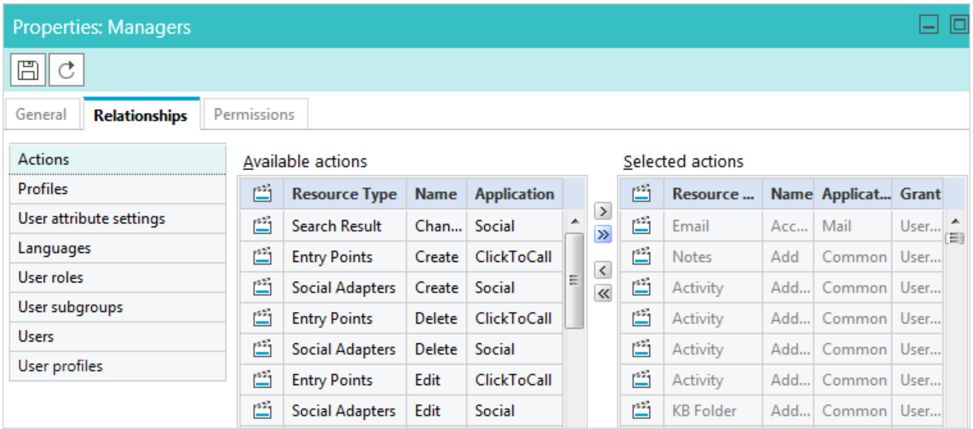
Available roles
Name
Agent (Read Only)
Analyst
Author
Offer Manager
Social Media Manager
Supervisor (Read Only)

Selected roles
Name
Administrator
Agent
Community User
Knowledge Base Manager
Supervisor
User Administrator

Select user roles

   c. Next, go to the Actions tab, and view the list of actions assigned to the user group. Here you can also assign additional actions to the user group. You can identify how actions are assigned from the Grant field in the Selected actions section. The actions assigned as part of the role show the name of the role, and actions assigned explicitly show the value "Explicit".

It is highly recommended that you do not assign actions directly to user groups. You should always create a user role, with the actions, and assign the role to the user. This makes user management easier. For more details on creating user roles, see "Creating User Roles" on page 162.



Available actions

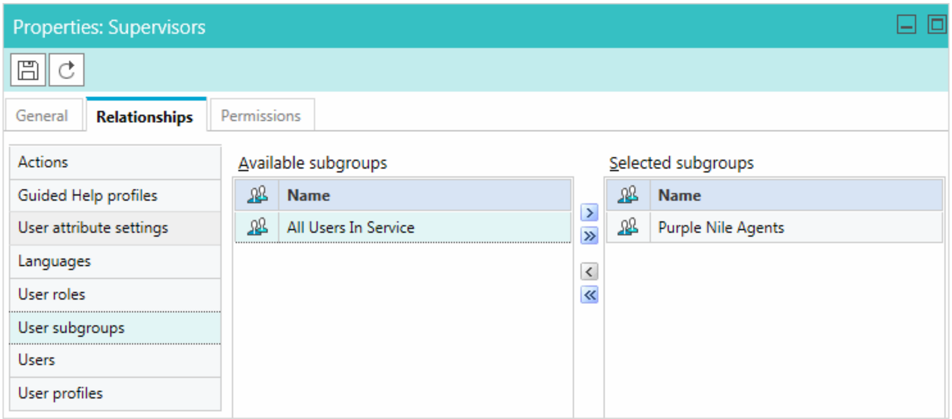
Resource Type	Name	Application
Search Result	Chan...	Social
Entry Points	Create	ClickToCall
Social Adapters	Create	Social
Entry Points	Delete	ClickToCall
Social Adapters	Delete	Social
Entry Points	Edit	ClickToCall
Social Adapters	Edit	Social

Selected actions

Resource ...	Name	Applicat...	Grant
Email	Acc...	Mail	User...
Notes	Add	Common	User...
Activity	Add...	Common	User...
Activity	Add...	Common	User...
Activity	Add...	Common	User...
Activity	Add...	Common	User...
KB Folder	Add...	Common	User...

Select actions

d. Next, go to the User subgroups section and select sub groups for the group. For more details on subgroups, see Creating User Subgroups on page 175.



Available subgroups

Name
All Users In Service

Selected subgroups

Name
Purple Nile Agents

Select user subgroup

e. Next, go the User attribute settings tab and select a user attribute setting for the group. This lets you control the level of access a user has in the system. For more details on user attribute settings, see *eGain Administrator's Guide to Tools Console.*

f. Next, in the Profiles section select the profile to be assigned to the user.

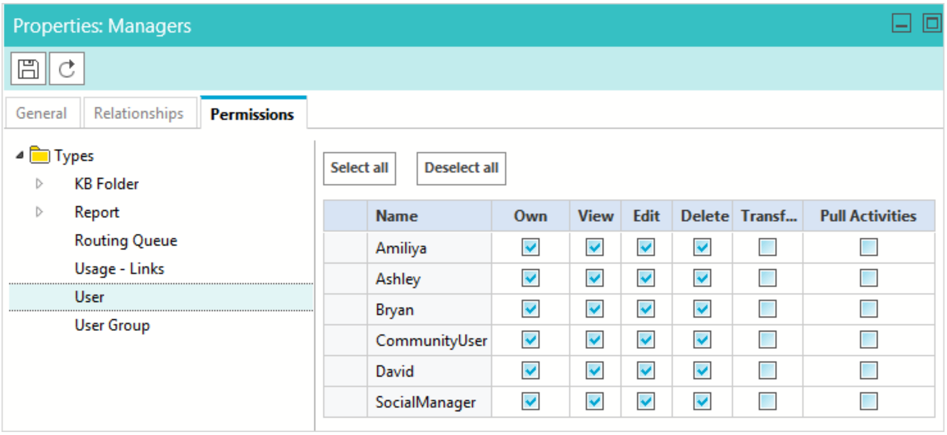
g. Lastly, in the Languages section, select the primary KB language for the user.

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

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

   - **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:** View, Run, Edit, Delete, Schedule
   - **Routing Queue:** Own, View, Edit, Delete, Transfer activities, Pull activities

- **Usage - Links:** Own, View, Edit, Delete, Execute
- **User:** Own, View, Edit, Delete, Transfer activities, Pull activities
- **User group:** Own, View, Edit, Delete, Transfer activities, Pull activities



Name	Own	View	Edit	Delete	Transf...	Pull Activities
Amiliya	☑	☑	☑	☑	□	□
Ashley	☑	☑	☑	☑	□	□
Bryan	☑	☑	☑	☑	□	□
CommunityUser	☑	☑	☑	☑	□	□
David	☑	☑	☑	☑	□	□
SocialManager	☑	☑	☑	☑	□	□

Set permissions

9. Click the **Save** button.

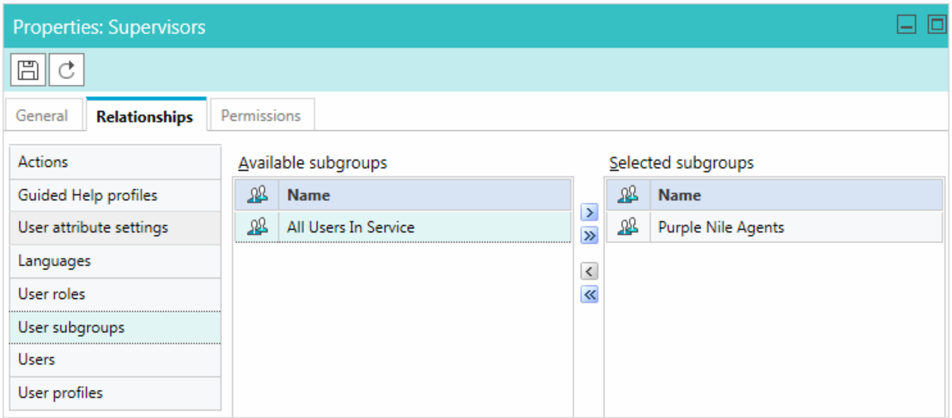
Creating User Subgroups

A group can be added as a subgroup to another group, to assign additional privileges such as, roles, actions, permissions, etc. to the subgroup. For example, if you want the administrator group to also act as supervisors, you can add the administrator group as the subgroup of the supervisor group. Along with the privileges the administrator group already has, it also gets all the privileges of the supervision group.

To create a subgroup:

1. In the Tree pane, browse to the **Users** node. Based on where you want to create a user subgroup, 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 > Groups.**
   - If you are a partition administrator, go to the business partition and browse to **Administrator > Partition:** *Partition_Name* **> User > Groups.**
   - If you are a department administrator, browse to **Administration > Departments >** *Department_Name* **> User > Groups.**
2. Select the group for which you want to create a subgroup.

- If you want to use an existing group as a subgroup, go to Relationships tab and in the User subgroups section, select from the available groups.



Name
All Users In Service

Name
Purple Nile Agents

Select subgroups

- If you want to create a new subgroup, follow steps 3 to 9 from one of the following sections: "Creating User Groups in System Partition" on page 167, "Creating User Groups in Business Partition" on page 170, or "Creating User Groups in Departments" on page 172. When you create a group under an existing group, it automatically becomes the subgroup of the group.

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

This section talks about:

- Creating System Administrators on page 177
- Creating Partition Administrators on page 182
- Creating Department Users on page 186

- Deleting Users on page 193
- Changing User Status on page 194
- Assigning Manager of Users on page 195
- Sharing Users with Other Departments on page 196

Creating System Administrators

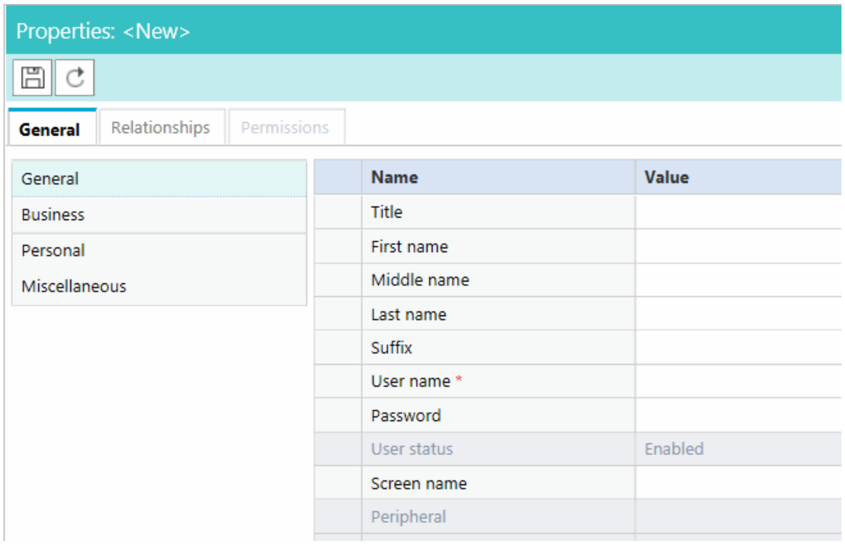
Important: **If you are editing the properties of an existing user who is logged into the application, the user updates take effect only on the next login.**

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.
      - **User status**: Select the status of the user. By default the new user’s status is **Enabled**. Once the user is saved, the following four options are available: Enabled, Disabled, Logged in, and Not logged in. For more information, see “Changing User Status” on page 194

      The following fields are optional.

      - **Title**
      - **First name**
      - **Middle name**
      - **Last name**
      - **Suffix**
      - **Screen name:** This field is not in use.
      - **Mobile number 1**
      - **User type**

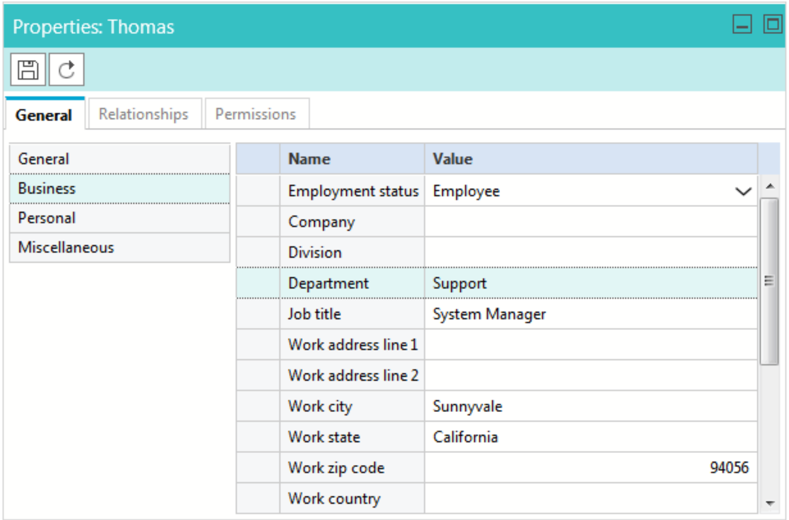


Name	Value
Title	
First name	
Middle name	
Last name	
Suffix	
User name *	
Password	
User status	Enabled
Screen name	
Peripheral	

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**

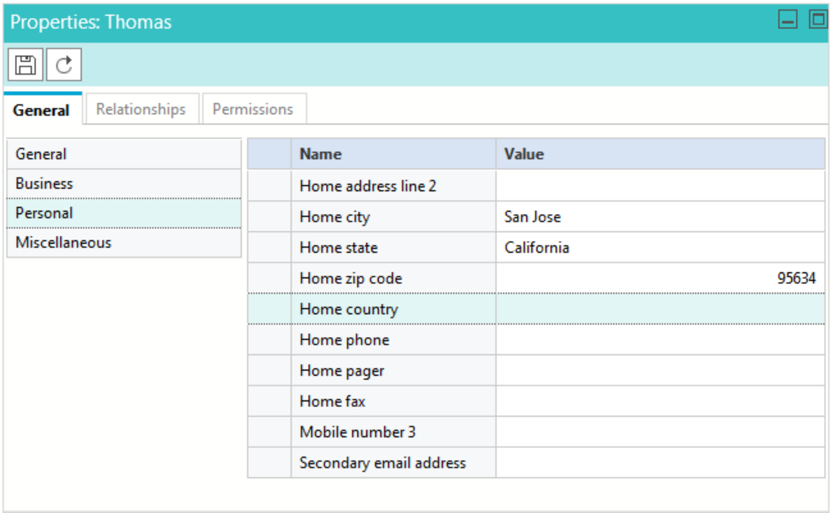


Name	Value
Employment status	Employee
Company	
Division	
Department	Support
Job title	System Manager
Work address line 1	
Work address line 2	
Work city	Sunnyvale
Work state	California
Work zip code	94056
Work country	

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**

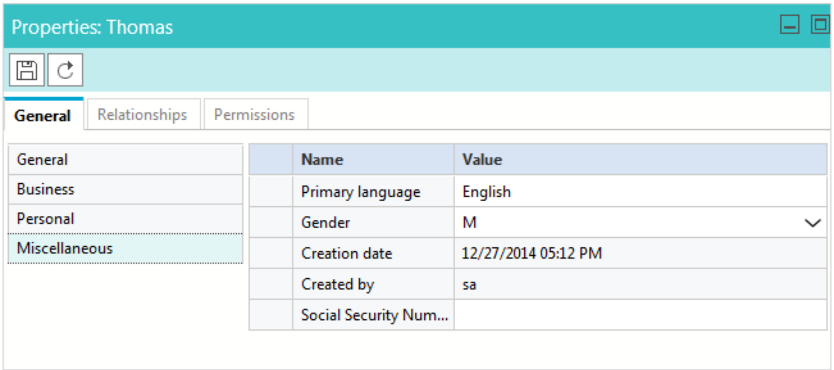


Name	Value
Home address line 2	
Home city	San Jose
Home state	California
Home zip code	95634
Home country	
Home phone	
Home pager	
Home fax	
Mobile number 3	
Secondary email address	

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**



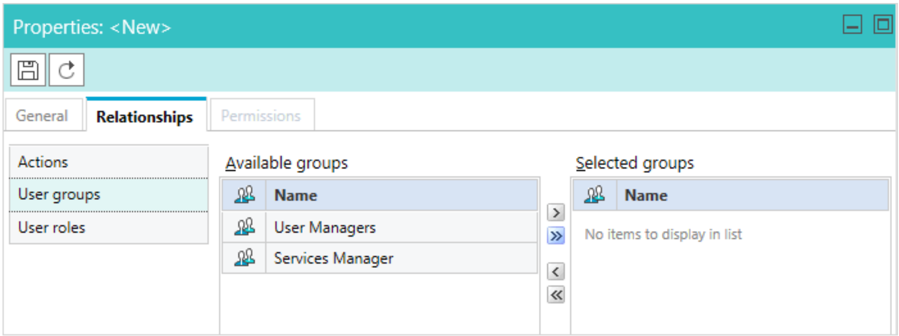
Name	Value
Primary language	English
Gender	M
Creation date	12/27/2014 05:12 PM
Created by	sa
Social Security Num...	

Set miscellaneous properties

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

a. Go to the User groups section and select the user group to which you want to add the user. If you have not created any user groups yet, you can create them and add the users later. For more details, see "Creating User Groups in System Partition" on page 167. Although it is optional to manage users through user groups, we highly recommend that you use groups as it makes user management easier.

When a user is added to a group, he is automatically assigned the roles and actions of the group. You can also choose to assign actions and roles to users individually; however, it is not recommended.



Available groups

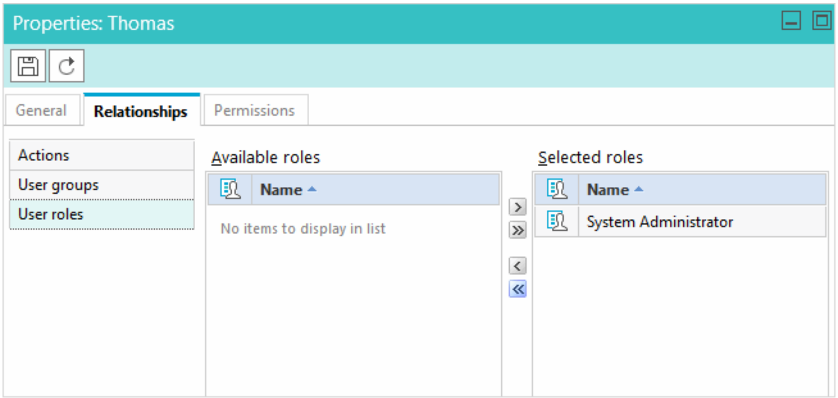
Name
User Managers
Services Manager

Selected groups

Name
No items to display in list

Select user groups

b. 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.



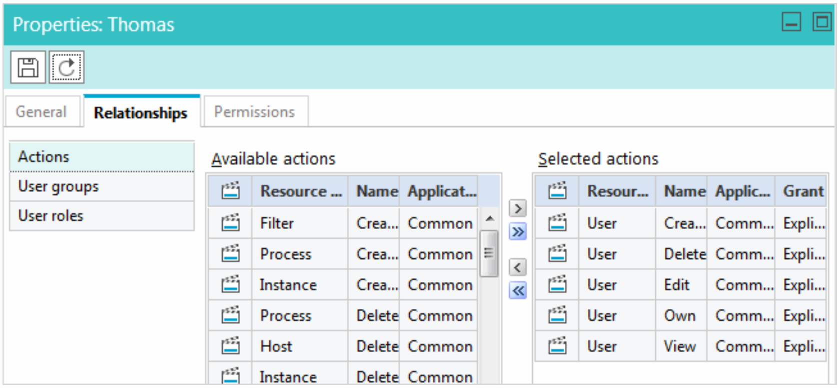
Name
No items to display in list

Name
System Administrator

Select user roles

c. 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 create a user role, with the actions, and assign the role to the user. This makes user management easier. For more details on creating user roles, see "Creating User Roles" on page 162.



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

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

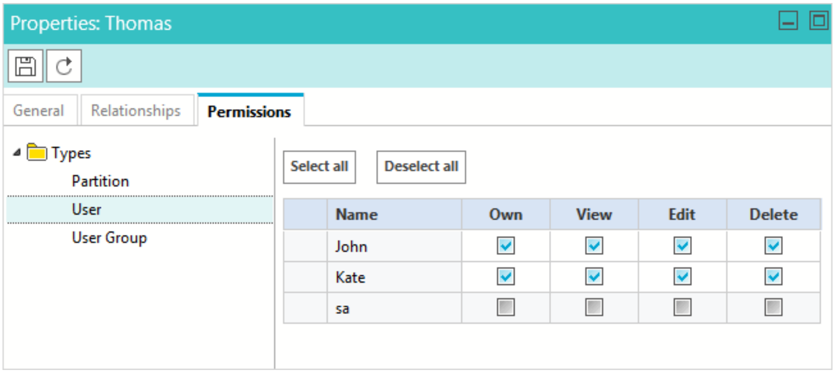
Select actions

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

If you have added a user to a user group, and the user group has permissions on various objects, then that permissions show selected and disabled. If you are using user groups for user management, you should assign permissions to user groups, and not to individual users.



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:

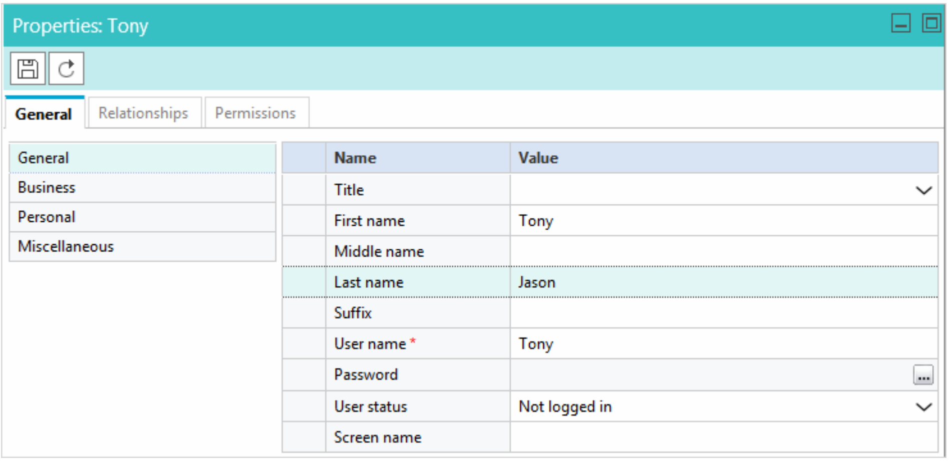
   a. In the General section, provide the following details:

   - **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.
   - **User status**: Select the status of the user. By default the new user's status is **Enabled**. Once the user is saved, the following four options are available: Enabled, Disabled, Logged in, and Not logged in. For more information, see "Changing User Status" on page 194.

   The following fields are optional.

   - **Title**
   - **First name**
   - **Middle name**
   - **Last name**
   - **Suffix**

- **Screen name:** This field is not in use.

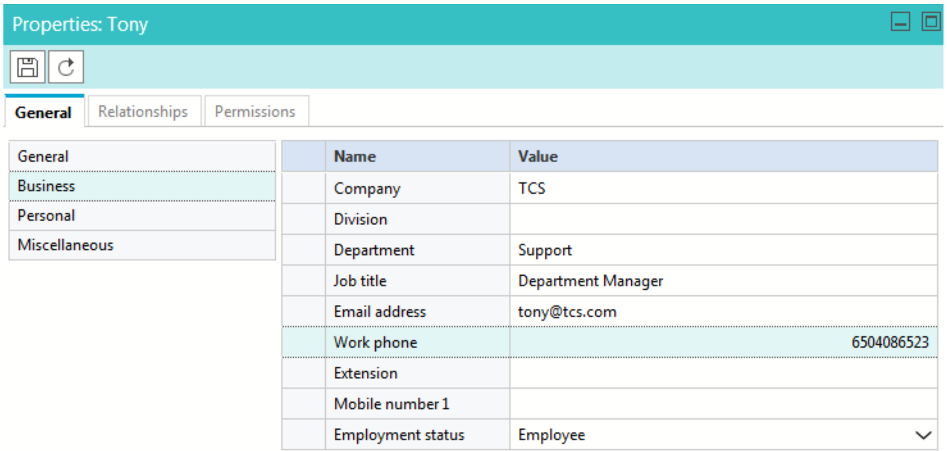


Name	Value
Title	
First name	Tony
Middle name	
Last name	Jason
Suffix	
User name *	Tony
Password	
User status	Not logged in
Screen name	

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.



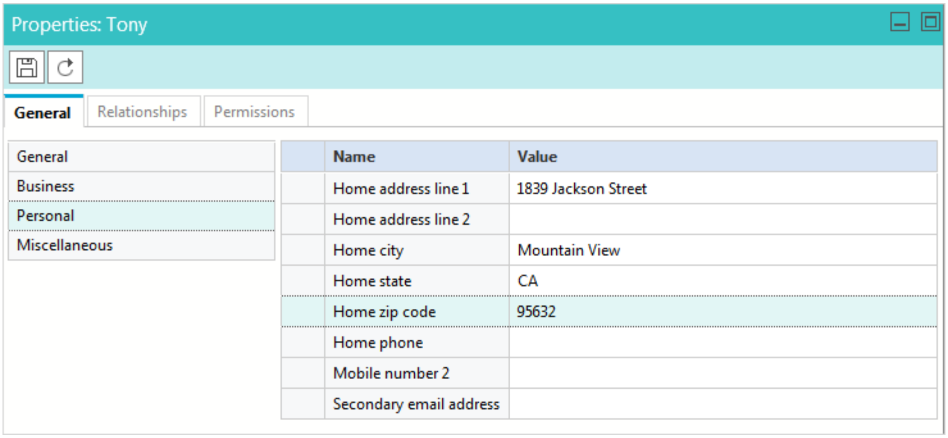
Name	Value
Company	TCS
Division	
Department	Support
Job title	Department Manager
Email address	tony@tcs.com
Work phone	6504086523
Extension	
Mobile number 1	
Employment status	Employee

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**

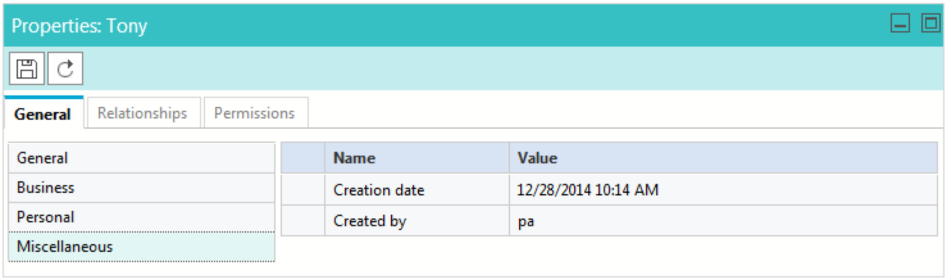


Name	Value
Home address line 1	1839 Jackson Street
Home address line 2	
Home city	Mountain View
Home state	CA
Home zip code	95632
Home phone	
Mobile number 2	
Secondary email address	

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.



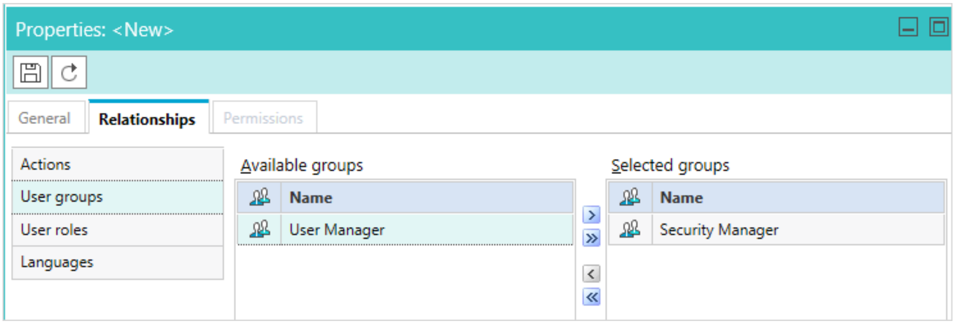
Name	Value
Creation date	12/28/2014 10:14 AM
Created by	pa

View miscellaneous properties

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

a. Go to the User groups section and select the user group to which you want to add the user. If you have not created any user groups yet, you can create them and add the users later. For more details, see "Creating User Groups in Business Partition" on page 170. Although it is optional to manage users through user groups, we highly recommend that you use groups as it makes user management easier.

When a user is added to a group, he is automatically assigned the roles and actions of the group. You can also choose to assign actions and roles to users individually, however, it is not recommended.



Available groups

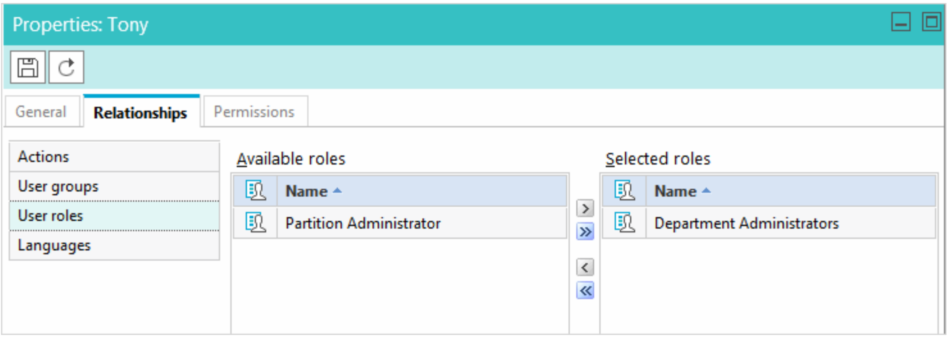
Name
User Manager

Selected groups

Name
Security Manager

Select user groups

b. 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

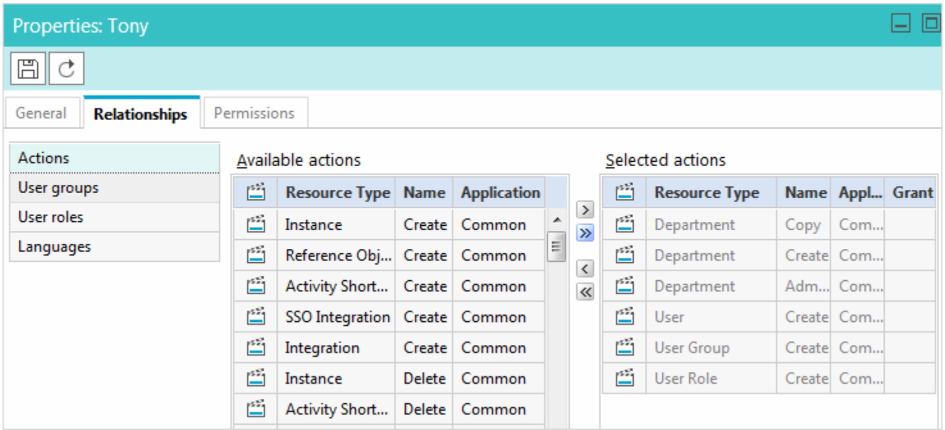
Selected roles

Name ▲
Department Administrators

Select user roles

c. 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 create a user role, with the actions, and assign the role to the user. This makes user management easier. For more details on creating user roles, see "Creating User Roles" on page 162.



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

d. 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

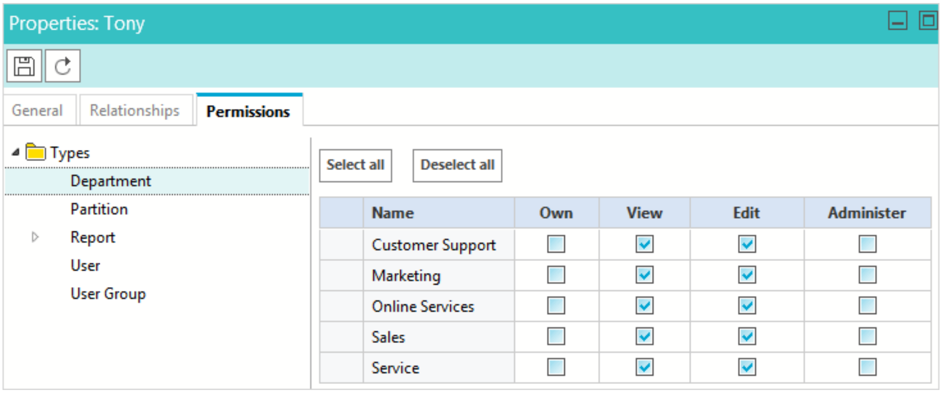
   ○ **Partition:** Own, View, Edit, Administer

   ○ **Report:** View, Run, Edit, Delete, Schedule

   ○ **User:** Own, View, Edit, Delete

   ○ **User group:** Own, View, Edit, Delete, Own, View Edit, Delete

   If you have added a user to a user group, and the user group has permissions on various objects, then those permissions show selected and disabled. If you are using user groups for user management, you should assign permissions to user groups, and not to individual users.



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

Set permissions

8. Click the **Save** button.

Creating Department Users

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 department user:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> User > Users.**

2. In the List pane toolbar, click the **New** button.

3. In the Properties pane, on the General tab, set the following.

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

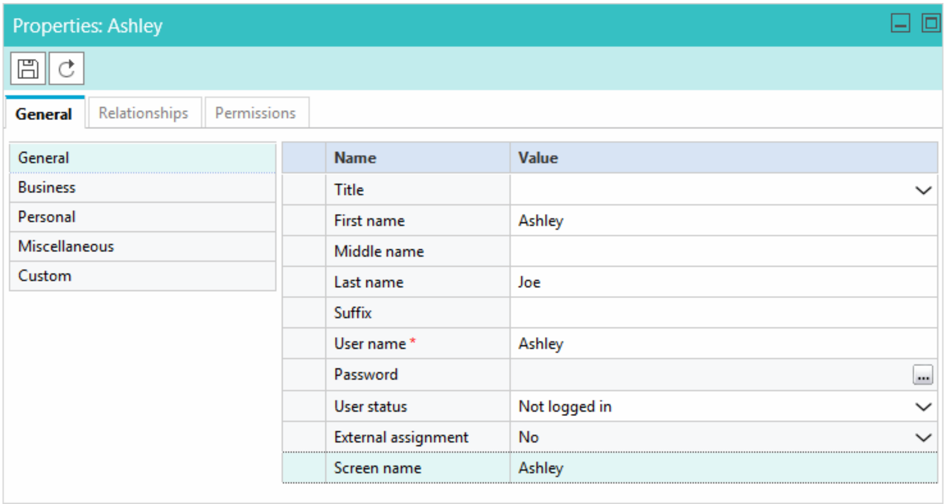
   - **User name**: Type a name for the user. This name is used by the user to log in to the application.
   - **Password**: Type the password. There are important setting related to setting up password. For more details, see "User Account Settings" on page 54.
   - **Screen name:** You need to set the screen name for a user who has the eGain ChatPlus license. This is the name displayed to chat customers in the Chat Customer Console. You can use the same

screen name for more than one user in the system. Do not change the screen name of an agent when the agent is logged in the application and is servicing chats.

- **Authentication type:** By default, Local login is selected and cannot be changed when single sign-on has not been configured. If single sign-on has been enabled, by default, the value is set to SSO. This field can only be configured if single sign-on was configured for a partition and it allows local login for specific users. Select **SSO** to require agents to use their single sign-on authentication links to access the application or **Local login** to allow agents to access the application directly without the SSO authentication links. For more information, see "Agent Single Sign-On" on page 218.
- **User status**: Select the status of the user. By default the new user's status is **Enabled**. Once the user is saved, the following four options are available: Enabled, Disabled, Logged in, and Not logged in. For more information, see "Changing User Status" on page 194.
- **First name:** This field is required
- **Last name:** This field is required

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.



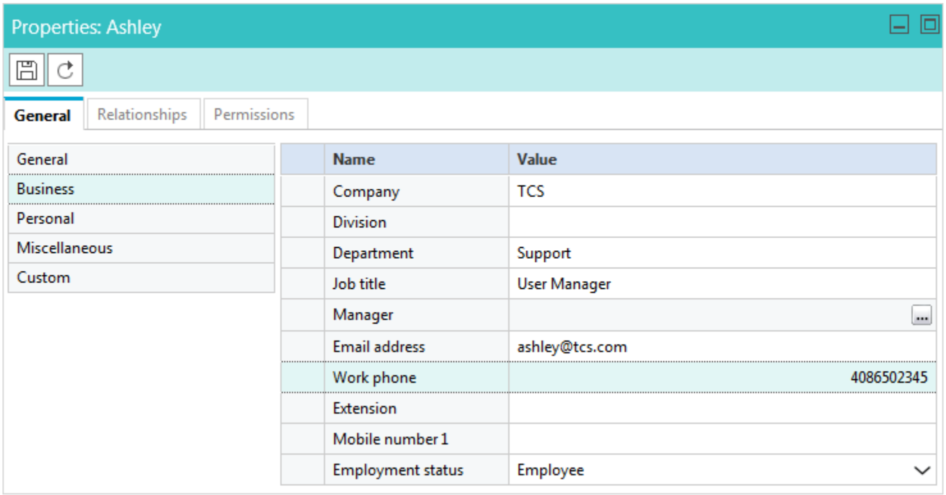
Name	Value
Title	
First name	Ashley
Middle name	
Last name	Joe
Suffix	
User name *	Ashley
Password	
User status	Not logged in
External assignment	No
Screen name	Ashley

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 195.
- **Email address**
- **Work phone**

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

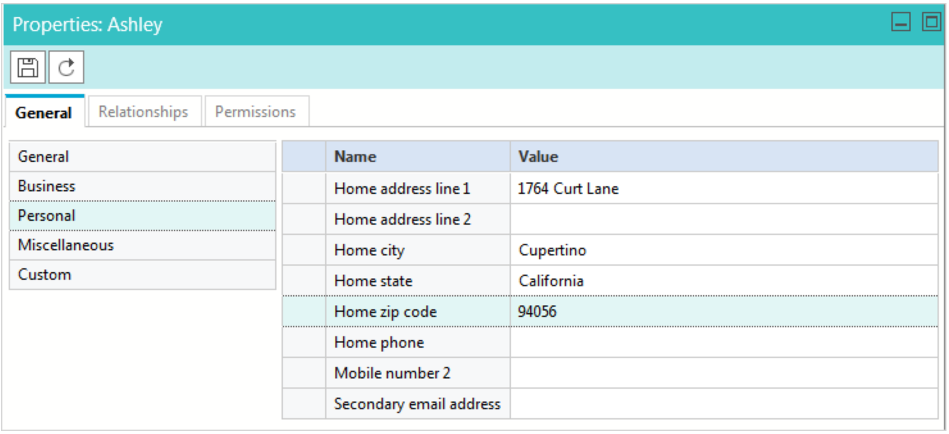


Name	Value
Company	TCS
Division	
Department	Support
Job title	User Manager
Manager	...
Email address	ashley@tcs.com
Work phone	4086502345
Extension	
Mobile number 1	
Employment status	Employee

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**

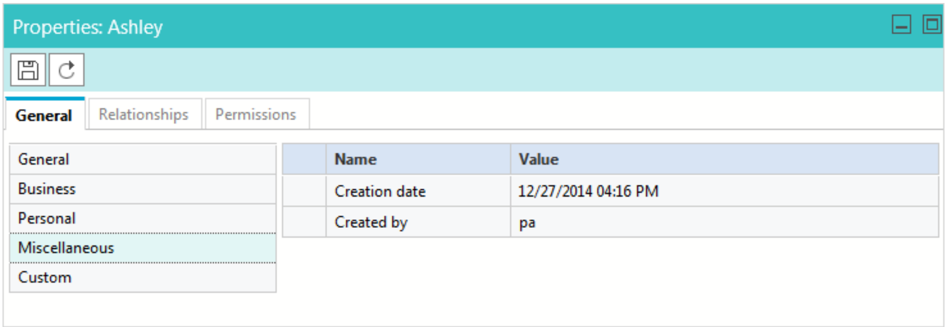


Name	Value
Home address line 1	1764 Curt Lane
Home address line 2	
Home city	Cupertino
Home state	California
Home zip code	94056
Home phone	
Mobile number 2	
Secondary email address	

Set personal properties

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

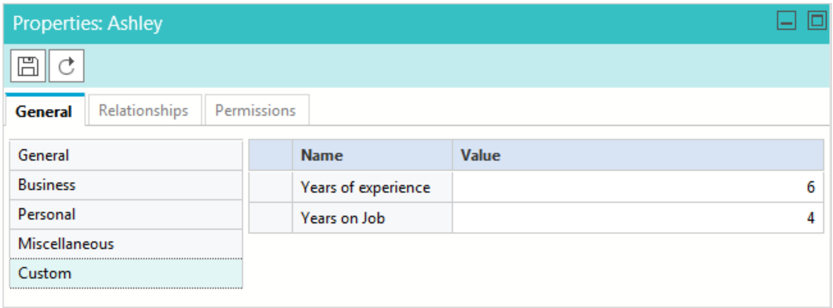
- **Creation date**: This field displays the name of the user who created the user. The value is populated automatically when the user is saved and it cannot be changed.
- **Created by**: This field displays the date and time the user is created. The value is populated automatically when the user is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



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

View miscellaneous properties

e. Finally, go to the Custom section. This displays the list of custom attributes created for users. You can add these custom attributes from the Tools Console. First, you need to create the custom attribute from **Tools > Partition:** *Partition_Name* **> Business objects > Attributes setting > System > User data.** Then, add the custom attribute to **Administration Console - Users - General - Custom screen** available at, **Tools > Departments >** *Department_Name* **> Business objects > Attributes settings > Screen.** For more details on custom attribute, see *eGain Administrator's Guide to Tools Console.*



Name	Value
Years of experience	6
Years on Job	4

Set custom properties

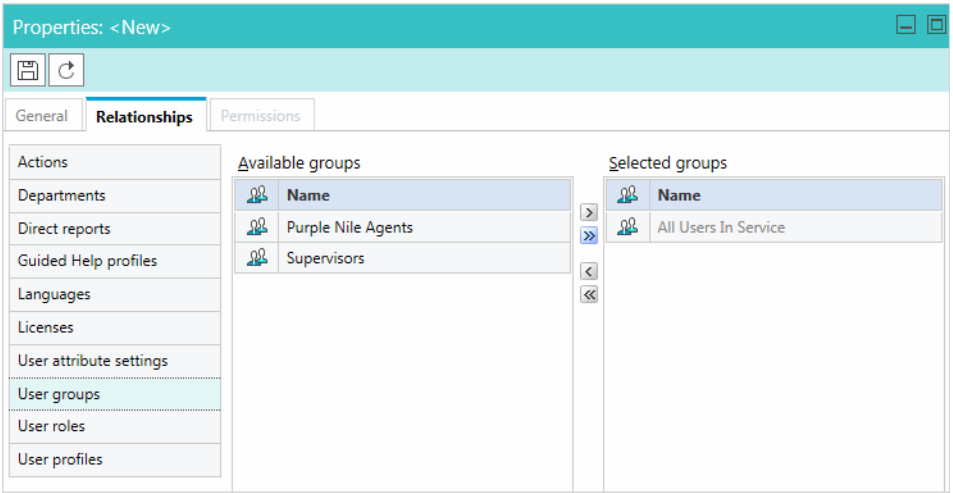
4. Next, go to the Relationships tab, and set the following.

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

      - eGain Advisor Desktop
      - eGain Platform
      - eGain CallTrackPlus
      - eGain ChatPlus
      - eGain CobrowsePlus
      - eGain MailPlus
      - eGain Offers
      - eGain Knowledge+AI

b. Go to the User groups section and select the user group to which you want to add the user. If you have not created any user groups yet, you can create them and add the users later. For more details, see "Creating User Groups in Business Partition" on page 170. Although it is optional to manage users through user groups, we highly recommend that you use groups as it makes user management easier.

When a user is added to a group, he is automatically assigned the roles and actions of the group. You can also choose to assign actions and roles to users individually; however, it is not recommended.

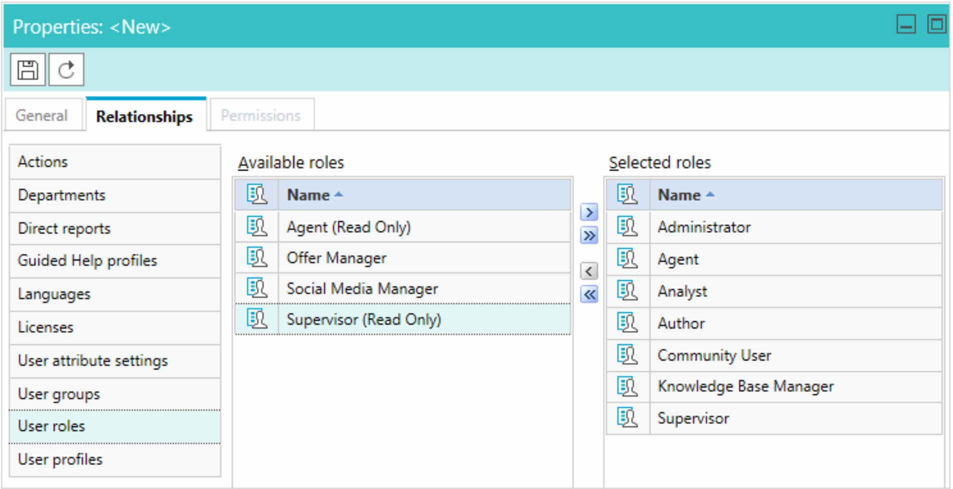


Available groups: Name
Purple Nile Agents
Supervisors

Selected groups: Name
All Users In Service

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.



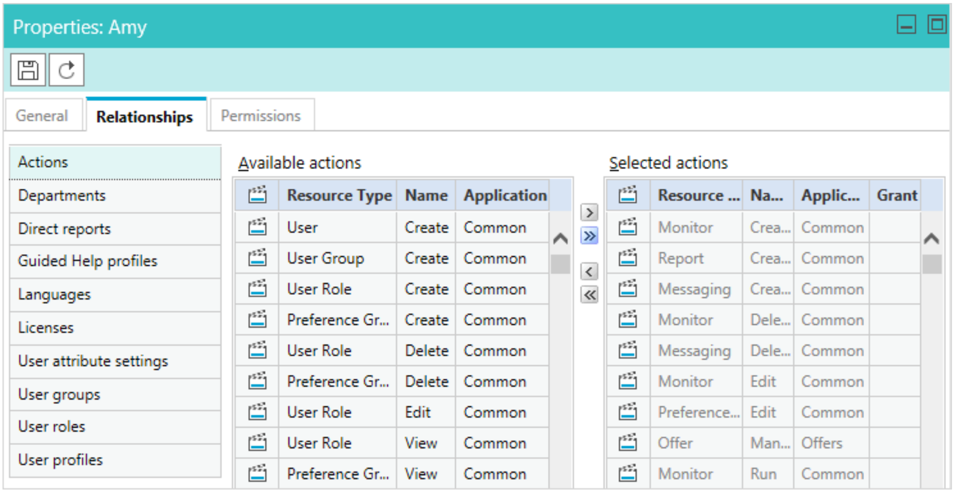
Available roles: Name
Agent (Read Only)
Offer Manager
Social Media Manager
Supervisor (Read Only)

Selected roles: Name
Administrator
Agent
Analyst
Author
Community User
Knowledge Base Manager
Supervisor

Select user roles

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 create a user role, with the actions, and assign the role to the user. This makes user management easier. For more details on creating user roles, see “Creating User Roles” on page 162.



Properties: Amy

General | Relationships | Permissions

- Actions
- Departments
- Direct reports
- Guided Help profiles
- Languages
- Licenses
- User attribute settings
- User groups
- User roles
- User profiles

Available actions

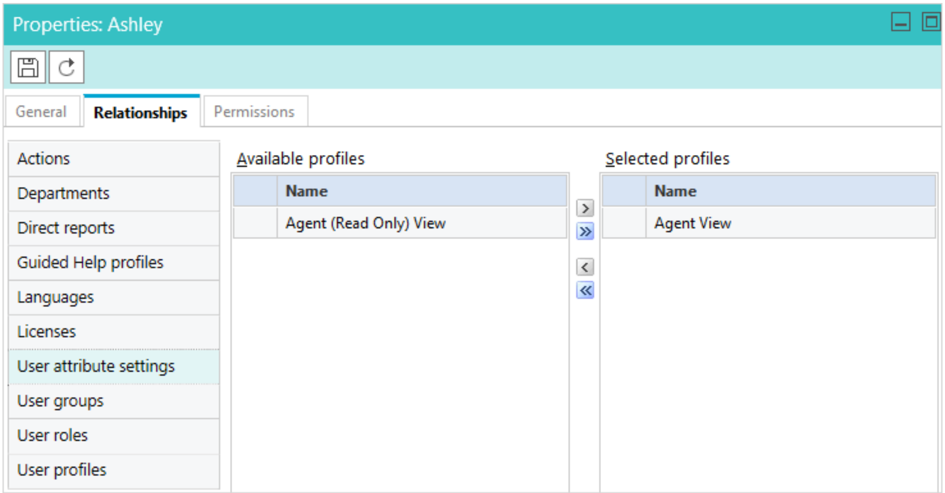
Resource Type	Name	Application
User	Create	Common
User Group	Create	Common
User Role	Create	Common
Preference Gr...	Create	Common
User Role	Delete	Common
Preference Gr...	Delete	Common
User Role	Edit	Common
User Role	View	Common
Preference Gr...	View	Common

Selected actions

Resource ...	Na...	Applic...	Grant
Monitor	Crea...	Common	
Report	Crea...	Common	
Messaging	Crea...	Common	
Monitor	Dele...	Common	
Messaging	Dele...	Common	
Monitor	Edit	Common	
Preference...	Edit	Common	
Offer	Man...	Offers	
Monitor	Run	Common	

Select actions

e. Next, go the User attribute settings tab and select a user attribute setting for the group. This lets you control the level of access a user has in the system. For more details on user attribute settings, see *eGain Administrator’s Guide to Tools Console.*



Properties: Ashley

General | Relationships | Permissions

- Actions
- Departments
- Direct reports
- Guided Help profiles
- Languages
- Licenses
- User attribute settings
- User groups
- User roles
- User profiles

Available profiles

Name
Agent (Read Only) View

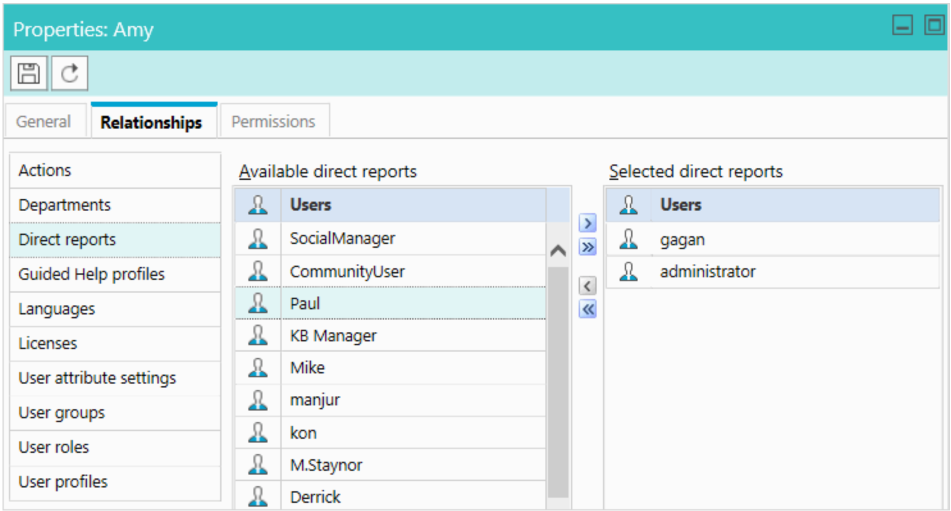
Selected profiles

Name
Agent View

Select user attributes

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

g. 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 195.

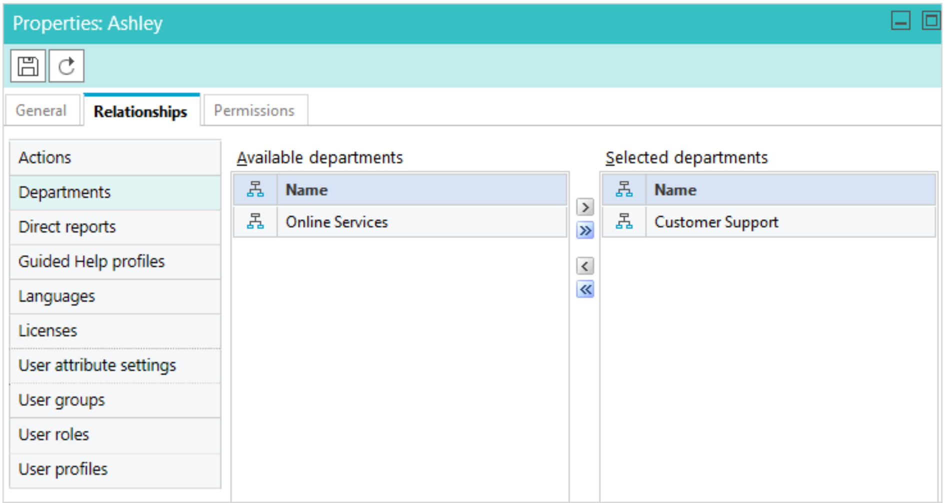


Users
SocialManager
CommunityUser
Paul
KB Manager
Mike
manjur
kon
M.Staynor
Derrick

Users
gagan
administrator

Select users for direct reports

h. Next, in the Departments section you can share the user across departments. For more details, see "Sharing Users with Other Departments" on page 196.



Name
Online Services

Name
Customer Support

Select departments

i. Next, in the User search profiles section you can select the search profiles for the user. For more details, about search profiles, see the *eGain Knowledge Manager's Guide*.

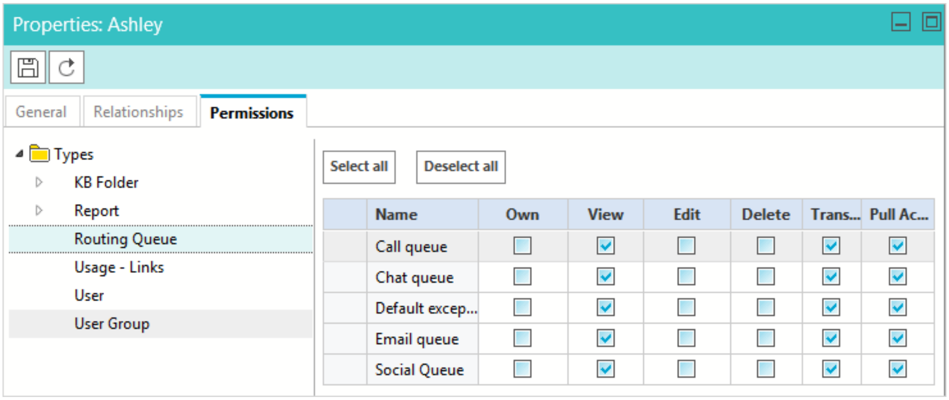
5. Click the **Save** button to enable the various options in the Permissions tab.

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

   - **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:** View, Run, Edit, Delete, Schedule
   - **Routing Queue:** Own, View, Edit, Delete, Transfer activities, Pull activities

- **Usage - Links:** Own, View, Edit, Delete, Execute
- **User:** Own, View, Edit, Delete, Transfer activities, Pull activities
- **User group:** Own, View, Edit, Delete, Transfer activities, Pull activities

If you have added a user to a user group, and the user group has permissions on various objects, then that permission shows selected and disabled. If you are using user groups for user management, you should assign permissions to user groups, and not to individual users.



Name	Own	View	Edit	Delete	Trans...	Pull Ac...
Call queue	□	☑	□	□	☑	☑
Chat queue	□	☑	□	□	☑	☑
Default excep...	□	☑	□	□	☑	☑
Email queue	□	☑	□	□	☑	☑
Social Queue	□	☑	□	□	☑	☑

Set permissions

7. 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.

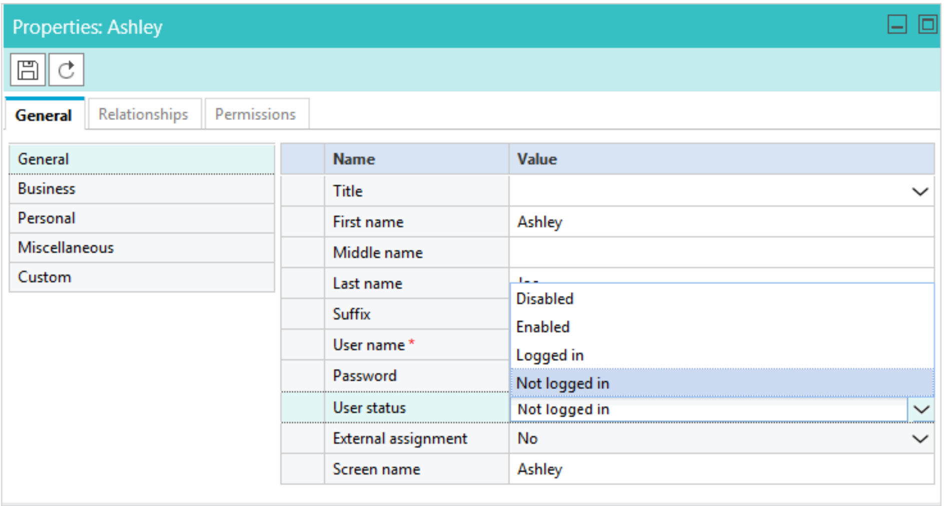
Changing User Status

The user status feature allows you to enable or disable users in the system. It also helps you know which users are logged in to the application. A user can have one of the following status:

- **Enabled**: This status indicates that the user is enabled and can log in to the application.
- **Disabled**: This status indicates that the user is disabled. A disabled user cannot login to the application.
- **Logged in:** This status indicates that the user is logged in to the application.
- **Not logged in:** This status indicates that the user is not logged in to the application.

To change the status of a user:

1. In the Tree pane, browse to the **Users** node. Based on where the user is, do one of the following:
   - If you are in system partition, browse to **Administrator > Partition:** *Context_Root_Name* **> User > Users.**
   - If you are in business partition, browse to **Administrator > Partition:** *Partition_Name* **> User > Users.**
   - If you are in a department, browse to **Administration > Departments >** *Department_Name* **> User > Users.**
2. In the List pane, select the user whose status you want to change.
3. In the Properties pane, go to the General tab.
4. Go to the General section, and in the User status field select the **Enabled** option to enable the user, or select the **Disabled** option to disable the user. If a user is logged in to the application and you want to end his session, select the **Not logged in** option. The user is then logged out and displayed a message saying that their session has ended.



Name	Value
Title	
First name	Ashley
Middle name	
Last name	
Suffix	
User name *	
Password	
User status	Not logged in
External assignment	No
Screen name	Ashley

Select status

5. Click the **Save** button.

Assigning Manager of Users

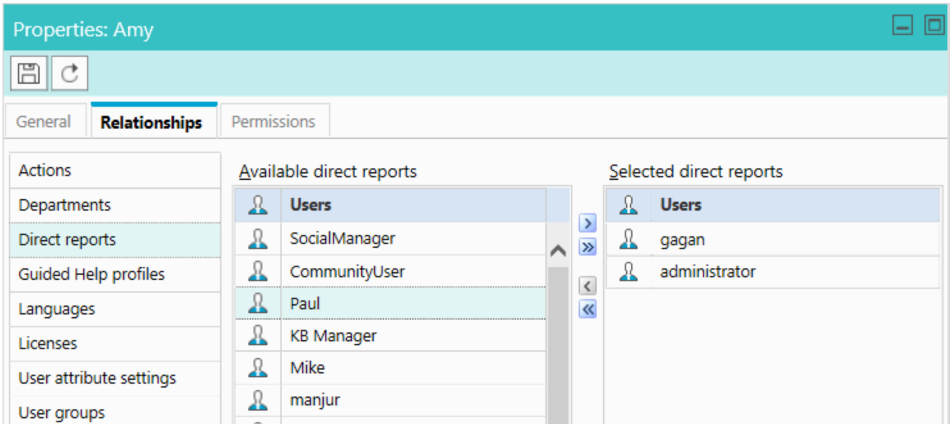
A manager can monitor the activities and cases assigned to agents from the Advisor Desktop. A manager has a My Team folder in his Inbox tree, in the Advisor Desktop, in which all the users who report to the user are listed. The manager has a read only view of the activities and cases assigned to the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

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

You cannot assign managers of user groups.

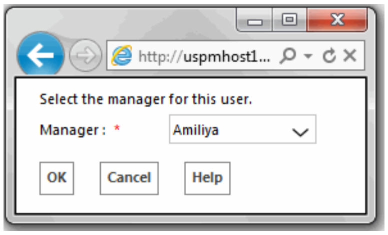
To assign a manager of a user:

1. In the 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.

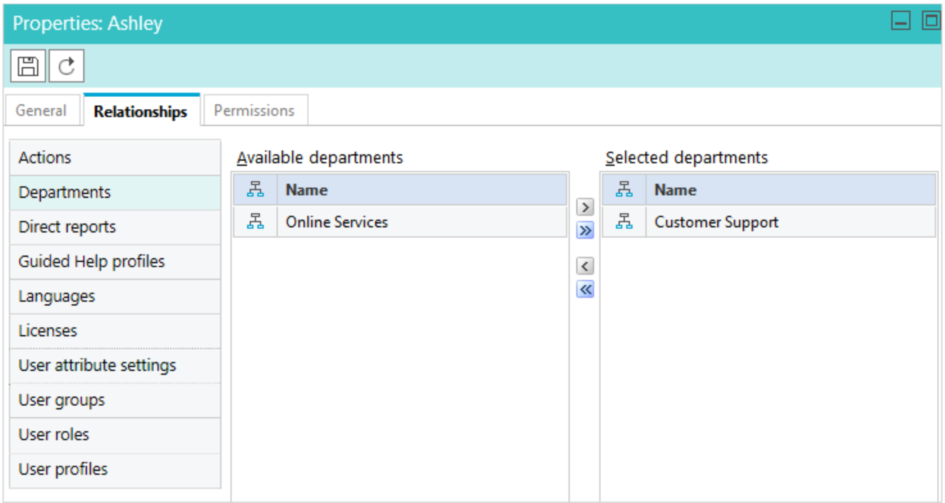
Sharing Users with Other Departments

To be able to share users among departments, first the departments should be shared with each other. Only partition administrators can share departments. For more details see, "Sharing Department Resources" on page 264.

Shared users show as foreign users in the other departments.

To share a user with other departments:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> User > Users**.
2. In the List pane, select a user.
3. In the Properties pane, on the Relationships tab, go to the Departments section and select a department from the list. If you do not see any departments in the list, contact your partition administrator.



Available departments
Name
Online Services

Selected departments
Name
Customer Support

Select department

4. Click the **Save** button.

4

Data Masking

About Data Masking

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

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

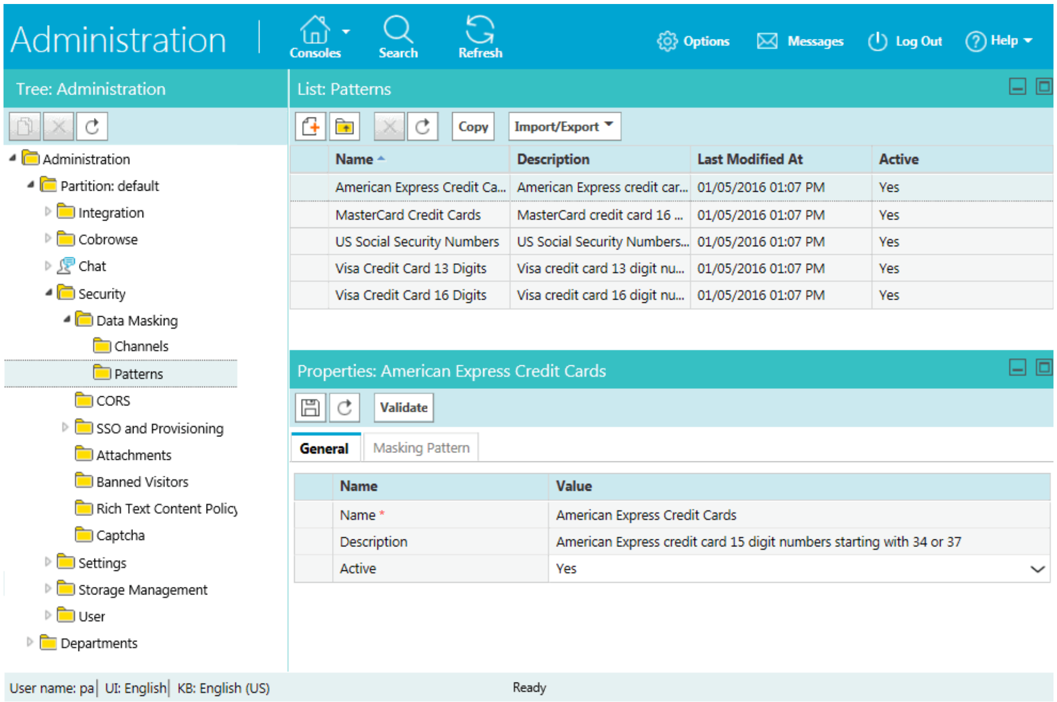
Data masking is available for emails and chats.

About Patterns

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

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

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



Name	Description	Last Modified At	Active
American Express Credit Ca...	American Express credit car...	01/05/2016 01:07 PM	Yes
MasterCard Credit Cards	MasterCard credit card 16 ...	01/05/2016 01:07 PM	Yes
US Social Security Numbers	US Social Security Numbers...	01/05/2016 01:07 PM	Yes
Visa Credit Card 13 Digits	Visa credit card 13 digit nu...	01/05/2016 01:07 PM	Yes
Visa Credit Card 16 Digits	Visa credit card 16 digit nu...	01/05/2016 01:07 PM	Yes

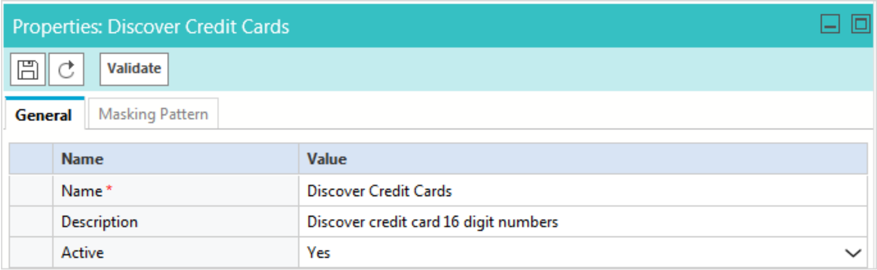
Name	Value
Name *	American Express Credit Cards
Description	American Express credit card 15 digit numbers starting with 34 or 37
Active	Yes

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.

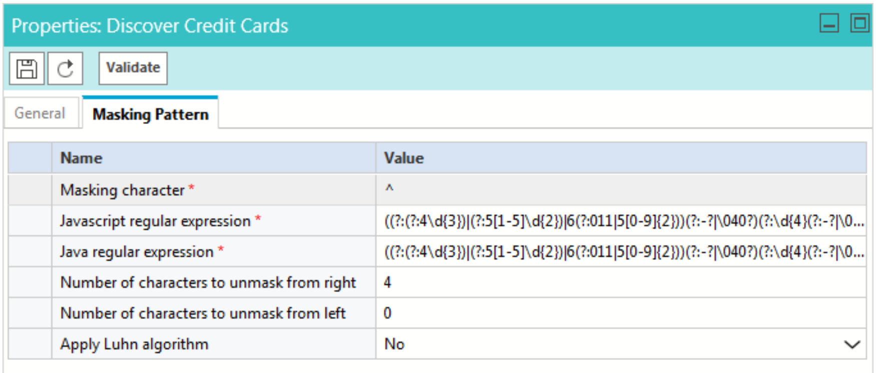


Name	Value
Name *	Discover Credit Cards
Description	Discover credit card 16 digit numbers
Active	Yes

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 shows as *****3545
   - **Number of characters to unmask from left:** Provide the number of characters, from the left, that should be ignored while masking. For example, if you are masking a 10 digit account number and you do not want to mask the first 4 numbers of the account number, the account number shows as 8765******

- **Apply Luhn Algorithm:** Select **Yes** to apply the Luhn algorithms to credit card numbers.



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

Configure the pattern properties

5. Click the **Save** button.

Creating Patterns in XML File

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

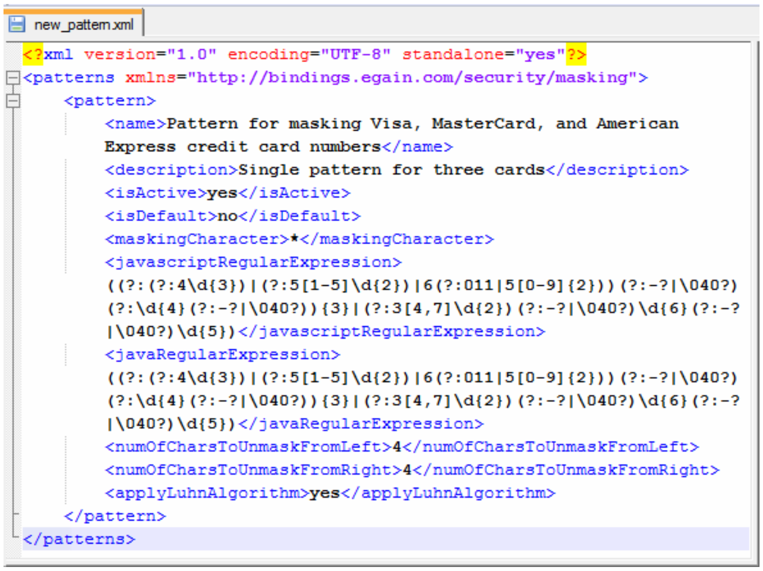
- Only XML files can be used to import patterns.
- You can name the file anything you want.
- Elements should be defined in the order specified in the pattern file exported from the application.
- Elements and values of elements in the XML file are case sensitive.
- For user created patterns, the **isDefault**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

The following table lists the names of the properties as they appear in the file and on the UI. For the description of each field, see "Creating Patterns" on page 199.

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

Name on the UI	Name in the file
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:

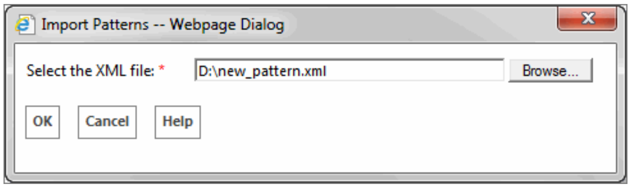
1. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security> Data Masking > Patterns.**
2. In the List pane toolbar, from the **Import/Export** button select the **Export Patterns** option.
3. A prompt appears to save the patterns XML file.

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

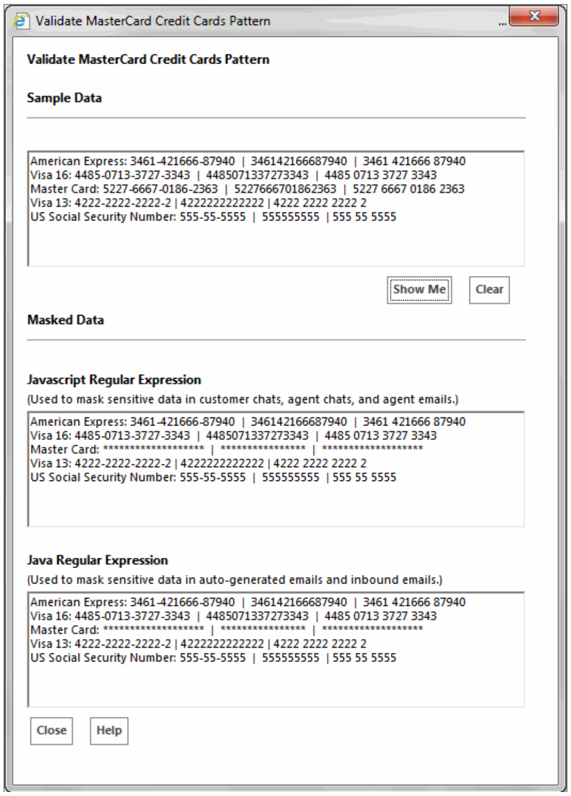
Validating Individual Patterns

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, the Javascript regular expression and Java regular expression applied to the sample data are visible. All the settings configured in the Masking Pattern tab will be applied to the sample data.

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



Validate 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

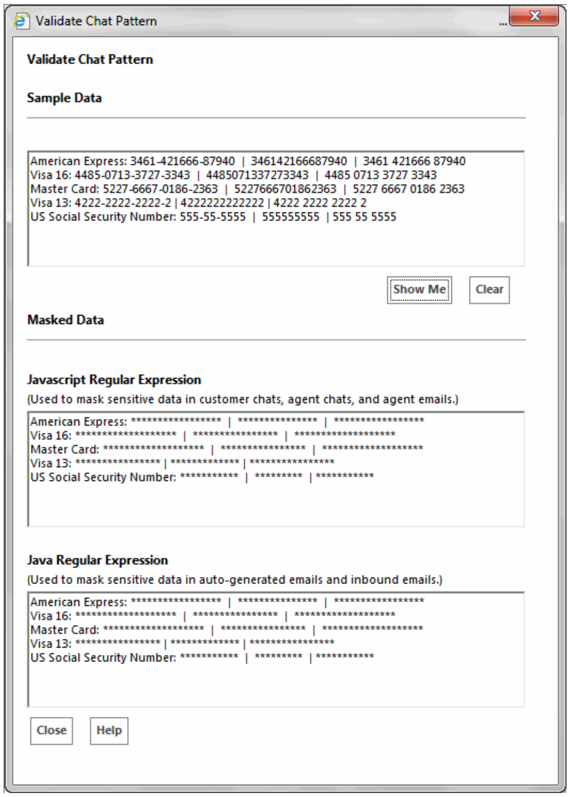
In addition to validating individual patterns, you can validate the patterns selected for a channel and make sure that they work properly as a group and the order of the selected pattens is correct.

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, all the selected patterns applied to the sample data are visible.

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 necessary actions can perform these tasks:

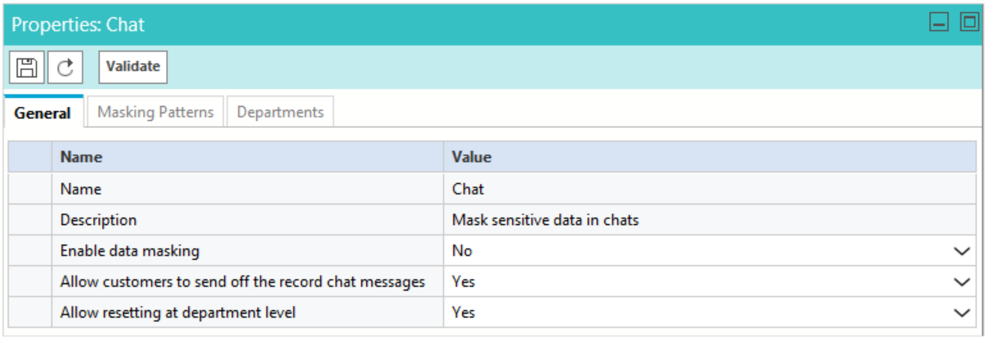
- **Manage Application Security:** Allows the administrator to view the patterns applied to channels and to apply patterns to channels.
- **View Application Security:** Gives a read-only view of the patterns applied to channels. Users with this action cannot change any configurations.

What can the partition administrator do?

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

To apply patterns to the chat channel:

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

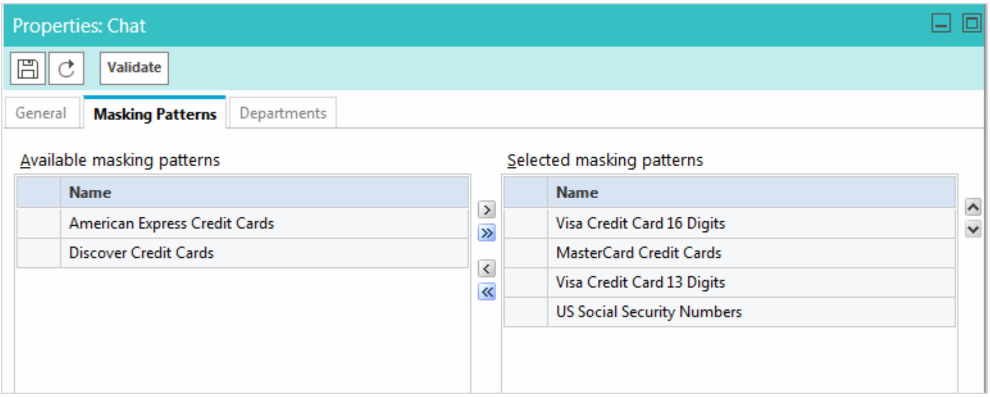


Name	Value
Name	Chat
Description	Mask sensitive data in chats
Enable data masking	No
Allow customers to send off the record chat messages	Yes
Allow resetting at department level	Yes

Set the general properties

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

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



Available masking patterns

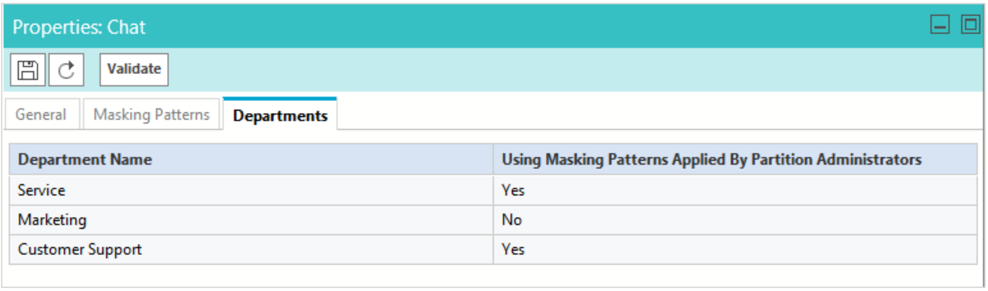
Name
American Express Credit Cards
Discover Credit Cards

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 204.

At the Department Level

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

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

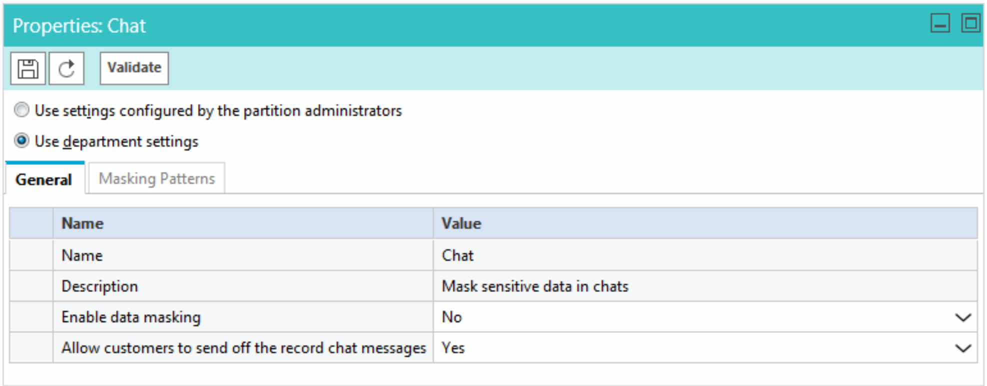
- **View Department Security:** Gives a read-only view of the patterns applied to channels. Users with this action cannot change any configurations.

How much control do department administrators get?

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

To apply patterns to the chat channel:

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

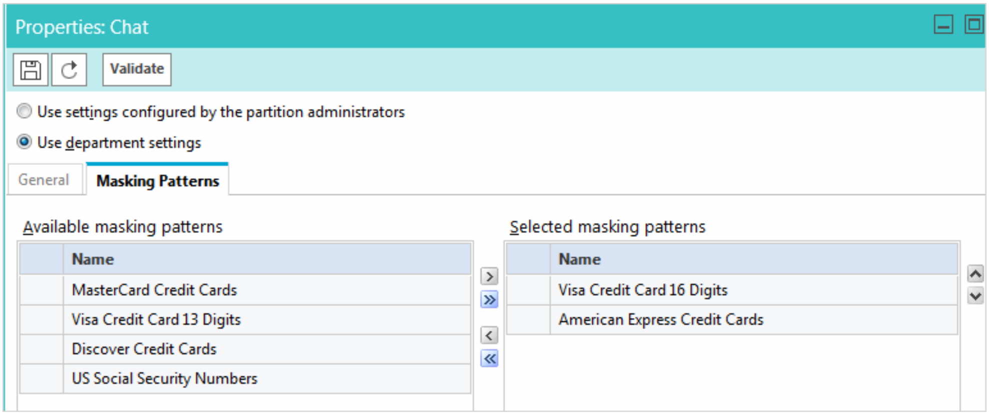


○ Use settings configured by the partition administrators
● Use department settings

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 204.

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.

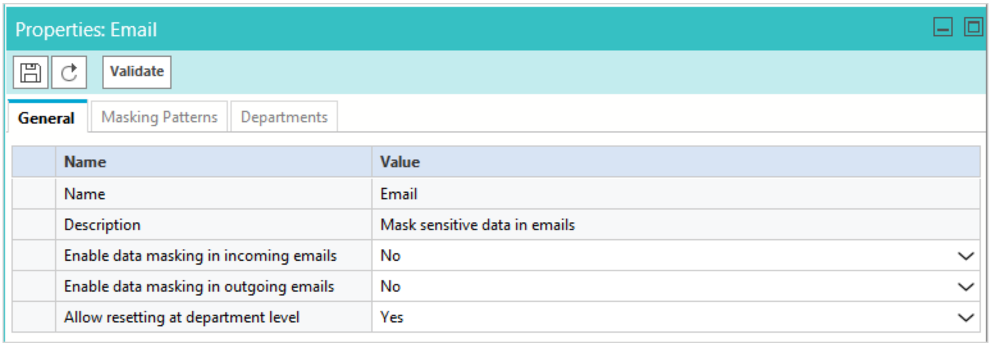
What can the partition administrator do?

- 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**.

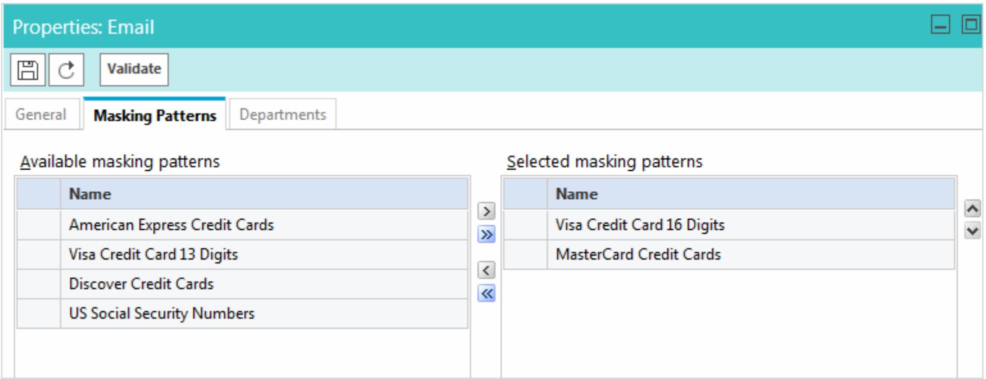


Name	Value
Name	Email
Description	Mask sensitive data in emails
Enable data masking in incoming emails	No
Enable data masking in outgoing emails	No
Allow resetting at department level	Yes

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

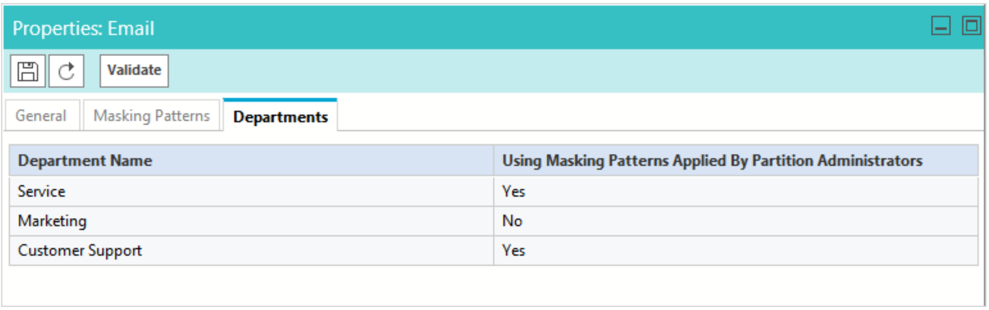
Name
American Express Credit Cards
Visa Credit Card 13 Digits
Discover Credit Cards
US Social Security Numbers

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 204.

At the Department Level

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

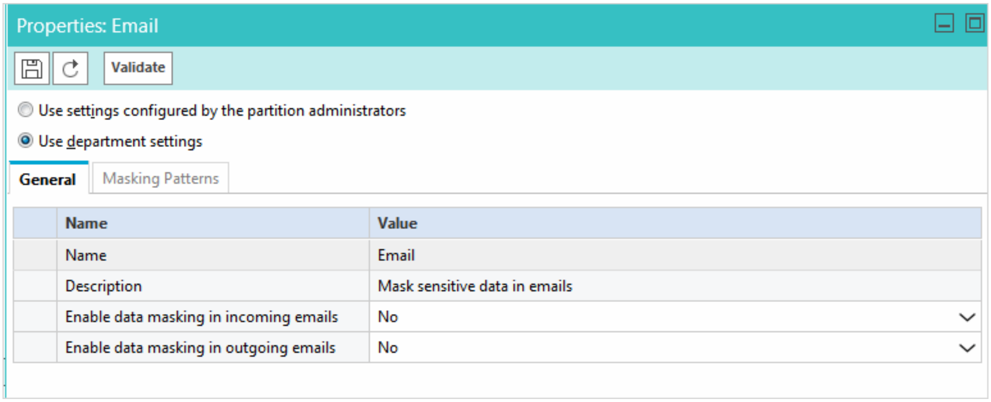
- **Manage Department Security:** Allows you to view the patterns applied to channels and to apply patterns to channels.
- **View Department Security:** Gives a read-only view of the patterns applied to channels. Users with this action cannot change any configurations.

How much control do department administrators get?

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

To apply patterns to the email channel:

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

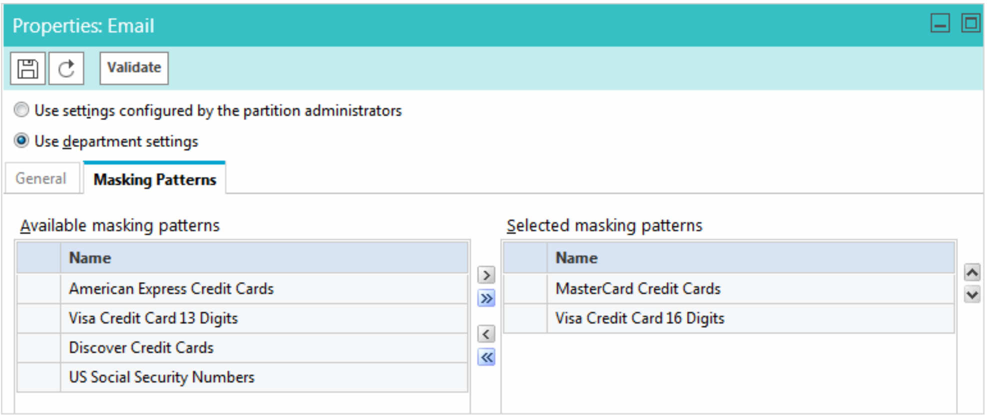


○ Use settings configured by the partition administrators
● Use department settings

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.



○ Use settings configured by the partition administrators

● Use department settings

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 204.

Masking Content of Completed Activities

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

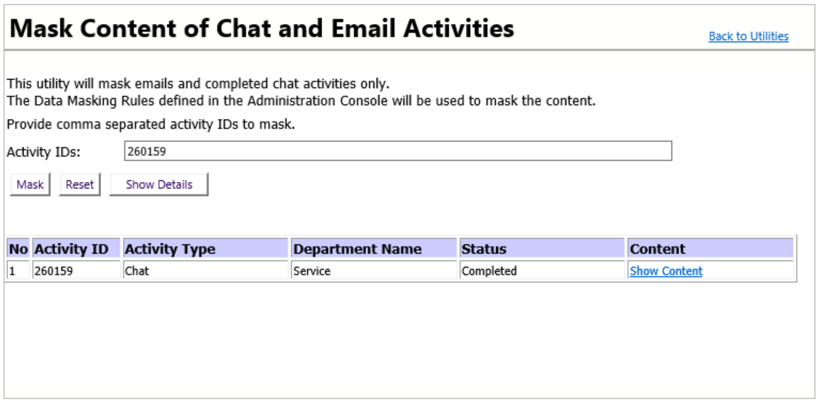
> Important: **This utility can only be run by a department administrator.**

To mask content of completed activities:

1. While signed in to the Tools Console as a department administrator, click the **Utilities** button.

2. In the Utilities window, in the Mask Content of Chat and Email Activities field, click the **Go** button.

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



Mask Content of Chat and Email Activities

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

Provide comma separated activity IDs to mask.

Activity IDs: 260159

No	Activity ID	Activity Type	Department Name	Status	Content
1	260159	Chat	Service	Completed	Show Content

Use the Show Details button to search for activities

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

5 Cross-Origin Resource Sharing

About Cross-Origin Resource Sharing

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

You need to configure CORS when you are invoking eGain Rest API from a web page that is in a domain which is different than the eGain application domain. For example, the eGain application is in Company.com domain and the website is in customer.com domain, you will need to configure CORS in order to allow requests from the web pages in customer.com domain to the eGain APIs in the company.com domain.

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

CORS also needs to be configured for cobrowsing external websites when the landing page and the eGain application are in separate domains. For details about external cobrowing, see *eGain Administrator's Guide to Chat and Collaboration Resources.*

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

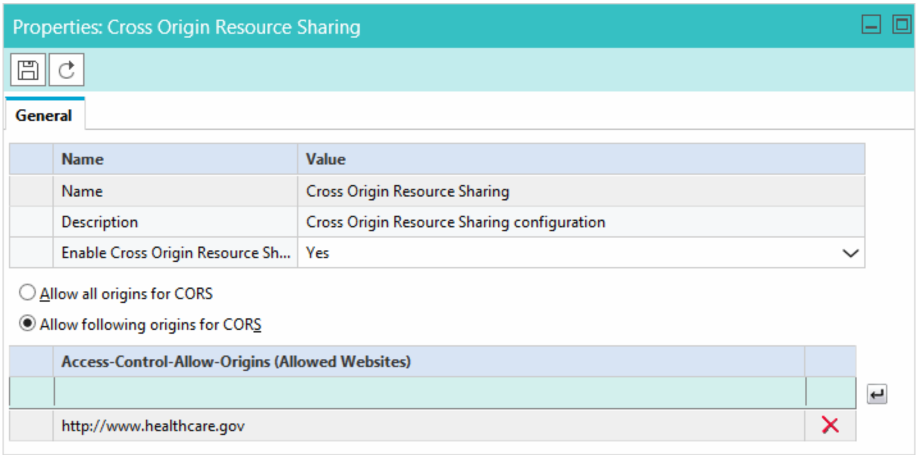
- **Manage Application Security:** Allows you to enable or disable CORS and configure the list of allowed websites for CORS.
- **View Application Security:** Gives a read-only view of the CORS settings. Users with this action cannot change any configurations.

Enabling Cross-Origin Resource Sharing

To enable cross-origin resource sharing:

1. In the Tree pane, browse to **Administration** > **Partition:** *Partition_Name* > **Security**> **CORS**.
2. In the List pane, select Cross Origin Resource Sharing.
3. In the Properties pane, set the following:
   - **Enable Cross Origin Resource Sharing:** Select **Yes** to enable CORS. By default, CORS is disabled in the application.
   - Select **Allow all origins for CORS** or select **Allow following origins for CORS** and provide the list of allowed websites for CORS. The URL must contain a protocol, `http` or `https` (in lower case),

followed by the domain name or IP address. The domain name can contain only numbers, alphabets, dot (.), and hyphen (-). For example, `http://company-name.com` or `https://10.10.20.30`


Properties: Cross Origin Resource Sharing

General

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

○ Allow all origins for CORS

● Allow following origins for CORS

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

Enable CORS

4. Click the **Save** button.

6 Agent Single Sign-On

About Single Sign-On (SSO)

Organizations and their staff often must use multiple applications that require authentication in order to perform their necessary tasks. However, each application typically has its own authentication mechanism. This creates extra work for the administration of users if they must be created and maintained in each system. It is also inconvenient to the end user as they must remember login credentials for each system.

Single sign-on (SSO) is a feature that allows users to use the same credentials to access their applications without having to needlessly go through the individual authentication process for every application. SSO can be enabled on any system that uses the following:

- Siteminder (page 219)
- LDAP (Lightweight Directory Access Protocol) (page 221)
- SAML 1.1 (Security Assertion Markup Language) (page 222)
- SAML 2.0 (page 223)

Single sign-on also can be configured for customers to use specific services of the application. Customers who are already recognized on the company website can use a SSO-enabled entry point to chat with a customer without having to provide redundant information. Customers can also access secure message centers, which act as private mail inboxes in which businesses can share sensitive information with their customers without the risk of compromising security. For information on how to configure SSO for customers, see “Customer Single Sign-On” on page 233.

Important things to note about agent Single Sign-On:

- The process of configuring a system for single sign-on must be performed in the Security node at the partition level by a partition user with the following necessary actions: View Application Security and Manage Application Security.
- Once SSO has been configured, all users in the deployment are enabled for SSO.
- For users to log into the consoles, 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 46 for more information.

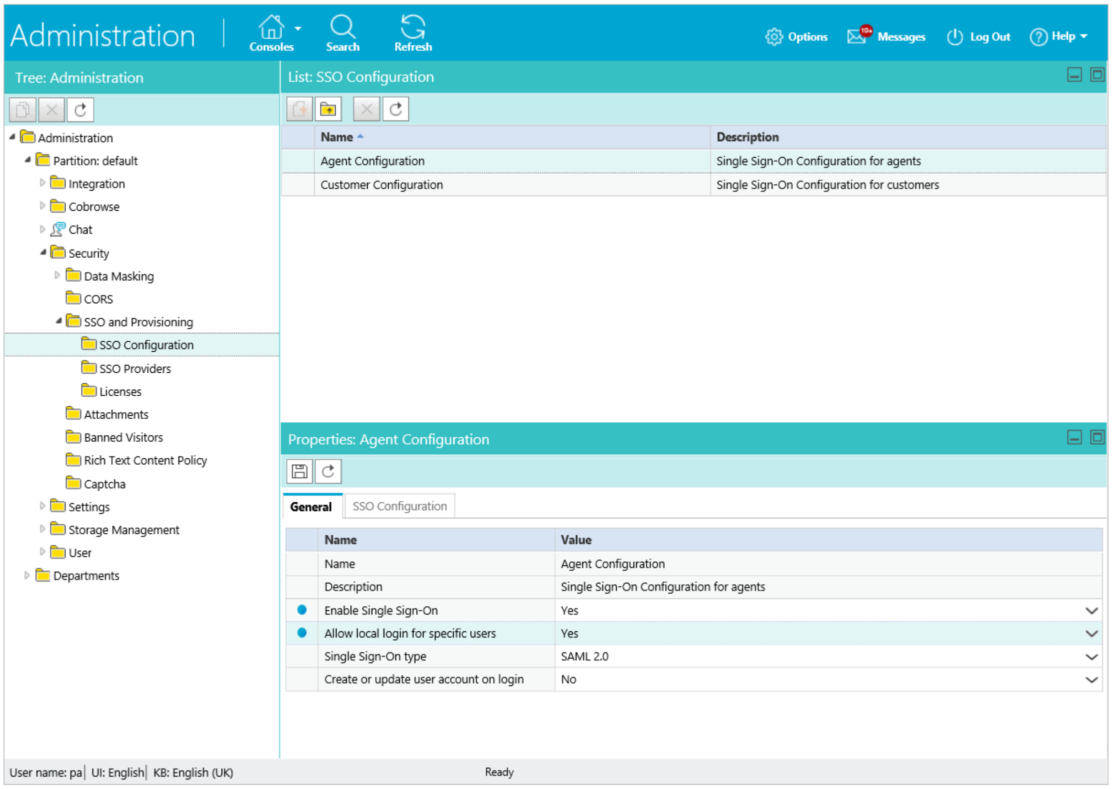
Configuring Single Sign-On (SSO) for Siteminder Systems

Important things to note about Siteminder Single Sign-On:

- Siteminder SSO can only be enabled for on-premise installations. Siteminder SSO is not available for cloud installations.

To configure SSO for Siteminder systems:

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



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

Name	Value
Name	Agent Configuration
Description	Single Sign-On Configuration for agents
Enable Single Sign-On	Yes
Allow local login for specific users	Yes
Single Sign-On type	SAML 2.0
Create or update user account on login	No

Users must have access to Security settings at the partition level

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

3. In the Properties pane, under the General tab, set the following:

   ○ **Enable Single Sign-On:** Select **Yes** to enable SSO.

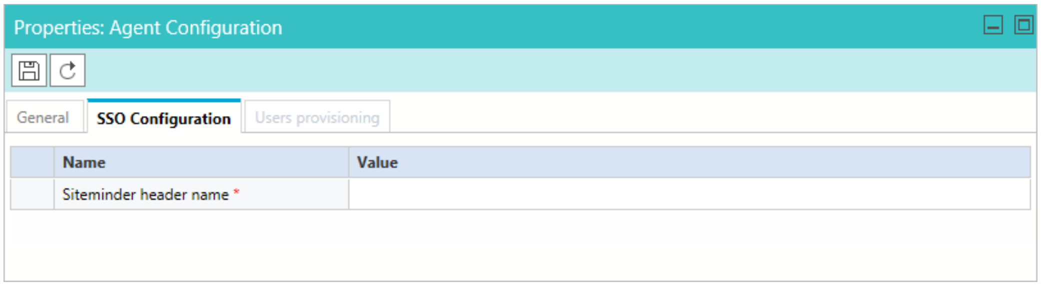
   ○ **Allow local login for specific users:** Select whether users should only be able to log in to the application through the SSO authentication methods or if they can log in to the application locally as well. Select **Yes** to enable local login, **No** to disable. The type of authentication required of a user can be controlled at the user level. See "Creating Department Users" on page 186 for more details.

   ○ **Single Sign-On Type:** Select **Siteminder**.

4. Click the **SSO Configuration** tab.

5. Under the SSO Configuration tab, provide the following:

- **Siteminder header name:** The name of the attribute in the HTTP header which Siteminder uses to pass the user name to the application.



Name	Value
Siteminder header name *	

Provide Siteminder configuration details

6. Click the **Save** button.

Configuring Single Sign-On (SSO) for LDAP Systems

Important things to note about LDAP Single Sign-On:

- A Java Keystore (JKS) file is needed to enable SSL for LDAP configuration. Contact your IT to obtain the Java Keystore file.
- LDAP SSO can only be enabled for on-premise installations. LDAP SSO is not available for cloud installations.

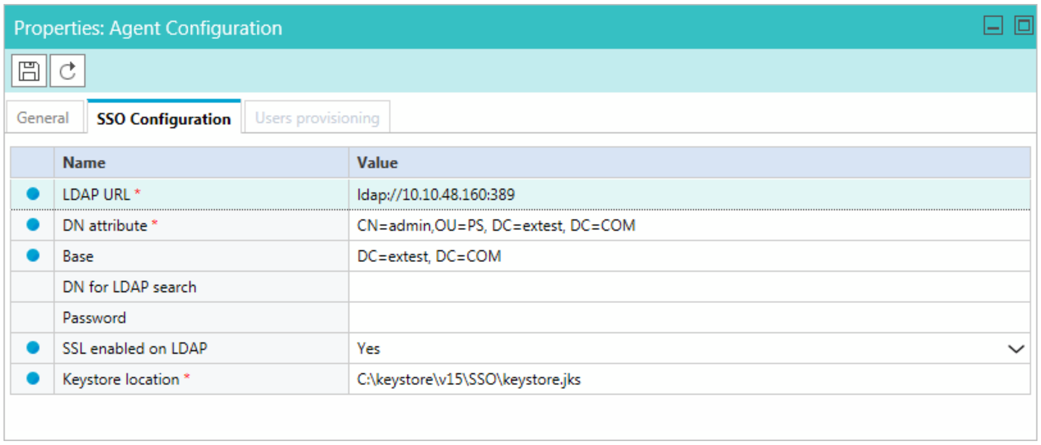
To configure SSO for LDAP systems:

1. In the Tree pane, browse to **Administration** > **Partition:** *Partition_Name* > **Security** > **Single Sign On** > **Configurations**
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.
   - **Allow local login for specific users:** Select whether users should only be able to log in to the application through the SSO authentication methods or if they can log in to the application locally as well. Select **Yes** to enable local login, **No** to disable. The type of authentication required of a user can be controlled at the user level. See “Creating Department Users” on page 186 for more details.
   - **Single Sign-On Type:** Select **LDAP**.
4. Click the **SSO Configuration** tab.
5. Under the SSO Configuration tab, provide the following:
   - **LDAP URL:** The URL of the LDAP server
   - **DN attribute:** The attribute of the DN that contains the user login name. For example, CN.
   - **Base:** The value specified for Base is used by the application as the search base. Search base is the starting location for search in LDAP directory tree. For example, `DC=mycompany, DC=com`.
   - **DN for LDAP search:** Perform one of the following:

    - If your LDAP system does not allow anonymous bind, provide the DN of a user who has search permissions on the LDAP directory tree.
    - If the LDAP server allows anonymous bind, leave this field blank.
  - **Password:** Perform one of the following:
    - If your LDAP system does not allow anonymous bind, provide the password of a user who has search permissions on the LDAP directory tree.
    - If the LDAP server allows anonymous bind, leave this field blank.

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

  - **SSL enabled on LDAP:** If SSL is enabled on the LDAP server, set the value to **Yes**. If not, set the value to **No.**
  - **Keystore location:** The location of the Java KeyStore (JKS), eg: `C:\keystore\v15\SSO\keystore.jks`. This must be provided if SSL is enabled.



	Name	Value
●	LDAP URL *	ldap://10.10.48.160:389
●	DN attribute *	CN=admin,OU=PS, DC=extest, DC=COM
●	Base	DC=extest, DC=COM
	DN for LDAP search	
	Password	
●	SSL enabled on LDAP	Yes
●	Keystore location *	C:\keystore\v15\SSO\keystore.jks

Provide LDAP configuration details

6. Click the **Save** button.

Configuring Single Sign-On (SSO) for SAML 1.1 Systems

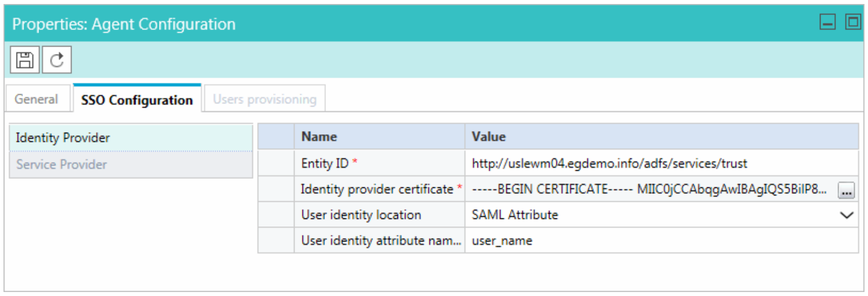
Important things to note about SAML 1.1 Single Sign-On:

- An identity provider certificate is required for SAML 1.1 configurations. Consult your IT department about obtaining the certificate.

To configure SSO for SAML 1.1 systems:

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

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.
   - **Allow local login for specific users:** Select whether users should only be able to log in to the application through the SSO authentication methods or if they can log in to the application locally as well. Select **Yes** to enable local login, **No** to disable. The type of authentication required of a user can be controlled at the user level. See "Creating Department Users" on page 186 for more details.
   - **Single Sign-On Type:** Select **SAML 1.1**.
4. Click the **SSO Configuration** tab.
5. In the **Identity Provider** section, provide the following:
   - **Entity ID:** Entity ID or the issuer.
   - **Identity provider certificate:** The public key certificate. The certificate must start with "`-----BEGIN CERTIFICATE-----`" and end with "`-----END CERTIFICATE-----`"
   - **User identity location:** Select either **SAML Subject Identifier** or **SAML Attribute**.
   - **User identity attribute name:** Applicable only when User ID Location value is an SAML attribute.



Name	Value
Entity ID *	http://uslewm04.egdemo.info/adfs/services/trust
Identity provider certificate *	-----BEGIN CERTIFICATE----- MIIC0jCCAbqgAwIBAgIQS5BiIP8...
User identity location	SAML Attribute
User identity attribute nam...	user_name

Provide SAML configuration details

6. Click the **Save** button.

Configuring Single Sign-On (SSO) for SAML 2.0 Systems

Configuring Single Sign-On for SAML 2.0

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

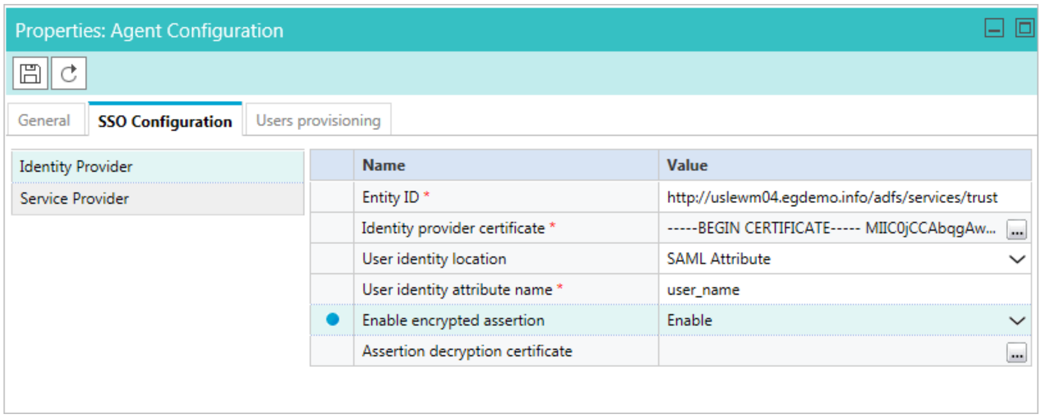
- An identity provider certificate is required for SAML 2.0 configurations. Consult your IT department about obtaining the certificate.
- Encrypted SAML assertion is supported. If you wish to enable encrypted SAML assertion, you will need a Java Keystore (JKS) file for the decryption certificate. Contact your IT to obtain the Java Keystore file.

- Metadata ensures a secure transaction between an identity provider and a service provider. SAML 2.0 provides a well-defined, interoperable metadata format that can be used to expedite the trust process between the SP and IDP. Consult your IT department about obtaining IDP and SP metadata. Note: SP Metadata for customer portals, Chat, Agent portals, and the Advisor Desktop should be provided separately.
- SAML is a time sensitive protocol and the IDP determines the time-based validity of a SAML assertion. If the identity provider and the service provider clocks are not synchronized, the assertion becomes invalid and stops the SAML SSO feature. Consult your IT department about synchronizing the IDP clock with the SP clock.
- Information provided here can also be applied to secure chat and secure messaging single sign-on settings. For more information, see "Customer Single Sign-On" on page 233.

To configure SSO for SAML 2.0 systems:

1. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security > Single Sign On > Configurations**
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.
   - **Allow local login for specific users:** Select whether users should only be able to log in to the application through the SSO authentication methods or if they can log in to the application locally as well. Select **Yes** to enable local login, **No** to disable. The type of authentication required of a user can be controlled at the user level. See "Creating Department Users" on page 186 for more details.
   - **Single Sign-On Type:** Select **SAML 2.0**.
   - **Create or update user account on login:** You may adjust this field if your configuration is using Auto-Provisioning. For more information, see "User Auto-Provisioning" on page 228.
4. Click the **SSO Configuration** tab.
5. Under the SSO Configuration tab, the Service Provider can be allowed to initiate the authentication for SAML in addition to Identity Provider. For Service Provider initiated authentication, ensure that the partition level setting Web Server URL or Load Balancer URL is correctly configured. For more information, see "Web Server URL or Load Balancer URL" on page 46.
   - Under the Identity Provider option, provide the following:
     - **Identity provider certificate:** The public key certificate. The certificate must start with "`-----BEGIN CERTIFICATE-----`" and end with "`-----END CERTIFICATE-----`"
     - **User Identity Location:** Select SAML **Subject Identifier** to set the identity location in the certificate to the default SAML subject identifier. Select **SAML Attribute** to assign the identity location to a specific attribute in the certificate, e.g. `email.address`. Provide the attribute in the **User Identity Attribute Name** field.
     - **User Identity Attribute Name:** Applicable only when User ID Location value is an SAML attribute. This can be adjusted within the SAML assertion and used to select a different attribute for the authentication of users, such as an email address. It can also be used to create new users with a SAML Attribute. For example, if a customer is identified through the value provided in the email.address attribute, and the value of email address provided doesn't match any customer in the system, a new customer is created with the provided SAML attributes.

  - **Enable encrypted assertion:** If you wish to enable SAML assertion for console login, set the value to **Enable**. If not, set the value to **Disable**.
  - **Assertion decryption certificate:** If Enable Encrypted Assertion is set to **Enable**, click the **Assistance** … button and provide the following in the Assertion Decryption Certificate window:
    - **Java keystore file:** Provide the file path of your Java Keystore File. This file will be in .jks format and contains the decryption key the system needs to access files secured by SAML.
    - **Alias name:** The unique identifier for the decryption key.
    - **Keystore password:** The password required for accessing the Java Keystore File.
    - **Key password:** The password required for accessing the Alias' decryption key.



	Name	Value
	Entity ID *	http://uslewm04.egdemo.info/adfs/services/trust
	Identity provider certificate *	-----BEGIN CERTIFICATE----- MIIC0jCCAbqgAw... …
	User identity location	SAML Attribute
	User identity attribute name *	user_name
●	Enable encrypted assertion	Enable
	Assertion decryption certificate	…

Provide SAML configuration details

- If you wish to allow the Service Provider to initiate the authentication for SAML, provide the following under the Service Provider option:
  - **Service provider initiated authentication:** Set to Enable.
  - **Entity ID:** Entity ID or the Service Provider.
  - **Request signing 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 aame:** 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.
  - **Signing algorithm:** Set the signing algorithm for the service provider. You may set the value to **SHA-1** or **SHA-256**.
  - **Identity provider login URL:** The URL for SAML authentication.
  - **Logout URL:** The URL to which users will be redirected upon logging out.

Important: **Enabling the Service Provider to initiate SAML authentication is optional, but providing the authentication information to for the Identity Provider is mandatory.**

6. Click the **Save** 💾 button.

Utilizing SAML 2.0 Metadata

If you are configuring your system for use SAML 2.0, the SAML metadata may be necessary. Be aware that the metadata differs for systems with auto-provisioning enabled. For more information, see "User Auto-Provisioning" on page 228.

When configuring the `<saml:AttributeValue>`*Application Type*`</saml:AttributeValue>` property in the metadata, refer to the following table containing possible values for the application to which users will be signed-in:

Application Type Value	Application
APPLICATION_TYPE_CONSOLE	partition 1 console
APPLICATION_TYPE_PORTAL_KA	KA portal if the system has been upgraded from eGain 14 or earlier, or the system is using Sunburst templates
APPLICATION_TYPE_PORTAL_KA_STATELESS	KA portal (for templates other than Sunburst)
APPLICATION_TYPE_ADVISOR_DESKTOP	Advisor Desktop

When using the XML metadata sample provided below, replace the variable values. For more information about these values, see "Configuring Single Sign-On for SAML 2.0" on page 223 and "Post-Configuration" on page 230.

Metadata Sample for Users with Auto-Provisioning

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
entityID="https://ServiceProvider.com/SAML">

    <SPSSODescriptor AuthnRequestsSigned="true"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

    <KeyDescriptor use="signing">

        <ds:KeyInfo>

        <ds:X509Data>

        <ds:X509Certificate>ServiceProvider.com SSO Key</ds:X509Certificate>

        </ds:X509Data>

        </ds:KeyInfo>

    </KeyDescriptor>

    <KeyDescriptor use="encryption">

        <ds:KeyInfo>

        <ds:X509Data>

        <ds:X509Certificate>ServiceProvider.com Encrypt Key</ds:X509Certificate>

        </ds:X509Data>

        </ds:KeyInfo>

        <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa- 1_5" />

    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://anyserver.com/SAML/SLO/Browser" />

    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
    format:unspecified</NameIDFormat>

    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
    POST" Location="https://egainserver.com/system/SAML/SSO/POST.controller" index="0" />

    <AttributeConsumingService index="1">

        <ServiceName xml:lang="en-US">eGain</ServiceName>

        <RequestedAttribute Name="application_type">

        <saml:AttributeValue>Application Type</saml:AttributeValue>

        </RequestedAttribute>

        <RequestedAttribute Name="user_name">

        <saml:AttributeValue>User name</saml:AttributeValue>

        </RequestedAttribute>

        <RequestedAttribute Name="department">

        <saml:AttributeValue>Department name</saml:AttributeValue>

        </RequestedAttribute>

        <RequestedAttribute Name="firstName">

        <saml:AttributeValue>User first name</saml:AttributeValue>

        </RequestedAttribute>

        <RequestedAttribute Name="lastName">

        <saml:AttributeValue>User last name</saml:AttributeValue>

         </RequestedAttribute>

        <RequestedAttribute Name="screenName">

        <saml:AttributeValue>User screen name</saml:AttributeValue>

        </RequestedAttribute>

         <RequestedAttribute Name="user.groups">

    <saml:AttributeValue>Comma-separated values of existing user groups in the department of the
    user.</saml:AttributeValue>

    </RequestedAttribute>

    </AttributeConsumingService>

    </SPSSODescriptor>

</EntityDescriptor>
```

Metadata Sample for Users without Auto-Provisioning

```
<?xml version="1.0" encoding="UTF-8"?>

<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
entityID="https://ServiceProvider.com/SAML">
```

```
    <SPSSODescriptor AuthnRequestsSigned="true"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
        <ds:KeyInfo>
        <ds:X509Data>
        <ds:X509Certificate>ServiceProvider.com SSO Key</ds:X509Certificate>
        </ds:X509Data>
        </ds:KeyInfo>
    </KeyDescriptor>
    <KeyDescriptor use="encryption">
        <ds:KeyInfo>
        <ds:X509Data>
        <ds:X509Certificate>ServiceProvider.com Encrypt Key</ds:X509Certificate>
        </ds:X509Data>
        </ds:KeyInfo>
        <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa- 1_5"/>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://anyserver.com/SAML/SLO/Browser" />
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
    format:unspecified</NameIDFormat>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
    POST" Location="https://egainserver.com/system/SAML/SSO/POST.controller" index="0" />
    <AttributeConsumingService index="1">
        <ServiceName xml:lang="en-US">eGain</ServiceName>
        <RequestedAttribute Name="application_type">
        <saml:AttributeValue>Application Type</saml:AttributeValue>
        </RequestedAttribute>
    </AttributeConsumingService>
    </SPSSODescriptor>
</EntityDescriptor>
```

User Auto-Provisioning

Important: **This feature is only available for SAML 2.0 configurations.**

With SAML 2.0 configured in your system, you can set up a user groups for auto-provisioning to make user management easier and quicker. Once established, auto-provisioning allows for the following to occur upon an authenticated SAML user logging in to the application:

- If the SAML user record exists, but that record does not exist in the application, a new record is created in the application.
- If the SAML user record exists in the application, but the user’s record differs in the application, it is updated with to match the SAML record.

With auto-provisioning, large numbers of existing SAML users can be created or updated within the application and given the necessary licenses to begin immediately working upon being authenticated.

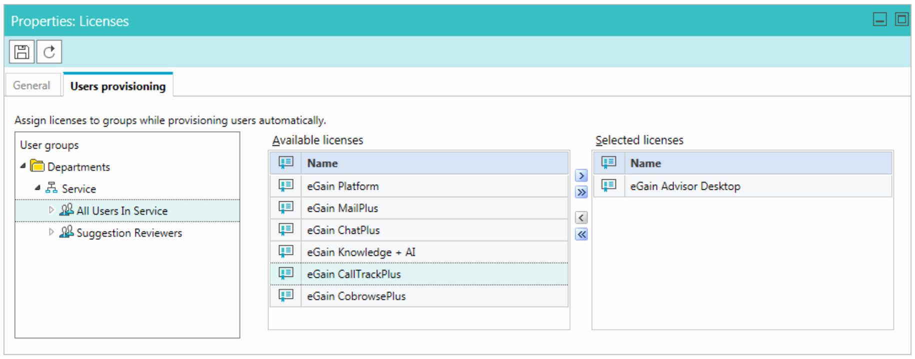
Important things to note about auto-provisioning:

- Auto-provisioning is only supported on SAML 2.0
- Auto-provisioning is only supported for users logging into one of the eGain consoles or the Knowledge Agent portal.
- Auto-provisioning is only supported for department-level users.
- Auto-provisioning allows for the use of custom attributes.
- Roles, languages, user profiles, and guided help profiles, still need to be configured at the group level even with auto-provisioning enabled.

To configure auto-provisioning:

1. In the Tree pane, browse to **Administration >** *Partition: Partition_Name* **> Security > SSO and Provisioning > Licenses.**
2. In the List pane, select **Licenses**.
3. In the Properties pane, select the **Users provisioning**.
4. Under the User provisioning tab, select user groups from the various departments in the partition.
5. From the list of Available licenses, move the desired licenses for that group to the Selected licenses list. This maps user groups to licenses and allows the application to automatically assign licenses to users based on the groups in which they reside.

   Users of the groups selected here acquire the necessary licenses immediately upon being created or updated in the system when they are authenticated via SAML.



Assign licenses to groups while provisioning users automatically.

Name
eGain Platform
eGain MailPlus
eGain ChatPlus
eGain Knowledge + AI
eGain CallTrackPlus
eGain CobrowsePlus

Name
eGain Advisor Desktop

Provide the necessary licenses for the user group

6. Click the **Save** button.

7. In the Tree pane, browse to **Administration >** *Partition: Partition Name* **> Security > SSO and Provisioning > SSO Configurations**.
8. In the List pane, select **Agent Configuration**.
9. In the Properties pane, under the General tab for your SAML 2.0 configuration, click the Create/Update user account on login field and select **Yes**. This field is disabled if your single sign-on configuration type is anything other than SAML 2.0.
10. Click the **Save** button.

Post-Configuration

Once SSO has been configured, minor changes are made to the application that may alter your user experience.

Logging in with SSO

The URL needed for users to access the application or the knowledge portal may be different from what you were previously using, depending on which SSO type you are using.

Important: **LDAP systems do not require a new URL to access the application or portal. Users just need to use their LDAP credentials to log in to the application.**

Logging in with Siteminder SSO

Once you have configured your system to use Siteminder, use the following URLs to access the application and the portal:

- **Partition 1:** `http(s)://`*HOST_NAME*`/`*context_root*`/Siteminder/SSO/POST.controller`
- **Partition 0:** `http(s)://`*HOST_NAME*`/`*context_root*`/Siteminder/SSO/POST.controller?partitionId=0`
- **Knowledge Portal:** `http(s)://`*HOST_NAME*`/`*context_root*`/Siteminder/SSO/POST.controller?application_type=APPLICATION_TYPE_PORTAL_KA&portal_id=`*portal_id*`&template_name=`*template_name*`&language=`*language*`&country=`*country*

Logging in with SAML SSO

Once you have configured your system to use SAML 1.1 or 2.0, obtain the necessary tokens for your users and use the following URLs to access the application and the portal:

- **Partition 1:** `http(s)://`*HOST_NAME*`/`*context_root*`/SAML/SSO/POST.controller`
- **Partition 0:** `http(s)://`*HOST_NAME*`/`*context_root*`/SAML/SSO/POST.controller`

An access token is required to log in to this partition with this URL. The token must have an attribute named `application_url` containing the value: `/`*context_root*`/web/view/platform/common/login/root.jsp?partitionId=0`

- **Knowledge Portal:** There are two methods in which users may be able to access the portal with SAML systems:
  - **Application Assertion in Request**: The assertion about the target application (portal url, etc) must be present in html requests made to POST.controller.

    An access token is required to log in to the portal, which must have the following portal attributes and their values:

    - Template Name
    - Portal ID
    - Language
    - Country
    - `application_type=APPLICATION_TYPE_PORTAL_KA_STATELESS`

    Once the attributes have been established, users can use the following URL to log in: `http(s)://`*HOST_NAME*`/`*context_root*`/SAML/SSO/POST.controller`.
  - **Application Assertion in SAML Attribute**: The assertion about the target application must be present in the SAML token, etc.

    Users must have a token with the attribute named `application_type` containing the value `APPLICATION_TYPE_PORTAL_KA_STATELESS`. The following attributes are also required:

    - Portal ID
    - Template Name
    - Language
    - Country

    Once the attributes have been established, users can use the following URL to log in: `http(s)://`*HOST_NAME*`/`*context_root*`/SAML/SSO/POST.controller?application_type=APPLICATION_TYPE_PORTAL_KA_STATELESS&portal_id=`*portal_id*`&template_name=`*template_name*`&language=`*language*`&country=`*country*

Important: **If the system has been upgraded from eGain 14 or earlier, or the system is using Sunburst templates, replace application_type=APPLICATION_TYPE_PORTAL_KA_STATELESS with application_type=APPLICATION_TYPE_PORTAL_KA.**

Local Login Setting

Users of Partition 1 with the “administer partition” permission are able to log into the application locally without using SSO access methods by using the following URL: `http(s)://`*HOST_NAME*`/`*context_root*`/web/view/platform/common/login/root.jsp?partitionId=1&localLogin=true`. Users outside this partition, or without this permission, will not be able to log in to the application with this URL unless the **Allow local login for specific users** setting has been enabled and the user's authentication method has been configured for Local Login. Refer to the SSO configuration steps of your system and “Creating Department Users” on page 186 for more information.

For more information about this setting, see “Allow Local Login for Partition Administrators” on page 59.

7

Customer Single Sign-On

About Customer Single Sign-On

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

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

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

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

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

- Creating Identity Providers
- Configuring Customer Single Sign-On

Customer Single Logout

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

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

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

- **Configure Single Logout for the Identity Provider:** This involves providing SLO endpoints exposed by the eGain application to the IdP. For more information, see "Planning Your Configuration" on page 235.
- **Enable and Configure Customer SLO in the eGain Application:** This involves turning on single logout services for each provider configured in the eGain application, as well as providing additional details required by these services. For more information, see "Creating Identity Providers" on page 236.

Planning Your Configuration

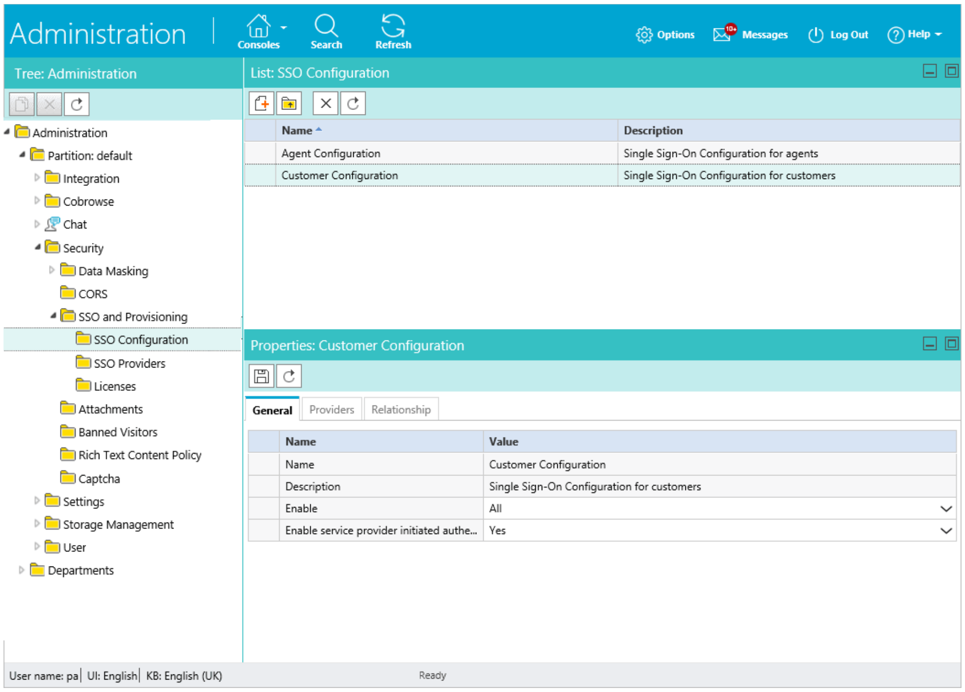
Before configuring this feature, perform the following:

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

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

Customer Single Sign-On Configuration

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



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

Name	Value
Name	Customer Configuration
Description	Single Sign-On Configuration for customers
Enable	All
Enable service provider initiated authe...	Yes

Before configuring customer SSO, configure the identity providers

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

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

- “Creating Identity Providers” on page 236
- “Configuring Customer Single Sign-On” on page 240

Creating Identity Providers

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

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

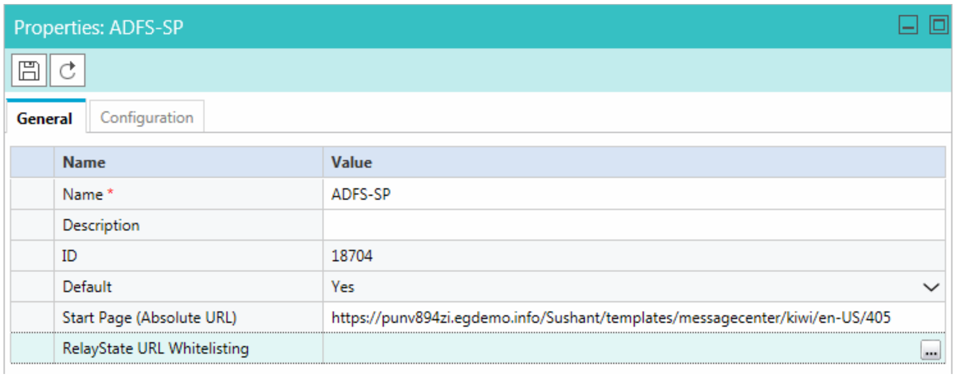
- An identity provider certificate is required for SAML 2.0 configurations. Consult your IT department about obtaining the certificate.
- Encrypted SAML assertion is supported. If you wish to enable encrypted SAML assertion, you will need a Java Keystore (JKS) file for the decryption certificate.
- A Java Keystore (JKS) file is necessary if the service provider is enabled to authenticate users in SAML 2.0, as well. Contact your IT to obtain the Java Keystore file.
-

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

To create identity providers:

1. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security > SSO and Provisioning > SSO Providers**.
3. In the List pane, click the **New** button.
4. In the Properties pane, under the General tab, provide the following:
    - **Name:** The name of the identity provider
    - **Description:** A description of the identity provider
    - **ID:** This field is automatically updated and cannot be changed.
    - **Default:** Select **Yes** to make this the default identity provider for customer single sign-on configurations. If not, select **No**.
    - **Start Page (Absolute URL):** Provide the URL for the page on which web-based customers should land when successfully logging in with single sign-on.
    - **RelayState URL Whitelisting:** A RelayState URL is an absolute URL of the web page where the user is redirected to after successfully logging in through SSO. RelayState URLs can serve the same purpose as the Start Page URL, however, RelayState URLs take precedence when configured. Use this optional field to whitelist any RelayState URLs used by the service provider. Click the **Assistance** button and select one of the following options from the pop-up window:
        - **Allow all RelayState URLs:** Whitelists all RelayState URLs of the service provider.

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



Properties: ADFS-SP

Name	Value
Name *	ADFS-SP
Description	
ID	18704
Default	Yes
Start Page (Absolute URL)	https://punv894zi.egdemo.info/Sushant/templates/messagecenter/kiwi/en-US/405
RelayState URL Whitelisting	...

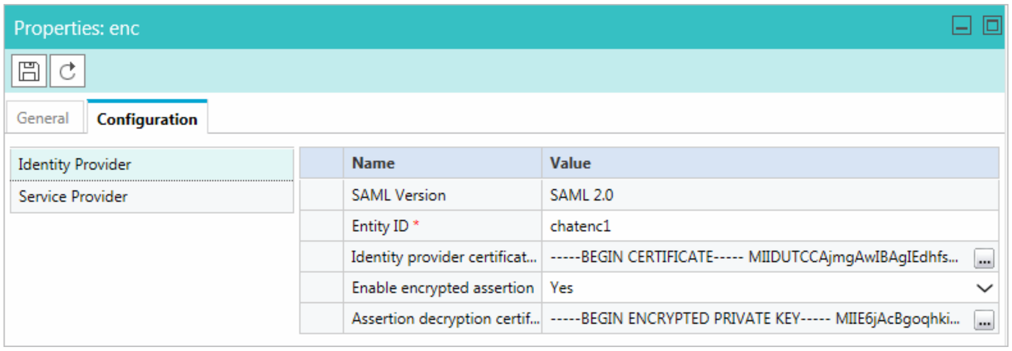
Provide the general information

5. Click the **SSO Configuration** tab. Under the SSO Configuration tab, the Service Provider can be allowed to initiate the authentication for SAML in addition to Identity Provider. For Service Provider initiated authentication, ensure that the partition level setting Web Server URL or Load Balancer URL is correctly configured. For more information, see “Web Server URL or Load Balancer URL” on page 46.

   ❍ Under the Identity Provider section, provide the following:

   - **SAML Version:** This is set to SAML 2.0 and cannot be changed.
   - **Entity ID:** Entity ID or the issuer.
   - **Identity provider certificate:** The public key certificate. The certificate must start with “-----BEGIN CERTIFICATE-----” and end with “-----END CERTIFICATE-----”
   - **Enable encrypted assertion:** Select **Yes** to enable assertion encryption or **No** to disable encryption.
   - **Assertion decryption certificate:** If **Enable Encrypted Assertion** is set to **Yes**, click the **Assistance** ... button and provide the following in the Assertion Decryption Certificate window:
     - **Java keystore file:** Provide the file path of your Java Keystore File eg: `C:\keystore\`*version_number*`\SSO\keystore.jks`. This file is in .jks format and contains the decryption key the system needs to access files secured by SAML.
     - **Alias name:** The unique identifier for the decryption key.
     - **Keystore password:** The password required for accessing the Java Keystore File.

        - **Key password:** The password required for accessing the Alias' decryption key.



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

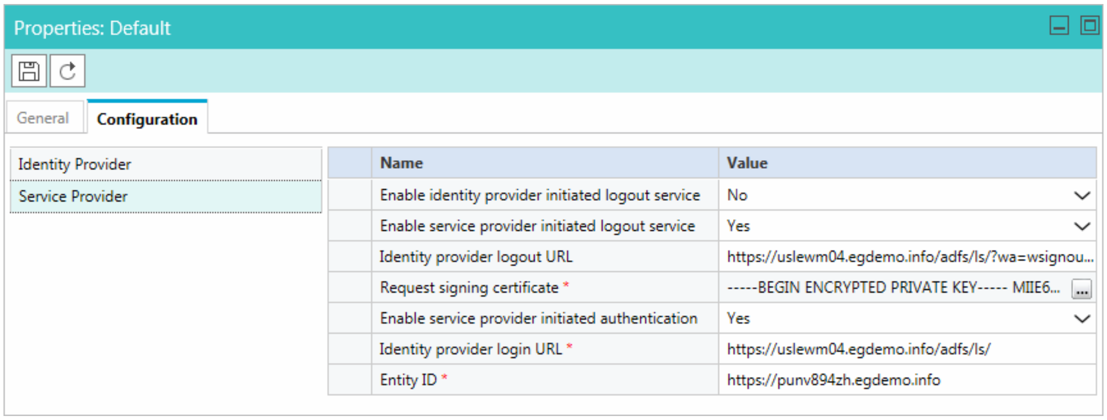
Provide the identity provider SAML configuration information

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

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

    - **Identity provider logout URL:** The IdP endpoint URL where the application submits its logout requests and logout responses. This must be provided if the **Enable identity provider initiated logout service** field or **Enable service provider initiate logout service** field is set to **Yes**.
    - **Request signing certificate:** Click the **Assistance** ... button, provide the following information in the next window, and click **OK**.
        - **Java keystore file:** Provide the file path of your Java Keystore File eg: `C:\keystore\`*version_number*`\SSO\keystore.jks`. This file is in .jks format and contains the decryption key the system needs to access files secured by SAML. On distributed installations, this should be stored on the application server.
        - **Alias name:** The unique identifier for the decryption key.
        - **Keystore password:** The password required for accessing the Java Keystore File.
        - **Key password:** The password required for accessing the Alias' decryption key.
    - **Enable service provider initiated authentication:** Set to **Yes** to Enable. Setting this field to **Yes** enables the **Identity provider login URL** field and the **Entity ID** field.
    - **Identity provider login URL:** The URL for SAML authentication.

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



Name	Value
Enable identity provider initiated logout service	No
Enable service provider initiated logout service	Yes
Identity provider logout URL	https://uslewm04.egdemo.info/adfs/ls/?wa=wsignou...
Request signing certificate *	-----BEGIN ENCRYPTED PRIVATE KEY----- MIIE6...
Enable service provider initiated authentication	Yes
Identity provider login URL *	https://uslewm04.egdemo.info/adfs/ls/
Entity ID *	https://punv894zh.egdemo.info

Provide the service provider SAML configuration information

6. Click the **Save** button.

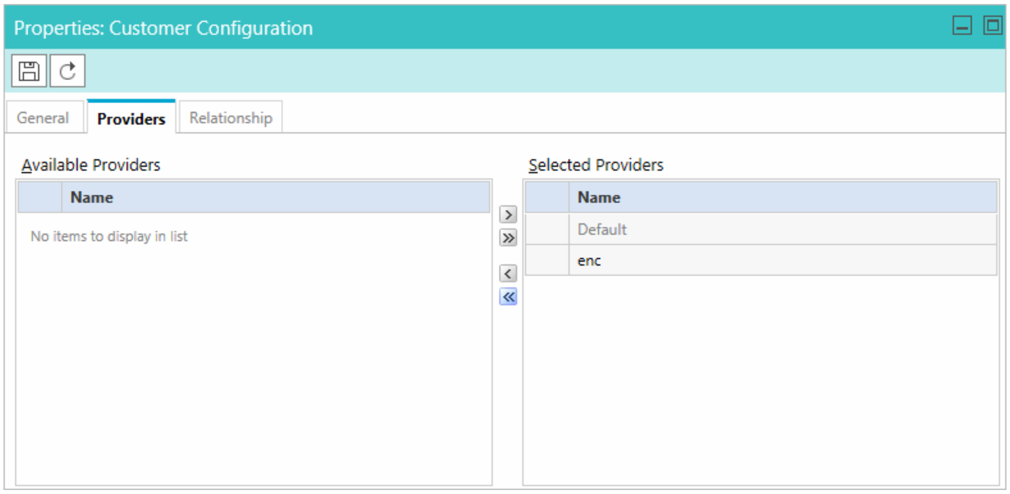
Configuring Customer Single Sign-On

To configure customer single sign-on:

1. Sign into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security > SSO and Provisioning > SSO Configuration**.
3. In the List pane, select **Customer Configuration**.
4. In the Properties pane, under the General tab, set the **Enable** field to one of the following options:
   - **Customer 360**: Enables customer single sign-on for Customer 360, which can be used by customers when accessing secure messaging centers.
   - **Chat**: Enables customer single sign-on for Secure Chat.
   - **All**: Enables customer single sign-on for both Customer 360 and Secure Chat.

   If the configuration is set to **Customer 360** or **All**, service provider initiated authentication can be enabled by setting the **Enable service provider initiated authentication** field to **Yes**. If you want to disable it, set the field to **No**.
5. In the Properties pane, under the Providers tab, move the identity providers that have been configured for single sign-on from the Available Providers list to the Selected Providers list. For more information about configuring identity providers, see “Creating Identity Providers” on page 236.

6. The Relationships tab displays all entry points in the partition that have been enabled for Secure Chat for reference. For information about configuring entry points, see *eGain Administrator's Guide to Chat and Collaboration Resources*.



Available Providers

Name
No items to display in list

Selected Providers

Name
Default
enc

Select the identity providers for the customer SSO configuration

7. Click the **Save** 💾 button.

Configuring Your Website for Secure Chat

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

Troubleshooting

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

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

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

8

Attachments

About File Attachments

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

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

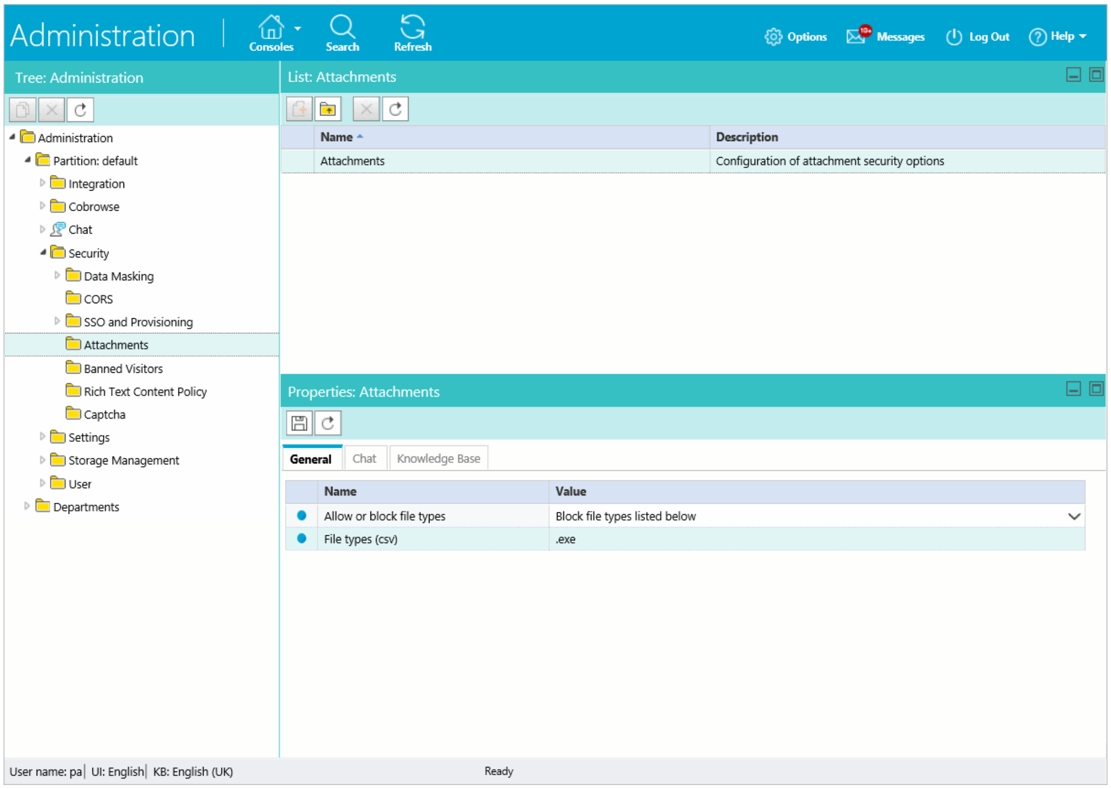
Configuring your list of blocked and allowed file types at this level affects all departments within the partition and supersedes any blocked file extensions for emails set at the department level. For more information about blocked file extensions for email, see the *eGain Administrator's Guide to Email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

Blocking Attachment File Types

To block file types for attachments:

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

5. In the File types (csv) field, enter the file extensions you wish to block. The extensions require a period in front of their names and a comma to separate each entry. For example: `.txt,.exe,.xls,.pdf,.png,.log,.xml`



Name	Description
Attachments	Configuration of attachment security options

Name	Value
Allow or block file types	Block file types listed below
File types (csv)	.exe

Select the file types to block

By default, `.csv` files are blocked.

6. Click the **Save** button.

Allowing Attachment File Types

To allow file types for attachments:

1. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security > Attachment**s.
3. In the List pane, select **Attachments**.
4. In the Properties pane, under the General tab, set the **Allow or block file types** field to one of the following:
   - **Allow all file types**
   - **Allow file types listed below**
5. If **Allow file types listed below** is selected, in the File types (csv) field, enter the file extensions you wish to specifically allow. The extensions require a period in front of their names and a comma to separate each entry. For example: `.txt,.exe,.xls,.pdf,.png,.log,.xml`

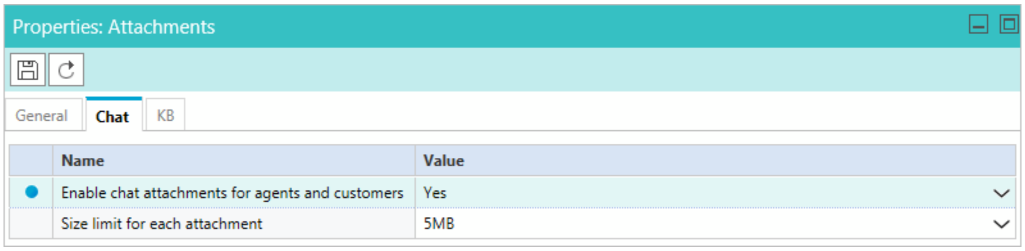
6. Click the **Save** button.

Enabling Chat Attachments

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

To enable chat attachments for agents and customers:

1. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security > Attachment**s.
3. In the List pane, select **Attachments**.
4. In the Properties pane, under the General tab, set the file types you wish to allow for attachments. See "Allowing Attachment File Types" on page 245 for details.
5. In the Properties pane, click the Chat tab and adjust the following fields:
   - **Enable chat attachments for agents and customers**: Set the value to **Yes** to enable chat attachments for the partition. Set the value to **No** to disable.
   - **Size limit for each attachment**: Set the maximum allowed size for a chat attachment from the dropdown menu. Values include: 2 MB, 3 MB, 4 MB, 5 MB, 6 MB, 7 MB, 8 MB, 9 MB, 10 MB.



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

Enable chat attachments for agents and customers

6. Click the **Save** button.

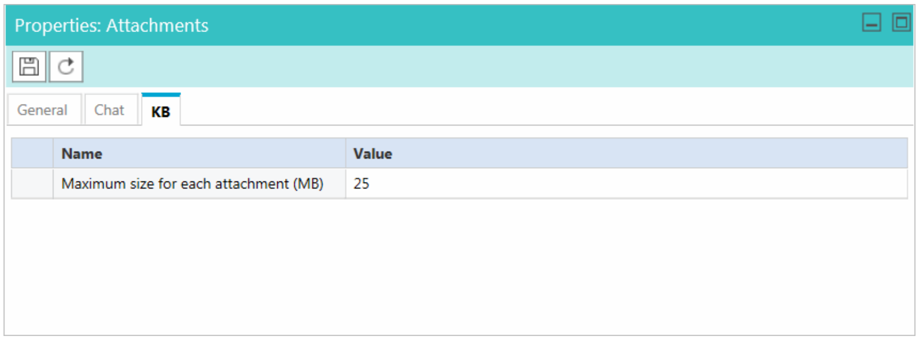
   This enables the use of chat attachments at a partition-level. Be aware that in order for attachments to be shared between agents and customers during chats, the "Enable chat attachments for agents and customers" setting must be enabled at the queue-level in a department. For more information about enabling chat queues for attachments, see *eGain Administrator's Guide to Routing and Workflows*.

Enabling Knowledge Base Attachments

With attachments enabled at the partition level, authors can attach files to the articles that they create in the knowledge base. To help control their use, limits are placed on the maximum allowed size for knowledge attachments for the partition.

To set the maximum size of knowledge attachments for a partition:

1. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security > Attachment**s.
3. In the List pane, select **Attachments**.
4. In the Properties pane, under the General tab, set the file types you wish to allow for attachments. See "Allowing Attachment File Types" on page 245 for details.
5. In the Properties pane, click the KB tab and adjust the following field:
   - **Maximum size for each attachment (MB):** Set the maximum size for any one article attachment for the partition. Minimum allowed value is 1 MB and maximum allowed value is 25 MB. By default, the value is set to 25 MB.



Name	Value
Maximum size for each attachment (MB)	25

Set the maximum allowed size for any one KB attachment

6. Click the **Save** 💾 button.

9 Rich Text Content Policies

About Rich Text Content Policies

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

- Chat messages sent by agents to customers
- Chat messages sent by customers to agents
- Content of standard and secure incoming emails
- Content of standard and secure outgoing emails
- Knowledge article content created by authors
- Knowledge article content submitted by customers
- Incoming social media content
- Outgoing social media content

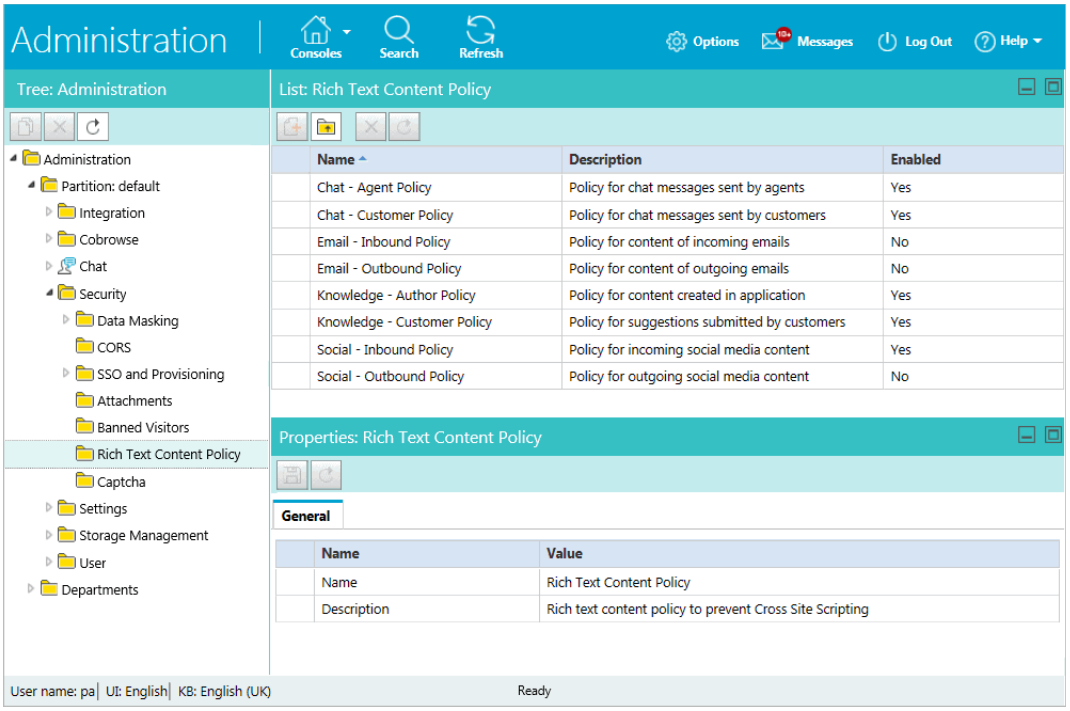
The content policy is an XML file that outlines the rules to be followed while parsing the content. It primarily addresses three things:

- 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 255.



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
Knowledge - Customer Policy	Policy for suggestions submitted by customers	Yes
Social - Inbound Policy	Policy for incoming social media content	Yes
Social - Outbound Policy	Policy for outgoing social media content	No

Name	Value
Name	Rich Text Content Policy
Description	Rich text content policy to prevent Cross Site Scripting

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 251.
7. Return to the Administration Console and select the **Import Policy** option from the same dropdown menu.
8. Locate the updated XML file and import it.
9. Click the **Save** button.

Configuring the Rich Text Content Policy File

The policy XML file has four notable sections:

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

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

Adding a Common Regular Expression

To create a common regular expression:

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

```
<common-regexps>
```

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

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

Allowing a New Tag

To allow a new tag:

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

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

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

Allowing a New Attribute for a Tag

To allow a new attribute for a tag:

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

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

Adding a Rule for an Attribute Value

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

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

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

To add a list of literal values:

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

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

```
<literal value="rtl"/>
</literal-list>
</attribute>
</tag>
```

To add a list of regular expressions:

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

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

Adding Validation for Attributes

To add validation for attributes:

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

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

Allowing a New CSS Property

To allow a new CSS property:

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

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

Adding a Rule for a CSS Property Value

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

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

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

To add a list of literal values:

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

```
<property name="width">

<literal-list>

<literal value="auto"/>

<literal value="inherit"/>

</literal-list>

</property>
```

To add a list of regular expressions:

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

```
<property name="width">

<regexp-list>

<regexp value="(\d)+(px)"/>

<regexp name="number"/>

</regexp-list>

</property>
```

Allowing Links in the Source Attribute of an iframe Tag

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

- Make the following entry in the XML file:

```
<tag name="iframe" action="validate">

<attribute name="src">

<regexp-list>

<regexp value="((http(s:|:))?)((//)?)((www.)?)(externaldomain/)((.)*)"/>

</regexp-list>

</attribute>
```

```
</tag>
```

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

Using a Plain Text Policy

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

To allow plain text content only:

- Import a policy file with only the following content:

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

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

</anti-samy-rules>
```

Restoring Rich Text Content Policies

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

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

To restore rich text content policies:

1. Log into the business partition and go to the Administration Console.
2. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Rich Text Content Policy**.
3. In the List pane, select the policy you wish to restore.
4. In the Properties pane, click the **Restore** button.
5. In the window that opens, click **Yes**.

10

reCAPTCHA Configuration

About reCAPTCHA

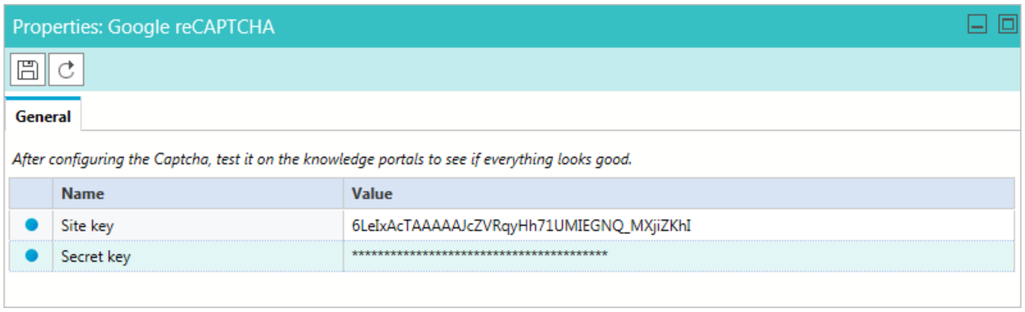
reCAPTCHA is a free service that protects the portals in your system from spam and abuse from automated software. It does this while still allowing your valid users to access your portal with minimal interference. reCAPTCHA is available for configuration in the application to enable users to share articles and information from the portal with one another, or send emails through the portal, without the risk of compromising the security of the portal.

Enabling reCAPTCHA

To configure the eGain application to use Google's reCAPTCHA, you need the Site key and Secret key from your Google account registered for your portal's domain. Consult your Google documentation for more details about obtaining these keys and adding the widget to your portals.

To enable reCAPTCHA:

1. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security > Captcha**.
2. In the List pane, select Google reCAPTCHA.
3. In the Properties pane, set the following:
   - **Site key**
   - **Secret key**



After configuring the Captcha, test it on the knowledge portals to see if everything looks good.

	Name	Value
●	Site key	6LeIxAcTAAAAAJcZVRqyHh71UMIEGNQ_MXjiZKhI
●	Secret key	**

Enable CAPTCHA

4. Click the **Save** 💾 button.

   Changes made to this setting affect all portals in the partition. After configuring the setting, KB Managers will need to enable the widget on the knowledge portals to be able to use it.

11

Blocked Visitors

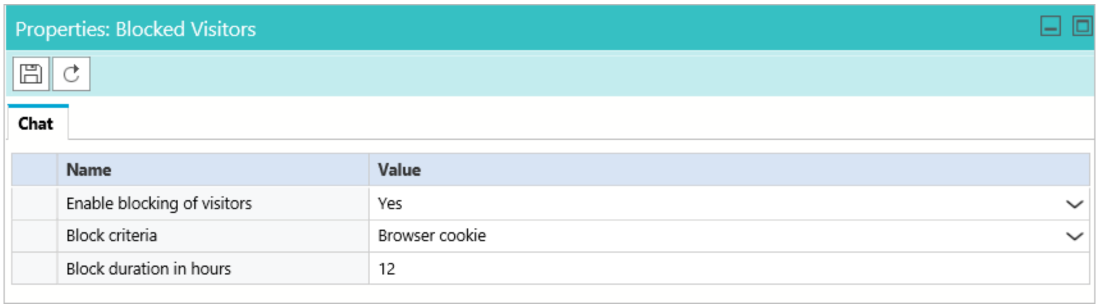
About Blocked Visitors

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

Configuring Blocked Visitor Settings

To enable visitor blocking:

1. In the Tree pane, browse to **Administration > Partition:** *Partition_Name* **> Security > Blocked Visitors**.
2. In the List pane, select **Blocked Visitors**.
3. In the Properties pane, set the following:
   - **Enable blocking of visitors:** Select **Yes** to enable the ability for agents to block customers and **No** to disable it.
   - **Block criteria:** Select the method in which the user is identified for the ban. Select **Browser cookie** to use cookies to identify and ban the user. Select **Visitor IP address** to ban the user based on the IP address.
   - **Block duration in hours:** Provide the number of hours in which an agent is banned when an agent blocks the customer. The minimum value for this field is 1 hour. The maximum value for this field when the criteria is set to **Browser cookie** is 168 hours (7 days). The maximum value for this field when the criteria is set to **Visitor IP address** is 87,600 hours (3650 days).



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

Enable the ability for agents to block users

4. Click the **Save** 💾 button.

12

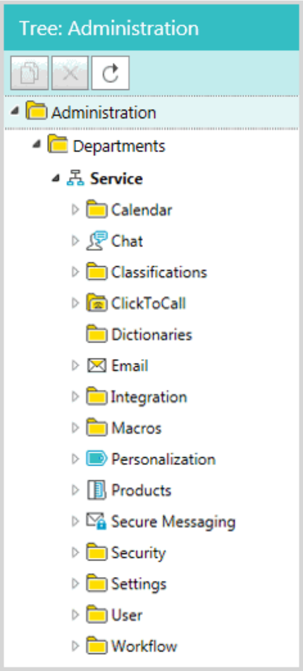
Departments

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 and shared departments.

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



The Administration Console tree

The following business objects are available in departments:

- Calendars: For more information, see "Business Calendars" on page 268.
- Chat: For more information, see, *eGain Administrator's Guide to Chat and Collaboration Resources.*
- Classifications: For more information, see "Classifications" on page 275.
- Dictionaries: For more information, see "Dictionaries" on page 287.
- Email infrastructure: For more information, see, *eGain Administrator's Guide to Email Resources.*
- Data Masking for emails and chat: For more information, see "Data Masking" on page 197.
- Data adapters: For more information, see *eGain Administrator's Guide to Data Adapters.*

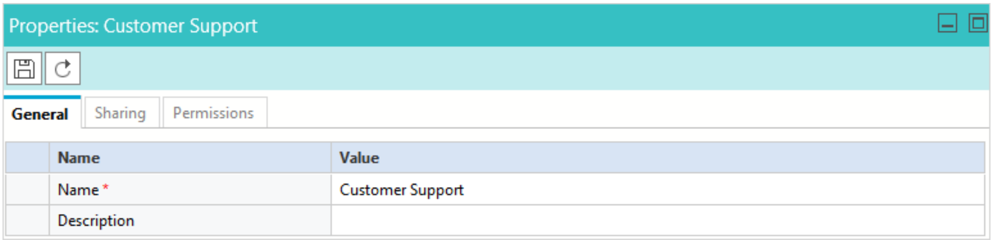
- Macros: For more information, see “Macros” on page 291.
- Personalization: For more information, see *eGain Knowledge Manager’s Guide.*
- Products: For more information, see “Products” on page 295.
- Profiles: For more information, see “Guided Help Profiles” on page 281.
- Settings: For more information, see “Settings” on page 39.
- Users: For more information, see “Users” on page 132.
- Workflows: For more information, see *eGain 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: < , . ? : > $ * \ / #



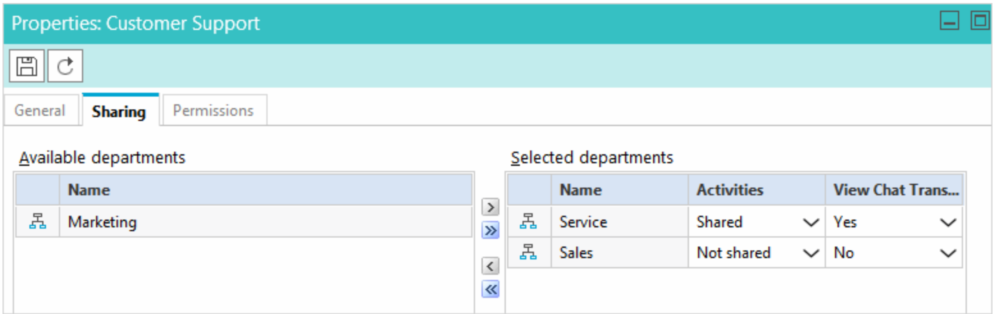
Properties: Customer Support

Name	Value
Name *	Customer Support
Description	

Set general properties

4. On the Sharing tab, select the departments that you want to share resources with from the list of available departments. Activities are not shared unless specified. To share activities with a particular department, locate it in the **Selected departments** list and change the value of the **Activities** column to **Shared** for this department.

   While transferring chats to other departments, you can choose to share the chat transcript from the original department with the agents of the other department. To enable this, select **Yes** in the **View Chat Transcript** column. By default chat transcripts are not shared between departments. If this setting is set to **No**, the chat transcript for a chat activity, once it has been transferred to a separate department can no longer be viewed. This means that when a chat activity is transferred to a department other than its original department, even if the agent in the receiving department responds to the chat with the customer and exchanges multiple messages, that agent is still unable to view the chat transcript for the activity. If you want your agents to be able to view chat transcripts for activities that have been transferred this field must be enabled.



Available departments

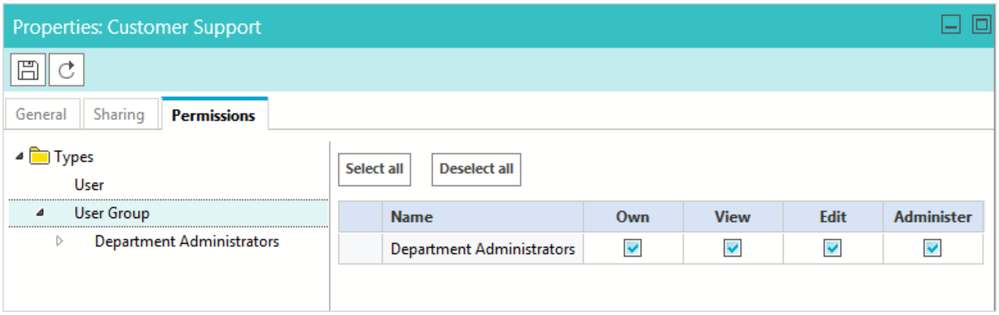
Name
Marketing

Selected departments

Name	Activities	View Chat Trans...
Service	Shared	Yes
Sales	Not shared	No

Share department resources with other departments

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.

Sharing Department Resources

Resources can be shared with other departments.

To share resources with other departments:

1. In the Tree pane, browse to the department whose resources are to be shared.
2. Now, go to the Properties pane. On the Sharing tab, do the following:
   a. From the list of available departments, select the departments that should be allowed to share resources with your department. For example, if you select the Sales department from the list, the administrator of the Sales department will be able to share users with your department. Such shared users become **Foreign** users in your department.

   b. Activities are not shared unless specified. To share activities with a particular department, locate it in the **Selected departments** list and change the value of the **Activities** column to **Shared** for this department. When you share activities, all users of the selected department are able to see the activities from your department. Users do not need to be foreign users in your department to view the activities.

c. While transferring chats to other departments, you can choose to share the chat transcript from the your department with the agents of the other department. To enable this, select **Yes** in the **View Chat Transcript** column. By default chat transcripts are not shared between departments.

3. Click the **Save** 💾 button.

Copying Departments

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

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

#	Object name	Notes
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.	ClicktoCall entry points	Copied as in original department
8.	Customer Associations	Copied as in original department
9.	Data masking for email and chat channels	Not copied
10.	Data Adapter Links (Access and Usage)	Copied as in original department
11.	Delivery Exceptions	Copied as in original department
12.	Department share	Department shares and foreign users are copied
13.	Dictionaries	Copied as in original department
14.	Macros	Copied as in original department
15.	Monitors	Copied as in original department
16.	Products	Copied as in original department
17.	Queues	Copied as in original department

#	Object name	Notes
18.	Service levels	Copied as in original department
19.	Settings	Copied as in original department
20.	Transfer codes	Copied as in original department
21.	User groups	Copied as in original department
22.	User roles	Copied as in original department
23.	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.
24.	Workflows	Copied as in original department with following exception: The **Active** field of workflows is set to **No**.
Objects in the Knowledge Base Console		
25.	Knowledge Base	Copied as in original department with following exception: User created folders and articles within are copied and same as original department. Personal folders are copied as *foldername_new_department_name.*
26.	Article bookmarks	Not copied
27.	Portals - Portals, Topics, and Templates	Not copied
28.	Profiles	Not copied
29.	Case bases	Not copied
Objects in the Social Console		
30.	Searches	Copied as in the original department
31.	Adapters	Copied as in the original department
32.	Settings	Copied as in the original department
Objects in the Tools Console		
33.	Screen Attribute Settings	Copied as in the original department
34.	User Attribute Settings	Copied as in the original department
35.	Relationships - Customer Associations	Copied as in the original department
36.	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.

13

Business Calendars

About Business Calendars

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

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

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

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

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

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

    8 am to 12 pm: Morning shift

    12 pm to 1 pm: Lunch break

    1 pm to 5 pm: Evening shift
  - Holiday

    12 am to 11.59 pm: Holiday

Use day labels to create calendars.

Managing Shift Labels

Creating Shift Labels

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

To create a shift label:

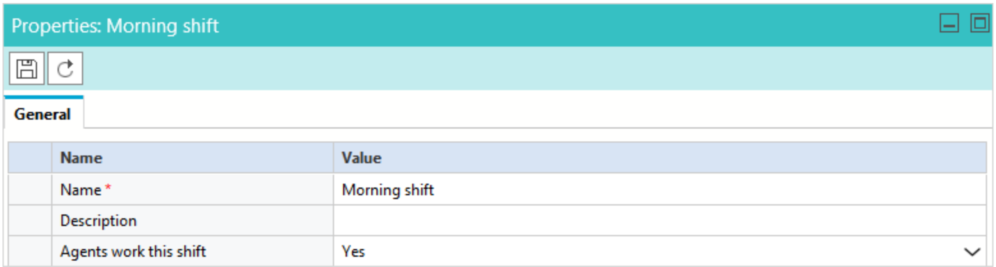
1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> Calendar > Shift Labels.**

2. In the List pane toolbar, click the **New** ⊞ button.

   The Properties pane refreshes to show the properties of the new shift label.

3. In the Properties pane, in the General tab, provide the following details.

   - **Name:** Type a name for the shift label. Do not use a comma (,) in the name.
   - **Description:** Type a brief description.
   - **Agents work this shift:** Specify if agents work in this shift or not. By default **Yes** is selected. Select **No** if agents do not work in this shift.



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

Set general properties

4. Click the **Save** 🖫 button.

Deleting Shift Labels

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

To delete a shift label:

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

Managing Day Labels

Creating Day Labels

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

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

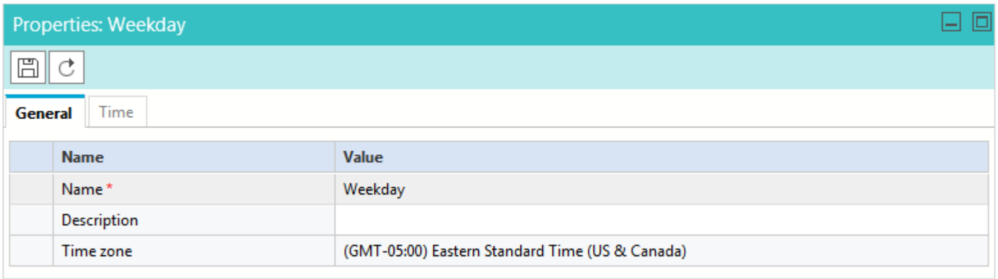
To create a day label:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> Calendar > Day Labels.**

2. In the List pane toolbar, click the **New** button.

   The Properties pane refreshes to show the properties of the new day label.

3. In the Properties pane, go to the General tab and provide the following details.
   - **Name:** Type a name for the day label. Do not use a comma (,) in the name.
   - **Description:** Type a brief description.
   - **Time zone:** It shows the time zone selected for the department. This field is disabled. If you want to change the time zone for your department, you can do it by changing the **Business calendar timezone** setting**.** For details on how to change this setting, see, “Setting the Time Zone” on page 272.

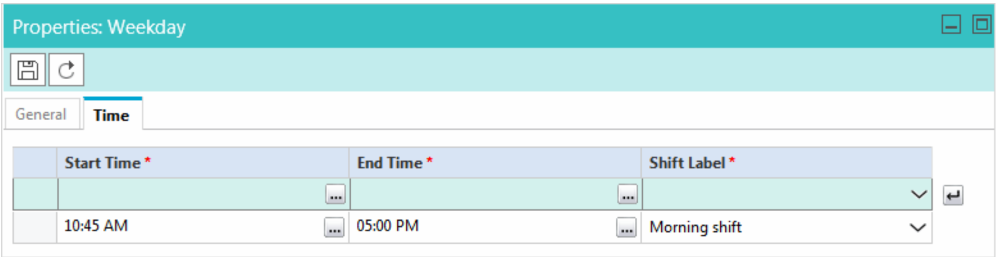


Name	Value
Name *	Weekday
Description	
Time zone	(GMT-05:00) Eastern Standard Time (US & Canada)

Set general properties

4. Next, go to the Times tab and provide the following details.
   - **Start time**: Select the start time for the day label.
   - **End time:** Select the end time for the day label.
   - **Shift label:** From the dropdown list, select the shift label to be used.

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



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

Set start times and end times for day labels

5. Click the **Save** button.

Deleting Day Labels

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

To delete a day label:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> Calendar > Day Labels.**
2. In the List pane, select the day label you want to delete.
3. In the List pane toolbar, click the **Delete** ☒ button.

Managing Business Calendars

Setting the Time Zone

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

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

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

To change the time zone setting:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> Settings > Department.**
2. In the List pane, select the department settings group.
3. In the Properties pane, go to the Attributes tab.
4. In the Attributes tab, select the **Business calendar timezone** setting**.** From the available time zones, select the time zone for your department.
5. Click the **Save** 💾 button.

Creating Business Calendars

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

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

To create a calendar:

1. In the Tree pane, browse to **Administration > Departments >** *Department_Name* **> Calendar > Calendars.**

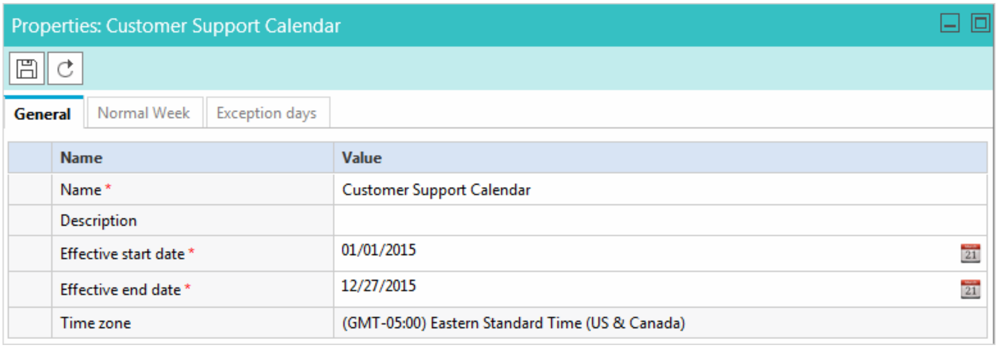
2. In the List pane toolbar, click the **New** button.

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

3. In the Properties pane, go to the General tab, and provide the following details.

   - **Name:** Type a name for the calendar.
   - **Description:** Type a brief description.
   - **Effective start date:** Select the date on which the calendar becomes active. Two calendars in a department cannot have overlapping dates. Also, the start date should be greater than the current date.
   - **Effective end date:** Select the date on which the calendar becomes inactive. Two calendars in a department cannot have overlapping dates. Also, the end date should be greater than the start date.

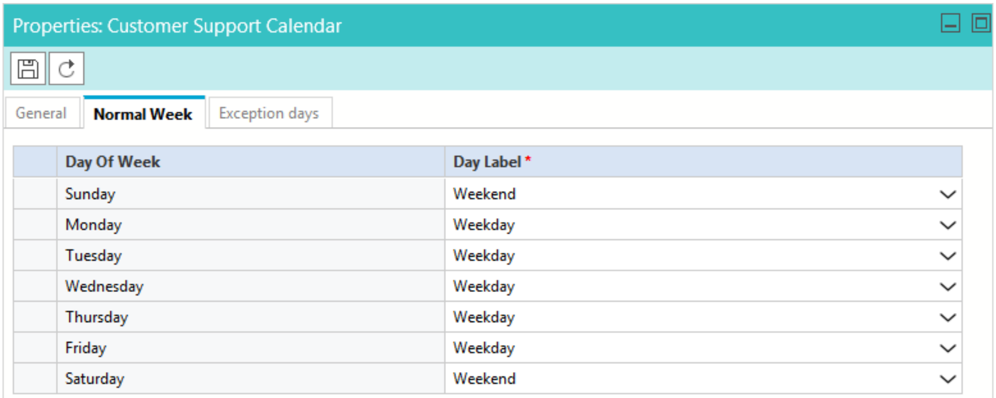
     On the set end date, the calendar becomes inactive. Once a calendar becomes inactive, the system considers the agents work time as 24*7*365, unless some other calendar becomes active automatically.
   - **Time Zone:** It shows the time zone selected for the department. This field is disabled. If you want to change the time zone for your department, you can do it by changing the **Business calendar timezone** setting. For details on how to change this setting, see, “Setting the Time Zone” on page 272.



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.

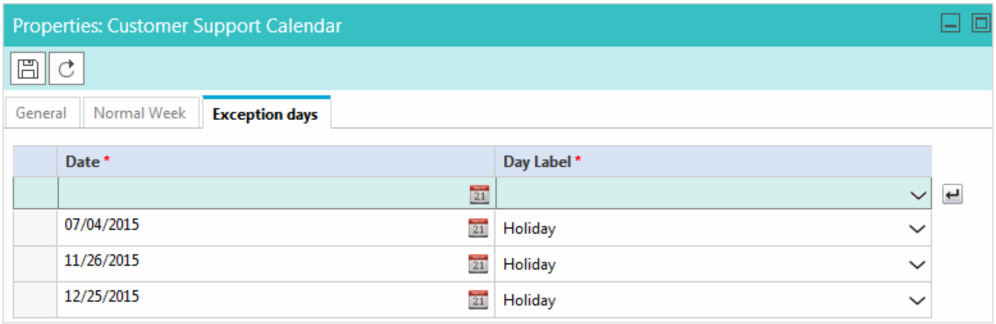


Day Of Week	Day Label *
Sunday	Weekend
Monday	Weekday
Tuesday	Weekday
Wednesday	Weekday
Thursday	Weekday
Friday	Weekday
Saturday	Weekend

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, and so on. Select the date on which there is some exception, and then select the day label to be used for that day.

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



Properties: Customer Support 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.

14

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 different codes meant to track the activity of agents and activities. Classifications are of the following types:

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

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

- Manually, from the Advisor Desktop
- Automatically, through workflows

Managing Transfer Codes

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

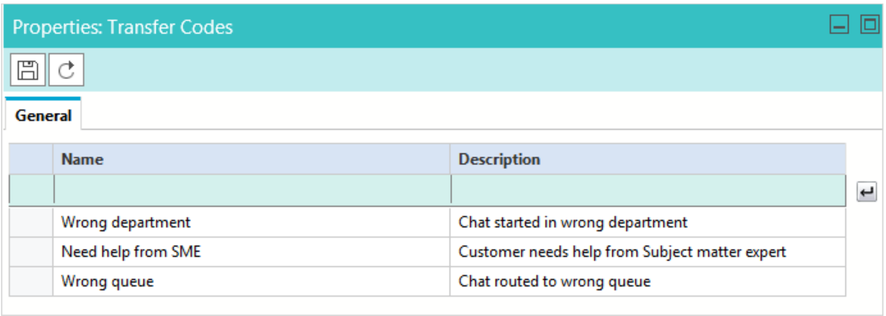
- Creating Transfer Codes on page 276
- Deleting Transfer Codes on page 277

Creating Transfer Codes

To create transfer codes:

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

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



Name	Description
Wrong department	Chat started in wrong department
Need help from SME	Customer needs help from Subject matter expert
Wrong queue	Chat routed to wrong queue

Create new transfer codes

3. Click the **Save** 💾 button.

Deleting Transfer Codes

To delete transfer codes:

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

Managing Not Ready Codes

To help supervisors and administrators track agent activity, Not Ready codes can be created to provide reasons as to why an agent might become unavailable. These codes can be made mandatory so that agents must select a reason code each time they mark themselves unavailable.

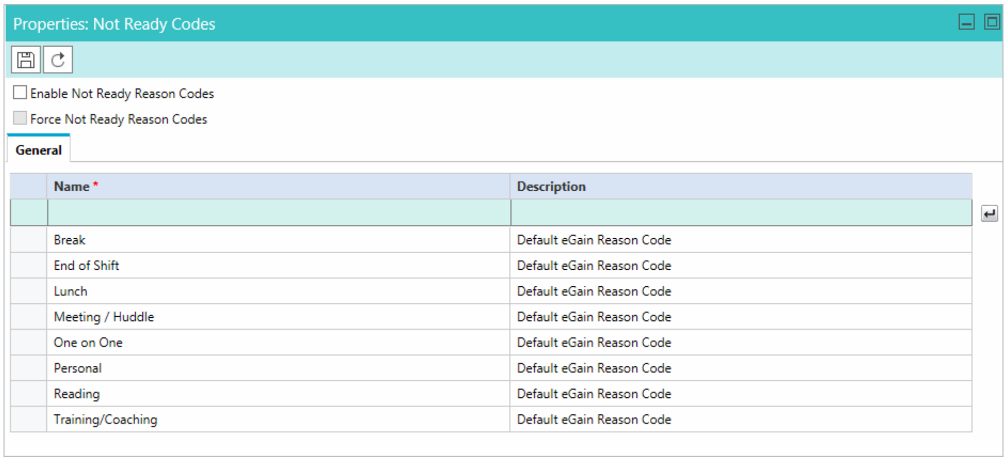
- Creating Not Ready Codes on page 277
- Deleting Not Ready Codes on page 278

Creating Not Ready Codes

To create a not ready code:

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

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



Properties: Not Ready Codes

☐ Enable Not Ready Reason Codes

☐ Force Not Ready Reason Codes

General

Name *	Description
Break	Default eGain Reason Code
End of Shift	Default eGain Reason Code
Lunch	Default eGain Reason Code
Meeting / Huddle	Default eGain Reason Code
One on One	Default eGain Reason Code
Personal	Default eGain Reason Code
Reading	Default eGain Reason Code
Training/Coaching	Default eGain Reason Code

Enable the reason codes

3. In the Properties pane, on the General tab, provide the following details.
   - **Name:** Type the name of the Not Ready Code.
   - **Description:** Provide a brief description.
4. Click the **Save** button.

Deleting Not Ready Codes

To delete a not ready code:

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

Managing Categories

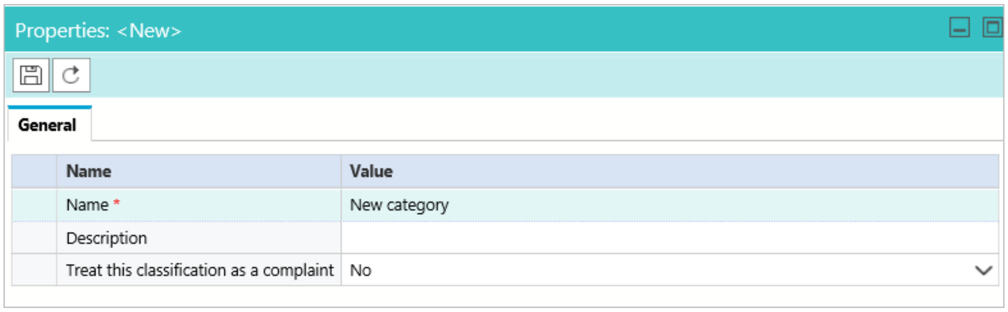
Categories are keywords or phrases that help you keep track of different types of activities. This section talks about:

- Creating Categories on page 279
- Deleting Categories on page 279

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 this classification as a complaint:** This field is not needed.



Name	Value
Name *	New category
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

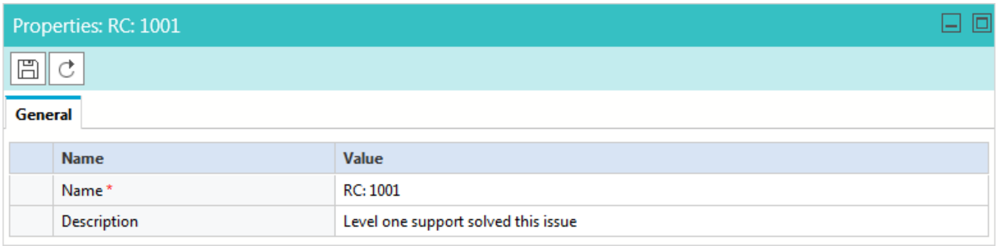
Resolution codes are keywords or phrases that help you keep track of how different activities were fixed. This section talks about:

- Creating Resolution Codes on page 280
- Deleting Resolution Codes on page 280

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.

15

Guided Help Profiles

About Guided Help Profiles

Profiles allow the user to separate the logical parts of the case base and thus restrict and control access to the case bases. A profile is required for any user to view data within the case base, so by default, the system profile is generally used and assigned to most users and consequently most case bases are built with case base objects that are defined to use the system profile, thus allowing all areas of the case base to be accessed by all users.

Channels, Expertise and Location are different attributes which can be used to control or restrict this access. For example, Channels allow you to define attributes such as Self-Service and Agent; Expertise allow you to define attributes such as Novice and Expert; Location allow you to define attributes such as Europe and North America or California and Nebraska. You can define profiles where certain attributes are selected with the purpose of restricting access to those users with matching profiles. You can create profiles based on channels, to restrict access to parts of the case base to Self-Service users only or Agent users only; similarly to Novice users only or Expert users only. They don't have to be one-dimensional; they can be two-dimensional or three-dimensional, so that in a complex configuration you could create a profile for a North American Novice Agent.

Each user defined to the system has a default guided help profile. You can also configure users of the system to have their own particular profile. If their particular profile allows them access to a particular part of the case base, then they can view the data within. This usually applies to users who search the case base; authors who build the case base generally have system profile to allow them to create the data in the case base without restriction.

In the case base itself, when building and designing the case base, there may then be requirements to build parts that are only applicable to a specific profile. For example, the articles that are created may differ depending on whether the end-user is a Self-Service user or Agent user. The profile setting for each article can then be set appropriately, thus keeping the main logic of the case base intact. An author can simply attach multiple articles to the same branch of the case tree, and the appropriate article is then displayed to the user during the search depending on profile. If a user has both profiles, the user sees both.

Guided help profiles can be used to affect logic flow by creating clusters with specific profiles or control actions with specific profiles. Different logic can then be programmed unique to that cluster or for control actions; thus additional questions can be presented in a cluster. For example, novice users might need more questions to be presented, or expert users perhaps have some default consequences quickly determined so a control action may be configured to jump to a different part of the case base or pre-answer some questions accordingly.

Guided help profiles can be added to clusters, control actions or articles to govern access at different levels of the case base depending on the desired logic and access restrictions. They can be applied to cases as well, but this would be for product selection case bases only.

To create a profile you need to create:

- Channels
- Expertise
- Locations

Creating Guided Help Profiles

In the system, by default a system profile is provided. The system profile is assigned all the locations, expertise and channels. When you create new locations, expertise or channels in the department, they are automatically assigned to the system profile. If you want you can change the name and other properties of the system profile.

To create a profile, specify:

- Channels
- Expertise types
- Business locations

Important: **The system profile cannot be deleted.**

To create a profile:

1. In the Administration tree, browse to **Departments >** *Department_Name* **> Personalization > Guided Help Profiles > Guided Help Profiles.**
2. In the List pane toolbar, click the **New** button.
3. In the Properties pane on the General tab provide the following information:
   - **Name:** Type a name of the profile.
   - **Description:** Type a brief description.
4. Next go to the Options tab:
   a. In the Channels section, from the available channels add the channels in the selected channels list.
   b. In the Expertise section, from the available Expertise add the Expertise in the selected expertise list.
   c. In the Locations section, from the available locations add the locations in the selected locations list.
5. Click the Relationships tab. In this tab you can assign the profile to users and user groups.
6. Click the **Save** button.

Deleting Guided Help Profiles

To delete a profile:

Important: **If a profile is assigned to any user, it cannot be deleted. Remove the reference to be able to delete it.**

1. In the Administration tree, select **Departments >** *Department_Name* **> Personalization > Guided Help Profiles > Guided Help Profiles.**
2. In the List pane, select a profile.
3. In the List pane toolbar, click the **Delete** button.

4. A message appears asking to confirm deletion. Click **Yes** to delete the profile.

Managing Channels

In the system, five default channels are provided:

- Chat
- Desktop
- Email
- IVR
- Web

Important: Predefined channels cannot be deleted.

Creating Channel

To create a channel:

1. In the Administration tree, select **Departments >** *Department_Name* **> Personalization > Guided Help Profiles > Channels.**
2. In the List pane toolbar, click the **New** button.
3. In the General tab provide the following information:
   - **Name:** Type a name of the channel.
   - **Description:** Type a brief description.
4. Click the **Save** button.

Deleting Channels

To delete a channel:

Important: If a channel is being used in a profile, it cannot be deleted. Remove the channel from the profile to be able to delete it.

1. In the Administration tree, select **Departments >** *Department_Name* **> Personalization > Guided Help Profiles > Channels.**
2. In the List pane, select a channel.
3. In the List pane toolbar, click the **Delete** ☒ button.
4. A message appears asking to confirm the deletion. Click **Yes** to delete the channel.

Managing Expertise

In the system, three default expertise are provided:

- Novice
- Expert
- Harvested

Important: **The default expertise cannot be deleted.**

Creating Expertise

To create an expertise:

1. In the Administration tree, select **Departments >** *Department_Name* **> Personalization > Guided Help Profiles > Expertise.**
2. In the List pane toolbar, click the **New** button.
3. In the General tab provide the following information:
   - **Name:** Type a name of the expertise.
   - **Description:** Type a brief description.
4. Click the **Save** button.

Deleting Expertise

To delete an expertise:

Important: **If an expertise is being used in a profile, it cannot be deleted. Remove the expertise from the profile to be able to delete it.**

1. In the Administration tree, select **Departments >** *Department_Name* **> Personalization > Guided Help Profiles > Expertise.**
2. In the List pane, select an expertise.
3. In the List pane toolbar, click the **Delete** button.
4. A message appears asking to confirm the deletion. Click **Yes** to delete the expertise.

Managing Locations

In the system, four default locations are provided:

- Asia Pacific
- Europe
- North America
- South America

Important: The default locations cannot be deleted.

Creating Locations

To create a location:

1. In the Administration tree, select **Departments >** *Department_Name* **> Personalization > Guided Help Profiles > Locations.**
2. In the List pane toolbar, click the **New** button.
3. In the General tab provide the following information:
   - **Name:** Type a name of the location.
   - **Description:** Type a brief description.
4. Click the **Save** button.

Deleting Locations

To delete a location:

Important: If a location is being used in a profile, it cannot be deleted. Remove the location from the profile to be able to delete it.

1. In the Administration tree, select **Departments >** *Department_Name* **> Personalization > Guided Help Profiles > Locations.**
2. In the List pane, select a location.
3. In the List pane toolbar, click the **Delete** ☒ button.
4. A message appears asking to confirm the deletion. Click **Yes** to delete the location.

16

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

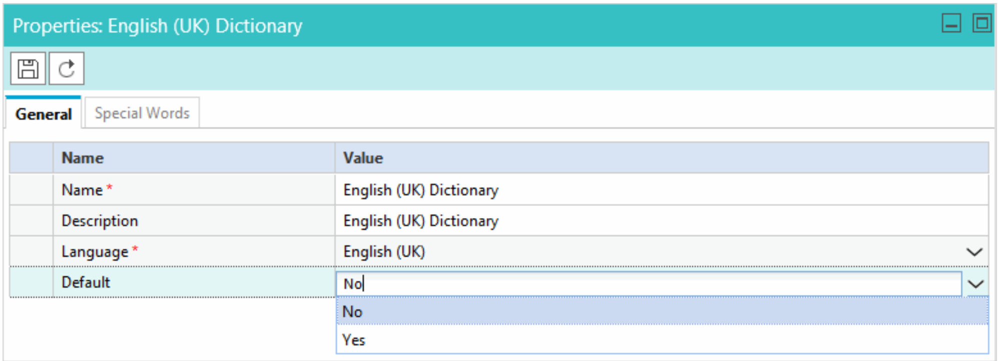
Important: **The application does not have dictionaries for the following languages: Chinese (Simplified), Chinese (Traditional), Czech, Greek, Japanese, Korean, Norwegian (Nynorsk), Portuguese (Brazilian), and Turkish.**

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

General | Special Words

Name	Value
Name *	English (UK) Dictionary
Description	English (UK) Dictionary
Language *	English (UK)
Default	No

No

Yes

Set a dictionary as the default dictionary for a department

4. Click the **Save** button.

Creating Dictionaries

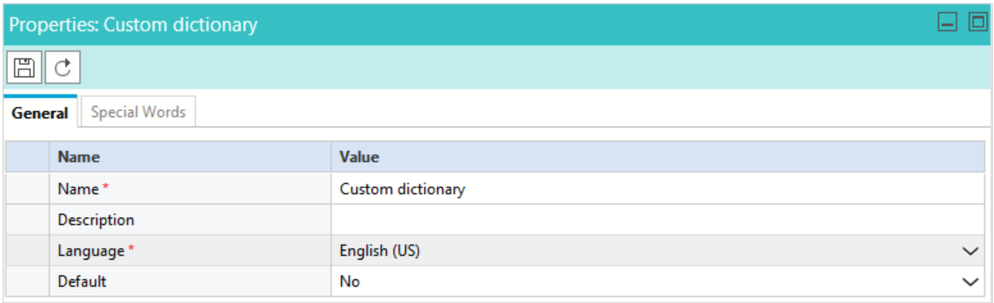
You can also create your own dictionary and store words in it and you can make this as the default dictionary for your department.

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

General | Special Words

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, and so on. 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.

17

Macros

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

About Macros

Macros are commands that fetch stored content. They are easy to use, and display the actual content, when expanded. Macros enable you to enter a single command to perform a series of frequently performed actions. For example, you can define a macro to contain a greeting for email replies. Instead of typing the greeting each time, you can simply use the macro. It is important to note that a macro's expansion is contextual to the object, and two macros of similar looking attribute expand differently depending upon the context object. For example, the macros "Email address of the contact point" and "Contact point data of the activity", both return the email address of the customer, but the first one returns the email address saved in the customer profile and the second one returns the email address associated with the activity in which the macro is used.

You can create two types of macros:

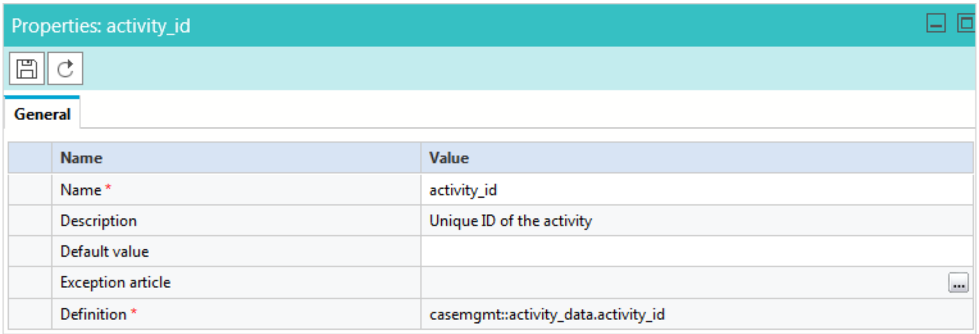
1. Business Objects macros: In Business Objects you can create macros for several objects. For example, Activity data, Customer data, User data, and so on. You have to define an attribute to a macro from the list of system provided attributes. Please note that you can define only a single attribute for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

Creating Business Object Macros

To create a business object macro:

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

- **Definition:** Click the **Assistance** button and from the Select Attribute window, select the attribute that defines this macro. Please note that for any date attributes (for example, case creation date) are displayed in the GMT timezone.



Properties: activity_id

General

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

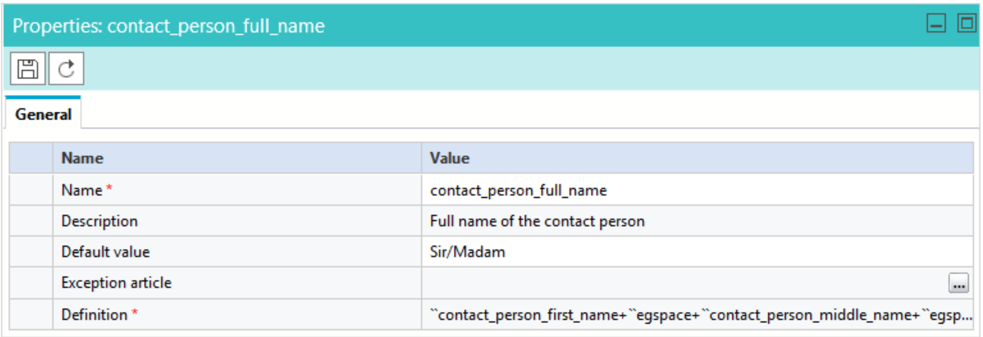
Set general properties

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.



Properties: contact_person_full_name

General

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.

18 Products

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

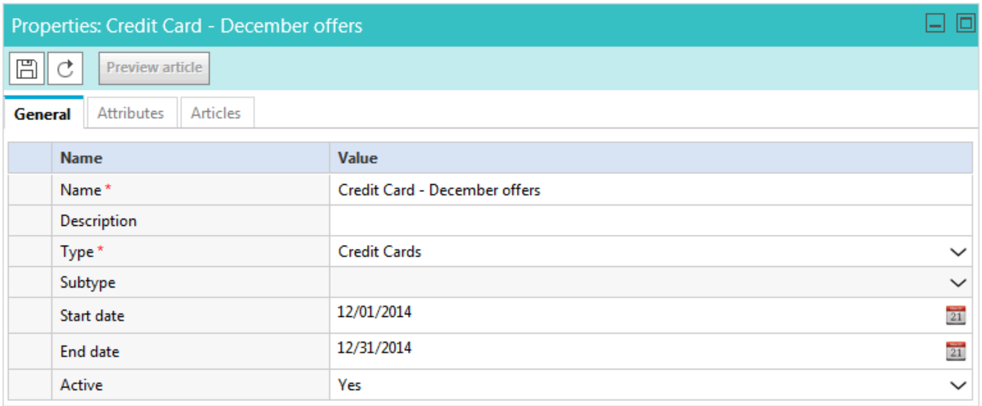
About Products

You can associate products from the product catalog in the system with customers in a department. A product catalog enables you to have a handy reference of your products within the system. You can configure the system to list your product catalogs with customized articles. A product catalog is a complete enumeration of items (products) arranged systematically with descriptive details.

Creating Product Catalogs

To create a product catalog:

1. In the Tree pane, browse to **Administration > Department >** *Department_Name* **> Products.**
2. In the List pane toolbar, click the **New** button.
3. In the Properties pane, on the General tab, provide a name and description for the product catalog.



Name	Value
Name *	Credit Card - December offers
Description	
Type *	Credit Cards
Subtype	
Start date	12/01/2014
End date	12/31/2014
Active	Yes

Set general properties

4. Click the Attributes tab to add more details about the product.
5. The Articles tab enables you to select an article from the Knowledge base.
6. Click the **Save** button.

Deleting Product Catalogs

To delete a product catalog:

1. In the Tree pane, browse to **Administration > Department >** *Department_Name* **> Products.**
2. In the List pane, select the product catalog you want to delete and click the **Delete** button.

19

Messaging Hub

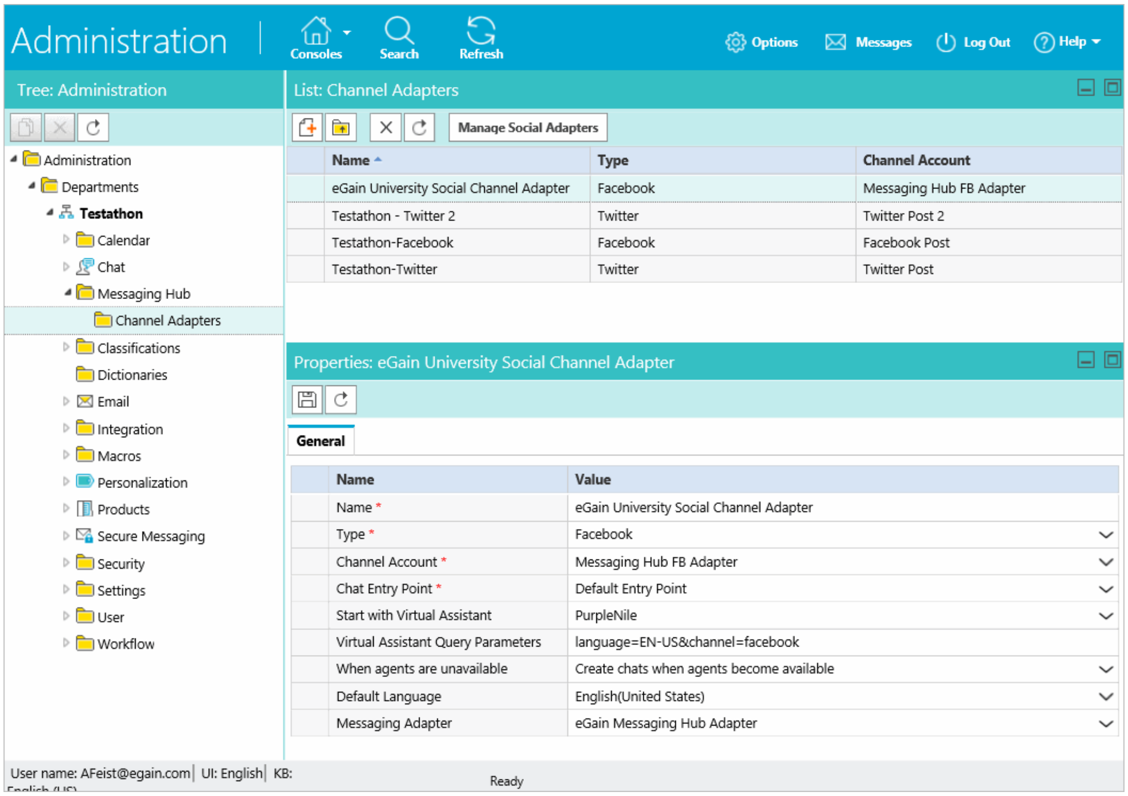
About Messaging Hub

The eGain Messaging Hub is designed to maximize live, real-time engagement with customers through digital social channels, similar to web chat. These channels can be configured to start with a Virtual Assistant (VA) before escalating to a live agent as needed.

Note that you will need an active OneTag account in order to use the Messaging Hub's features. For more information about setting up a OneTag account, see the *eGain Installation Guide*.

Messaging Hub currently supports the following messaging channels:

- Facebook Messenger
- Twitter Direct Messages (DMs)



Name	Type	Channel Account
eGain University Social Channel Adapter	Facebook	Messaging Hub FB Adapter
Testathon - Twitter 2	Twitter	Twitter Post 2
Testathon-Facebook	Facebook	Facebook Post
Testathon-Twitter	Twitter	Twitter Post

Name	Value
Name *	eGain University Social Channel Adapter
Type *	Facebook
Channel Account *	Messaging Hub FB Adapter
Chat Entry Point *	Default Entry Point
Start with Virtual Assistant	PurpleNile
Virtual Assistant Query Parameters	language=EN-US&channel=facebook
When agents are unavailable	Create chats when agents become available
Default Language	English(United States)
Messaging Adapter	eGain Messaging Hub Adapter

Messaging Hub is accessible for the department in the Tree pane

Social Adapters

Social adapters are required to configure channel adapters for Facebook Messages and Twitter DMs. They can be created in the Administration Console by navigating to **Departments >** *[Department Name]* **> Messaging**

Hub > Channel Adapters and clicking the **Manage Social Adapters** button. Any social adapters you have already created are managed here as well.

> Note: Social adapters can also be created in the Social Console.

For more information about creating and configuring post adapters for social networks like Facebook and Twitter, see the *eGain Social Media Manager's Guide*.

About Channel Adapters

Channel adapters let you engage with your customers through real-time conversations over social channels such as Twitter and Facebook. Channel adapters must be associated with a particular social account via a social adapter. You can either create a new social adapter for a particular social channel or use an existing one.

Note that channel adapters only create activities for private communications (visible to only the agent and the customer)for Twitter DMs and Facebook messages. Public social activities, such as tweets and Facebook wall posts, are created by social adapters and managed in the Social Console.

Configuring Channel Adapters

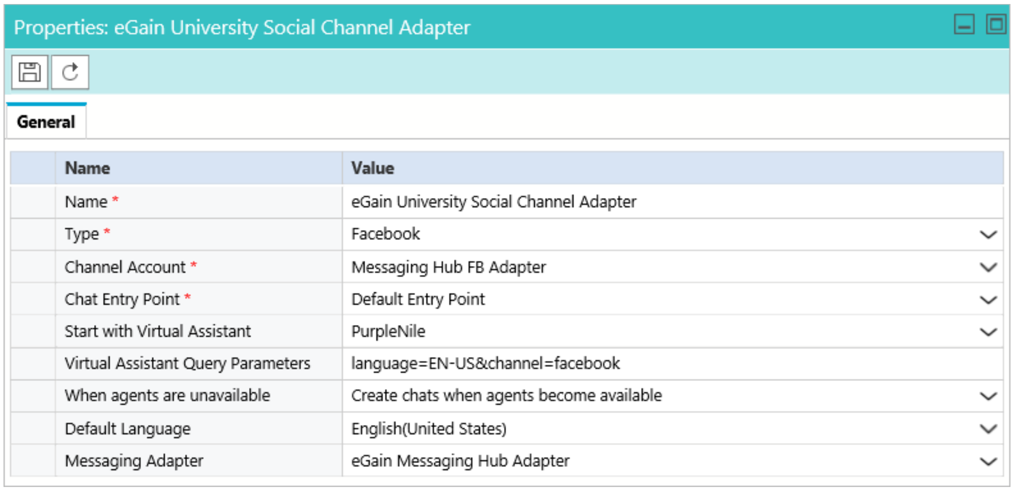
The following process details how to create and configure channel adapters. This section requires that you have already created the accompanying social adapters outlined above.

To configure channel adapters:

1. In the Administration Console, navigate to **Departments >** *[Department Name]* **> Messaging Hub > Channel Adapters**
2. Click the **New** button to create a new channel adapter or double-click an existing adapter to edit it.
3. In the Properties pane under the General tab, enter information for the following items:
   - **Name:** Enter a name for the channel adapter
   - **Type:** Select the adapter type from the dropdown menu
   - **Channel Account:** Select the desired channel account from the dropdown list. If you have created a social adapter, it will appear in this list.
   - **Chat Entry Point:** Select the desired chat entry point from the list. This determines which entry point will be used to funnel messages from the channel to your agents.
   - **Start with Virtual Assistant:** If you have an existing Virtual Assistant (VA) and you would like the VA to be the first point of contact in the channel, select the desired VA from the dropdown list. Note that any VAs that appear in this list are tied to your OneTag account.
   - **Virtual Assistant Query Parameters:** If you choose to use a VA, add any query parameters that you want the VA to search for when speaking with the customer. This helps the VA to better understand and route the conversation appropriately.

For example, you might add “language=EN-US&channel=twitter” into this field to direct your VA to look for English-language conversations that come in via your Twitter channel.

- **When agents are unavailable:** Select whether you want to hold incoming chat messages until an agent becomes available or display an automated off-hours message if no agents are available.
- **Default Language:** Determines the language for all system messages. This does not affect VA language settings.
- **Messaging Adapter:** Selects the messaging adapter to be used, with eGain Messaging Hub Adapter being the provided, out-of-the-box option. Any custom adapters you have created appear here.



Properties: eGain University Social Channel Adapter

General

Name	Value
Name *	eGain University Social Channel Adapter
Type *	Facebook
Channel Account *	Messaging Hub FB Adapter
Chat Entry Point *	Default Entry Point
Start with Virtual Assistant	PurpleNile
Virtual Assistant Query Parameters	language=EN-US&channel=facebook
When agents are unavailable	Create chats when agents become available
Default Language	English(United States)
Messaging Adapter	eGain Messaging Hub Adapter

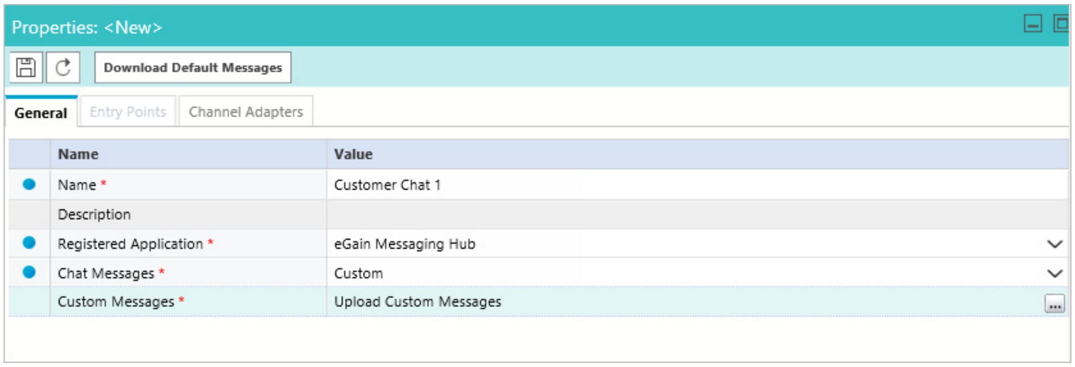
Configure the properties for the channel adapter

4. Click the Save 💾 button.

Customizing Chat Messages

If you want to customize the messages that get sent via your channel adapters, you can do so by navigating to **Departments >** *[Department Name]* **> Chat > Messaging Adapters**. You can choose to modify the default eGain Messaging Hub adapter or create a new one. However, ‘eGain Messaging Hub’ must be selected in the Registered Application field for all messaging adapters, whether you are using the default adapter or a custom one.

For more information about creating a custom messaging adapter, see the *eGain Administrator's Guide to Chat and Collaboration Resources*.



	Name	Value
●	Name *	Customer Chat 1
	Description	
●	Registered Application *	eGain Messaging Hub
●	Chat Messages *	Custom
	Custom Messages *	Upload Custom Messages

Customized message settings