

OpenText™ Identity and Access  
Management

**IAM Administration Administrator  
Guide**

The guide provides detailed information about the IAM Administration application for different types of administrators such as exchange operator, security administrator, service administrator, and others.

BNIMCO220100-AGD-EN-1

---

**OpenText™ Identity and Access Management  
IAM Administration Administrator Guide**  
BNIMCO220100-AGD-EN-1  
Rev.: 2022-Feb-28

**This documentation has been created for OpenText™ Identity and Access Management CE 22.1.**

It is also valid for subsequent software releases unless OpenText has made newer documentation available with the product, on an OpenText website, or by any other means.

**Open Text Corporation**

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111

Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440

Fax: +1-519-888-0677

Support: <https://support.opentext.com>

For more information, visit <https://www.opentext.com>

**Copyright © 2022 Open Text. All Rights Reserved.**

Trademarks owned by Open Text.

One or more patents may cover this product. For more information, please visit <https://www.opentext.com/patents>.

**Disclaimer**

No Warranties and Limitation of Liability

Every effort has been made to ensure the accuracy of the features and techniques presented in this publication. However, Open Text Corporation and its affiliates accept no responsibility and offer no warranty whether expressed or implied, for the accuracy of this publication.

---

# Table of Contents

<b>1</b>	<b>Getting Started</b> .....	<b>9</b>
1.1	What is IAM Administration? .....	9
1.2	Which browsers are supported? .....	9
1.3	How do I log into IAM Administration? .....	10
1.3.1	Log into IAM Administration through OpenText Supplier Portal .....	10
1.3.2	Log into IAM Administration directly using the application URL .....	10
1.4	Home Page .....	10
1.5	How do I log out of IAM Administration? .....	13
1.6	Roles and permissions .....	13
<b>2</b>	<b>Organization and User Registration</b> .....	<b>15</b>
2.1	Registration by Invitation .....	15
2.1.1	Inviting TLO to register .....	15
2.1.2	Inviting division to register .....	18
2.1.3	Inviting users to register .....	20
2.1.3.1	Managing by invitation user registration request .....	21
2.1.4	Assigning B2B Connect Service Package during TLO registration .....	22
2.1.5	Inviting existing TLO to register for a B2B service package .....	26
2.1.6	Inviting TLO to register for a DOD service package .....	29
2.1.7	Inviting user to register for DOD service package .....	31
2.2	Walk-in Registration .....	32
2.2.1	Walk-in Organization Registration .....	32
2.2.2	Managing walk-in organization registration request .....	35
2.2.3	Managing walk-in user registration request .....	36
2.3	Post registration .....	37
<b>3</b>	<b>Managing your profile details</b> .....	<b>39</b>
3.1	Managing my personal information .....	39
3.1.1	Account Info tab .....	39
3.1.2	Security tab .....	40
3.1.2.1	SMS mode for 2–step verification .....	42
3.1.2.2	Phone mode for 2–step verification .....	43
3.1.2.3	Email mode for 2–step verification .....	44
3.1.2.4	Google Authenticator mode for 2–step verification .....	45
3.1.3	Preferences tab .....	45
3.1.4	Roles tab .....	46
<b>4</b>	<b>Reports</b> .....	<b>47</b>
4.1	IAM Analytics .....	47
4.1.1	User Reports .....	48
4.1.2	Organization Reports .....	50

4.1.3	Package Reports .....	51
4.1.4	Federation Reports .....	52
4.1.5	Custom Reports .....	52
4.1.6	Working with reports .....	53
4.1.6.1	Creating and exporting a report .....	53
4.1.6.2	Scheduling report creation .....	54
4.1.6.3	Managing scheduled report creation jobs .....	56
4.1.6.4	Downloading completed reports .....	57
<b>5</b>	<b>Manage Organization .....</b>	<b>59</b>
5.1	Contents of the manage organization page .....	59
5.1.1	Organization hierarchy .....	60
5.2	Overview tab on the manage organization page .....	61
5.2.1	Adding a new user to your organization .....	62
5.2.2	Adding a new division to your organization .....	63
5.3	Users tab .....	64
5.3.1	Viewing user details .....	66
5.3.1.1	Suspending a user .....	66
5.3.1.2	Activating a suspended user .....	67
5.3.1.3	Deleting a suspended user .....	67
5.3.2	Overview tab for the selected user .....	68
5.3.3	Service Packages tab .....	69
5.3.3.1	Viewing service package details .....	70
5.3.3.1.1	Suspending a service package granted to a user .....	71
5.3.3.1.2	Activating a suspended service package granted to a user .....	71
5.3.3.1.3	Remove a suspended service package granted to a user .....	72
5.3.3.2	Assigning a service package to a user .....	72
5.3.4	Open Requests tab .....	74
5.3.5	History tab .....	75
5.3.6	Attributes tab .....	75
5.3.7	Security settings tab .....	75
5.3.8	Assigned roles tab .....	77
5.4	Service Packages tab .....	77
5.4.1	Service Packages list page .....	78
5.4.2	Viewing service package details .....	79
5.4.2.1	Suspending a service package granted to an organization .....	81
5.4.2.2	Activating a suspended service package granted to an organization ...	82
5.4.2.3	Deleting a suspended service package granted to an organization .....	82
5.4.3	SAO Hierarchy .....	83
5.4.3.1	Viewing and assign claim values for organizations in SAO hierarchy ..	85
5.4.3.2	Changing SAO designation .....	85
5.4.4	Assigning a service package to an organization .....	86

---

5.4.5	Requesting a service package for an organization .....	88
5.5	Pending requests tab for an organization .....	90
5.6	History tab for an organization .....	92
5.7	Administrators tab for an organization .....	93
5.8	Quick Search for users and organizations from Home Page .....	94
5.8.1	Search for users .....	94
5.8.2	Search for organizations .....	96
5.9	Unlocking locked user accounts .....	98
5.10	Managing divisions of your organization .....	99
5.10.1	Viewing a division's profile details .....	100
5.10.2	Managing users in divisions of your organization .....	102
5.10.3	Managing service packages in divisions of your organization .....	102
5.10.3.1	Assigning service packages to a division in your organization .....	102
5.10.3.2	Assigning claim code to a service package in a division .....	102
5.10.3.3	Suspending, activating, deleting service packages in divisions of your organization .....	103
5.10.4	Viewing pending requests for divisions in your organization .....	103
5.10.5	Viewing service package requests history for divisions in your organization .....	103
5.10.6	Viewing administrators for divisions in your organization .....	103
<b>6</b>	<b>My Access Management module .....</b>	<b>105</b>
6.1	Service Packages tab .....	105
6.1.1	Service Packages list page .....	106
6.1.2	Viewing service package details .....	107
6.1.2.1	Suspending a service package granted to a user .....	109
6.1.2.2	Activating a suspended service package granted to a user .....	109
6.1.2.3	Deleting a suspended service package granted to a user .....	110
6.1.2.4	Claim codes tab .....	110
6.1.2.4.1	Requesting claim values for claim code .....	111
6.1.2.4.2	Requesting ALLACCESS claim value for a claim code .....	112
6.1.2.5	Claim Roles tab .....	113
6.1.2.5.1	Requesting claim IDs for claim role .....	114
6.1.2.6	Remote Claim tab .....	115
6.1.2.6.1	Requesting claim value for remote claim .....	115
6.1.2.7	Service Administrators tab .....	116
6.1.3	Requesting a service package for yourself .....	117
6.2	Open Requests tab .....	119
6.3	History tab .....	120
<b>7</b>	<b>Administration Module .....</b>	<b>121</b>
7.1	Manage Groups .....	122
7.1.1	Manage Groups page .....	124

7.1.1.1	Filter groups .....	124
7.1.1.2	View and edit group details .....	125
7.1.1.2.1	Assign group members to a group .....	126
7.1.1.2.2	Remove members from a group .....	128
7.1.1.3	Create a new group .....	129
7.1.1.3.1	Create a restricted group .....	130
7.1.1.3.2	Create a subscription group .....	131
7.1.1.3.3	Create an all type group .....	135
7.1.1.4	Delete a group .....	138
7.2	Manage Roles .....	138
7.2.1	Manage roles page .....	139
7.2.1.1	Filter roles .....	140
7.2.1.2	View role details .....	140
7.2.1.3	Add users to a role .....	141
7.2.1.4	Remove users from a role .....	143
7.3	Manage Applications .....	145
7.3.1	Manage Applications page .....	146
7.3.1.1	Filter service packages .....	147
7.3.1.2	View service package details .....	148
7.3.1.3	Add a new subpackage .....	149
7.3.1.4	Remove a service package or a subpackage .....	151
7.3.1.5	View and edit subpackage details .....	152
7.4	Audits .....	154
7.4.1	View audit history by different audit types .....	156
7.4.1.1	Filter audit history list .....	156
7.4.2	Perform user audit .....	157
7.4.3	Perform user grant audit .....	160
<b>8</b>	<b>My Tasks Module – Manage Organization and User Requests .....</b>	<b>165</b>
8.1	Manage Organization Requests .....	166
8.1.1	New organization requests .....	166
8.1.1.1	Filter new organization requests .....	167
8.1.1.2	View, approve, or reject new organization requests .....	168
8.1.2	Service package requests .....	169
8.1.2.1	Filter service package requests .....	170
8.1.2.2	View , approve, or reject service package requests .....	170
8.1.3	Claim code requests .....	172
8.1.3.1	Filter claim code requests .....	172
8.1.3.2	View, approve, or reject claim code requests .....	173
8.1.4	Claim value requests .....	174
8.1.4.1	Filter claim value requests .....	175

---

8.1.4.2	View, approve, or reject claim value requests .....	176
8.2	Manage user requests .....	177
8.2.1	New user requests .....	178
8.2.1.1	Filter new user requests .....	178
8.2.1.2	View, approve, or reject new user requests .....	179
8.2.2	Service package requests by users .....	180
8.2.2.1	Filter service package requests by users .....	181
8.2.2.2	View, approve, or reject service package requests from users .....	182
8.2.3	Claim code requests by users .....	183
8.2.3.1	Filter claim code requests by users .....	184
8.2.3.2	View , approve, or reject claim code requests by users .....	184
8.2.4	Claim value requests by users .....	186
8.2.4.1	Filter claim value requests by users .....	186
8.2.4.2	View , approve, or reject claim value requests by users .....	187
<b>9</b>	<b>Appendix .....</b>	<b>189</b>
9.1	Administrator Roles .....	189





## Chapter 1

# Getting Started

This section provides an overview of the IAM (Identity and Access Management) Administration application including information about how to log in and out of the application, information about the tiles seen on the home page and how your user role controls the visibility and access to these tiles.

### 1.1 What is IAM Administration?

IAM (Identity and Access Management) Administration is a delegated administration tool designed to give power to people who are best in a position to manage user access and make security decisions. In some companies, this may be accomplished through a central office; while in other companies, this may be accomplished by delegating responsibility to people spread throughout the company. The delegated model allows each company to set up the structure that best fits their needs for managing access grants to their users.

The delegated model allows a single company to set up one or more organizations in IAM. IAM organizations are simply groupings of users with their own administrator(s) and their own available service packages. Organizations that are created below the parent organization are called divisions. Administrators in the parent organization can perform tasks on users in the divisions below.

### 1.2 Which browsers are supported?

IAM Administration is compatible with the listed version and the prior version of the following supported browsers:

- Microsoft Edge 98
- Google Chrome 98
- Mozilla Firefox 97

Browsers must be enabled for JavaScript, and popup blockers must be disabled.

## 1.3 How do I log into IAM Administration?

Users can access IAM Administration in two ways: from the OpenText OpenText™ Supplier Portal or using the URL for IAM Administration. Based on your situation, use the appropriate section to see login instructions.

### 1.3.1 Log into IAM Administration through OpenText Supplier Portal


Users who are already registered with Supplier Portal can use the URL provided to them by their customers or administrator to access Supplier Portal using their user ID and password.

Users who are not registered with Supplier Portal will be prompted to register themselves in order to log in to the Supplier portal and access the IAM Administration application.

#### To log into IAM Administration application

1. Log into Supplier Portal using your user ID and password.

The Home page opens.

2. Click the icon with your initials, for example , in the header area in the Home page.
3. Click **IAM Admin Console** in the list.

The IAM Administration application opens in another browser window.

### 1.3.2 Log into IAM Administration directly using the application URL

Access IAM Administration using the application website address. The URL is provided to you in an email when you are set up with a user profile.


## 1.4 Home Page

When you log into IAM Administration, the home page is the first page you see. The home page provides links to quickly access pages in the application for frequently performed workflows. These pages can also be accessed using the modules available in the navigation panel.


The home page consists of a header area and a body area, which include the following elements:





**Note:** Based on your role and permissions, you might see all of the following elements described in this topic or just a subset of them.

- The header section includes the following:
  - Menu : The main menu to open the navigation panel to access all or some of the modules in the application based on user role and permissions.

All the modules and submodules are listed here. Users will have visibility and access to all or some of these modules and submodules based on their role and permissions.


    - Home
    - Invite
    - Profile
    - Reports
      - Administration Reports
      - Upload Report Template
    - Manage Organization
      - Users
      - Service Packages
      - Pending Requests
      - History
      - Administrators
    - My Access Management
      - Service Packages
      - Open Requests
      - History
    - Administration
      - Manage Groups
      - Manage Roles
      - Manage Applications
      - Audits
    - My Tasks
  - Application name OpenText™ Identity and Access Management CE<*version number*>
  - Search : The search option to quickly search for users in the organization or divisions in the organization. See [“Quick Search for users and organizations from Home Page”](#) on page 94.

- An icon to access the **My Profile** and **Sign Out** options, for example . The icon shows the initials from user's name who is currently logged into IAM Administration application. For information about managing your profile details, see ["Managing my personal information" on page 39](#).
- The body of the Home page consists of many tiles as described here.
  - **Welcome** tile: Shows a greeting to the currently logged in user, user's name, and date and time of login.
  - **Quick Actions** tile: Provides links to quickly perform certain actions:
    -  **Tip:** Use the scroll bar to see all the links on this tile. Point the cursor to the right edge of the tile to see the scroll bar.
    - **Organization-related:** Open the Service Packages tab and Users tab for the current organization. Also, quickly open the page to request service packages for your organization
    - **Reports-related:** Launches IAM Analytics for report creation. Also provides a link to open the page to upload report templates.
    - **Audit-related:** Provides links to start quarterly user audit and annual user grant audit.
  - **Send Invitation** tile: Quickly opens the Invitation page to invite users, top-level organizations, and divisions to register. This tile is available for Exchange operators and Security administrators.
  - **Create User** tile: Quickly opens the page to create a new user. This tile is available for Exchange operators and Security administrators.
  - **Create Division:** Quickly opens the page to create and register a new division in the current organization. This tile is available for Exchange operators and Security administrators.
  - **Locked Accounts** tile: Displays the number of locked user accounts and on clicking, quickly opens the Users tab in the Manage Organization module for the current organization. The Users tab lists the names of the users whose accounts became locked. See ["Unlocking locked user accounts" on page 98](#).
  - **Pending Requests** tile: Displays the total number of pending requests from other organizations and users that the currently logged-in administrator needs to address.
  - **Organization Requests** tile: Displays the number of organization-related pending requests by subcategories: new organizations, service packages, and site code.
    - **New Organizations:** Clicking the link quickly opens the **Home > My Tasks** page for the New Organization Requests and from this page, the administrator can address pending new organization requests. See ["New organization requests" on page 166](#).

- **Service Packages:** Clicking the link quickly opens the **Home > My Tasks** page for the Service Package Requests from organizations and from this page, the administrator can address pending service package requests. See [“Service package requests” on page 169](#).
- **Site Code:** Clicking the link quickly opens the **Home > My Tasks** page for the Claim requests from organizations and from this page, the administrator can address pending claim requests. See [“Claim code requests” on page 172](#).
- **User Requests** tile: Displays the number of user-related pending requests by subcategories: new users, service packages, and site code.
  - **New Users:** Clicking the link quickly opens the **Home > My Tasks** page for the New User Requests and from this page, the administrator can address pending new user requests. See [“New user requests” on page 178](#).
  - **Service Packages:** Clicking the link quickly opens the **Home > My Tasks** page for the Service Package Requests from users and from this page, the administrator can address pending service package requests. See [“Service package requests by users” on page 180](#).
  - **Site Code:** Clicking the link quickly opens the **Home > My Tasks** page for the Claim requests from users and from this page, the administrator can address pending claim requests. See [“Claim code requests by users” on page 183](#).

## 1.5 How do I log out of IAM Administration?

### To sign out

1. Click the my profile icon in the header area of the Home page. The icon shows first letters of your first and last name, for example .
2. Click **Signout**.

## 1.6 Roles and permissions

User access to various modules in IAM Administration is determined by the roles that are assigned to a user profile. Each role is made of a group of permissions that determine which modules users can access and use. Some roles have more permissions and more access to IAM modules. See [“Administrator Roles” on page 189](#).



## Chapter 2

# Organization and User Registration

Administrators can register their organization or themselves as a user with IAM Administration. In IAM Administration, administrator users can create an Organization and select packages in order to register themselves in an Organization with relevant package access.

**New organization registration:** Top-level organizations (TLO) tie groups of users, service packages, and site codes together. After an organization is created, the administrator can create divisions to further segregate users into user groups that are managed by local division administrators, forming a hierarchy. When a new organization is created, a security administrator must also register and be assigned.

**New user registration:** After an organization is registered and approved, users can be added to it in various ways, such as, by addition from inside the organization, by invitation, or using walk-up registration to request access to a portal and its service packages. A service package is a grantable container that contains at least one application or tool accessed through IAM Administration. By requesting a service package, you can obtain access to additional applications. Some service packages contain subpackages.

## 2.1 Registration by Invitation

### 2.1.1 Inviting TLO to register


Administrators can invite top-level organizations (TLO) to register with IAM Administration.

There are three parts to the TLO invitation through the invitation process in IAM Administration:

- First, an IAM administration exchange operator sends an email invitation to the prospective security administrator of a top level organization to register their organization with IAM Administration.
- Second, the prospective security administrator receives the email invitation and proceeds to complete the registration. The exchange operator is also notified with an email about the request submission.
- Third, the IAM administration exchange operator receives a new organization request which they can approve or reject.

The three parts are described here.

**(For IAM Exchange Operator) To invite Top-Level Organization to register**

1. In the IAM Administration page, click the main menu  and in the navigation pane, click **Invite**.
2. In the Invitation page, click **Top level organization** to indicate who you want to send the invitation to.

The contents of the page get updated based on the selection. The Subject field shows default text that asks the invitation recipient to complete their profile and company registration.

The Choose Division field shows the division name of the current organization. The Service Packages section lists all the packages available in the selected division of the organization.

3. In the **Recipient Email** box, type the email address of the prospective security administrator of the TLO who you are inviting to register their organization. You can add up to 20 email addresses separated by commas or semicolons to invite multiple TLOs to register. Instead of typing multiple email addresses, you can also do the following:

- Click **Upload**  adjacent to the **Recipient Email** box to select a csv file containing the email addresses.

4. In the **Template** field, click the arrow  and from the list select one of the two options: **Template\_TLO\_Plaintext** or **Template\_TLO\_HTML**.

The invitation text in the Message box is updated based on the selection in the Template field. The invitation text cannot be edited.

5. In the **Service Packages** box, click the check box for the service packages you want to grant to the invited TLO. Only 10 packages can be selected.
6. Click **Send Invitation**.

Successfully sent invitation message is shown.

The email recipient would receive the email and then using the link in the email would proceed to complete their profile and company registration.




The invited prospective Security Administrator for the TLO receives the email invitation to register the organization and join the OpenText™ Cloud.

As a TLO or division Security Administrator, use the following procedure to register your organization.

**(For TLO or division security administrator) To register your organization**

In your Email Client, you would receive an invitation email with Subject “Action required: Complete your profile and company registration” from IAM Administration.



1. In the email, click the link to initiate the registration process.  
An instance of the IAM Administration opens in your browser. You are informed that you are registering as the Security Administrator and the responsibilities of the role are displayed.
2. Read the information provided about the Security Administrator role and if you want to accept the role and responsibilities, click **I Accept**. To decline, you can click **Do no accept**.  
On accepting the role, the organization registration wizard displays the Welcome page and takes you through the required steps for registration and account creation.
3. In the Organization Information page, provide the following details. The required fields are marked with an asterisk.
  - a. **Organization Name:** Provide a unique name for your organization and click on **Check for availability** to see if the name is available for use.  
A check mark with the word Available indicates you can use this name for your organization.
  - b. **Address:** Provide the organization address using all the address boxes if needed.
  - c. **City, State, Country, and Postal Code:** Provide the names of the city, province, country, and postal code.
  - d. Click **Next**.
4. In the Login and Personal Information page, provide the following details. The required fields are marked with an asterisk 
  - a. In the Login Details section, provide the following information:
    - i. **User ID:** Provide a unique user ID and click on **Check for availability** to see if the name is available for use.  
A check mark with the word Available indicates you can use this name for your organization.
    - ii. **Password:** Provide a password according to the password rules. To see the rules, point the mouse cursor to the  icon adjacent to **Retype Password**.
    - iii. **Retype Password:** Type your password again.
  - b. In the Personal Details section, provide your first and last name, address, city, province, country, postal code, email address, and phone number.  
Point the cursor to the  icon to see helpful additional information.
  - c. Click **Next**.
5. In the Application Packages page, the page shows the name of the service package that was selected in the invitation page. Do the following on the page:

- a. Click the arrow ▼ to expand the Application package details section. It shows the package name and the organization name that granted the package.
  - b. In the **Claim Code** field, type the claim value ID associated with the package.
  - c. Click **Next**.
6. The Summary page shows a summary of all the information entered in the previous steps.

If external call is configured for the requested package, you might be redirected to an external website to enter the claim value ID. After the value is entered, you will be redirected back to IAM Application.

Click **Submit** after you have checked all the information on the summary page.


Registration request submitted successfully message is shown. You can close this tab.

Appropriate administrator would receive the request for registration and would either approve or decline it as needed. See [“To manage the registration request” on page 35](#). For a new TLO registration, exchange operator of IAM Administration would receive the request for approval. For a new division registration, the security administrator of the TLO or division where the invited division would be registered, receives the request for approval.

## 2.1.2 Inviting division to register

Administrators can invite divisions to register in the current organization or under divisions in the current organization.


### To invite a division to register

1. In the IAM Administration page, click the main menu  and in the navigation pane, click **Invite**.
2. In the Invitation page, click **Division** to indicate who you want to send the invitation to.

The contents of the page get updated based on the selection. The Subject field shows default text that asks the invitation recipient to complete their profile and division registration.

The Choose Division field shows the name of the current organization. The Service Packages section lists all the packages granted to the current organization.

3. In the **Recipient Email** box, type the email address of the user who would be registered as the first user of the division to be registered and would be assigned the security administrator role for the division. You can add up to 20 email addresses separated by commas or semicolons to invite multiple users to register their division. Instead of typing multiple email addresses, you can also do the following:

- Click **Upload**  adjacent to the **Recipient Email** box to select a csv file containing the email addresses.




**Note:** If multiple email addresses are added, all the invited users become the default security administrator for their division.

4. In the **Template** field, click the arrow  and from the list select one of the two options: **Template\_Div\_Plaintext** or **Template\_Div\_HTML**.


The invitation text in the Message box is updated based on the selection in the Template field. The invitation text cannot be edited.

5. Leave the current organization name selected in the Choose Division field if you want to register the invited division under the current organization.

To register the invited division under another division of the current organization, in the **Choose Division** field, click the arrow  and from the list select the division where you want the invited division to register. You can also do the following:

- Click the organization hierarchy icon  adjacent to the Choose Division field.

The Select Division dialog box opens.

- i. Select a division or click the arrow  next to a division to navigate to the subdivisions of the division and select a subdivision.
- ii. Click **Apply**

The selected division displays in the Choose Division field. All the service packages that are granted to the selected division are listed in the Service Packages box.

6. (Optional) In the **Service Packages** box, click the check box for the service packages you want to grant to the invited division. Only 10 packages can be selected
7. Click **Send Invitation**.

Successfully sent invitation to recipients message is shown.

#### What happens next?

- The email recipient would receive the email and then using the link in the email would proceed to complete their profile and division registration. See [“\(For TLO or division security administrator\) To register your organization” on page 16](#).
- The TLO or division security administrator of the TLO or division will receive an email regarding the pending division registration request. The administrator can approve or decline the request. See [“To manage the registration request” on page 35](#).

- (Optional) The administrator can grant service packages and modify user roles.


### 2.1.3 Inviting users to register

Administrators can invite users to register with their organization or a division of their organization. When inviting a user to register with a division, it is important to correctly specify the division in which you want the user to belong.

Security Administrators of a division in an organization can view all the users in their organization.

Security Administrators of an organization, TLO or division, can invite new users to register in their organization's hierarchy.

#### To invite users to register

1. In the IAM Administration page, click the main menu  and in the navigation pane, click **Invite**.

In the Invitation page, you would have needed to select the User tab to start the process of inviting users to register. User is selected by default in the Invitation page.

The Subject field shows default text that asks the invitation recipient to complete their registration.


2. In the **Recipient Email** box, type the email address of the users you are inviting to register to a selected division. You can add up to 20 email addresses separated by commas or semicolons to invite multiple users to register. Instead of typing multiple email addresses, you can also do the following:


- Click **Upload**  adjacent to the **Recipient Email** box to select a csv file containing the email addresses.

3. In the **Template** field, click the arrow  and from the list select one of the two options: **Template\_User\_Plaintext** or **Template\_User\_HTML**.


The invitation text in the Message box is updated based on the selection in the Template field. The invitation text cannot be modified.

4. Leave the current organization name selected in the **Choose Division** field if you want to register the invited user under the current organization.

To register the invited user under another division of the current organization, in the **Choose Division** field, click the arrow  and from the list select the division where you want the invited user to register. You can also do the following:

- Click the organization hierarchy icon  adjacent to the Choose Division field.

The Select Division dialog box opens.

- i. Select a division or click the arrow  next to a division to navigate to the subdivisions of the division and select a subdivision.
- ii. Click **Apply**

The selected division displays in the Choose Division field. All the service packages that are granted to the selected division are listed in the Service Packages box.

5. (Optional) In the **Service Packages** box, click the check box for the service packages you want to grant to the invited users. Only 10 packages can be selected
6. Click **Send Invitation**.  
Successfully sent invitation to recipient message is shown.



#### What happens next?

- The email recipients would receive the email and then using the link in the email would proceed to complete their profile and division registration.
- The security administrator will receive an email regarding the user's pending request after the user submits the registration request. The administrator can approve or decline the user request. See [“Managing by invitation user registration request” on page 21](#).
- (Optional) The administrator can grant service packages and modify user roles.

### 2.1.3.1 Managing by invitation user registration request

The security administrator will receive an email regarding the user's pending request after the user submits the registration request. The administrator can approve or decline the user request.

#### To manage the user registration request

1. Log into IAM Administration as an exchange operator or security administrator responsible for the organization.
2. On the home page, on the **User Requests** tile, click **New Users**. Alternatively, you could click the main menu icon  > **My Tasks**. See [“My Tasks Module – Manage Organization and User Requests” on page 165](#).
3. In the Home > My Tasks page for user requests, open the Refine by pane by clicking the Filter icon  and use one or more of the options on the pane to find the new user request that you want to manage. See [“Filter new user requests” on page 178](#).  
The new user request displays in the page.
4. Click the user request record you want to manage in the list on the page.

The Request: New user dialog box opens and displays the person details of the user and the request details. See [“View, approve, or reject new user requests” on page 179](#).

5. To approve the request, the **Approve** action needs to be selected. In this case it is selected by default. If you want to decline the request, just click **Reject**.
6. In the **Reason** box, provide the reason for approving. In case of request rejection, provide a reason for rejecting the request.
7. If the new user registration request also includes service packages, they are available in the Included requests section. Approve or reject as needed and provide a reason.
8. Click **Submit**.

You have successfully submitted your decision message displays. The new user request also no longer displays on the page.

## 2.1.4 Assigning B2B Connect Service Package during TLO registration


Exchange Operators can invite TLOs to register in IAM Administration and assign them B2B Connect service package. The B2B Connect service package has a specific attribute setting to identify it as such.

B2B Connect service package request is only available for TLO registrations. It is not available for division or user registrations.

There are three parts to assigning B2B Connect service package through the TLO registration invitation process:

- First, the security administrator of the TLO is sent an email invitation to register.
- Second, the security administrator receives the email invitation and proceeds to complete the registration.
- Third, the IAM administration exchange operator receives the security administrator’s request for the service package which they can approve or reject.

### To invite a TLO for registration and assign a B2B Connect service package

1. In the IAM Administration page, click the main menu  and in the navigation pane, click **Invite**.
2. In the Invitation page, click **Top level organization** to indicate who you want to send the invitation to.

The contents of the page get updated based on the selection.

3. In the **Recipient Email** box, type the email ID of the security administrator of the TLO being registered and requesting a B2B Connect service package.

4. In the **Template** field, click the arrow ▼ and from the list select one of the two options: **Template\_TLO\_Plaintext** or **Template\_TLO\_HTML**.
5. In the **Service Packages** box, click the check box for the requested B2B Connect service package.
6. Click **Send Invitation**.  
Successfully sent invitation to one recipient message is shown.





#### What happens next?

- The security administrator for the TLO receives the email invitation to register the organization and join the OpenText™ Cloud. See “(For TLO Security administrator) To register your organization and get access to a B2B Connect service package” on page 23.
- The security administrator will receive an email regarding the organization's pending request after the TLO submits the request. The administrator can approve or decline the TLO request. See “View , approve, or reject service package requests” on page 170.




#### (For TLO Security administrator) To register your organization and get access to a B2B Connect service package

In your Microsoft Outlook, you would receive an invitation email with Subject “Action required: Complete your profile and company registration” from IAM Administration.

1. In the email, click the link to initiate the registration process.  
An instance of the IAM Administration opens in your browser. You are informed that you are registering as the security administrator and the responsibilities of the role.
2. Read the information provided about the Security Administrator role and if you want to accept the role and responsibilities, click **I Accept**. To decline, you can click **I do not accept**.  
On accepting the role, the organization registration wizard displays the Welcome page and takes you through the required steps for registration and account creation.
3. In the Organization Information page, provide the following details. The required fields are marked with an asterisk.
  - a. **Organization Name:** Provide a unique name for your organization and click on **Check for availability** to see if the name is available for use.  
A check mark with the word **Available** indicates you can use this name for your organization.
  - b. **Address:** Provide the organization address using all the address boxes if needed.

- c. **City, State, Country, and Postal Code:** Provide the names of the city, province, country, and postal code.
  - d. Click **Next**.
4. In the Login and Personal Information page, provide the following details. The required fields are marked with an asterisk.
  - a. In the Login Details section, provide the following information:
    - i. **User ID:** Provide a unique user ID and click on **Check for availability** to see if the name is available for use.  
A check mark with the word Available indicates you can use this name for your organization.
    - ii. **Password:** Provide a password according to the password rules. To see the rules, hover the mouse cursor over the  icon adjacent to **Retype Password**.
    - iii. **Retype Password:** Type your password again.
  - b. In the Personal Details section, provide your first and last name, address, city, province, country, postal code, email address and phone number.  
Point the cursor to the  icon to see helpful additional information.
  - c. Click **Next**.
5. In the Application Packages page, the page shows the name of the B2B Connect service package that was selected in the invitation page. Do the following on the page:
  - a. Click the arrow  to expand the Application package details section. It shows the package name and the organization name that granted the package.  
If the B2B Connect service package has claim associated with it, then along with B2B attribute text field, claim code field will also be displayed. If claim is not associated, then only B2B attribute text field will be displayed
  - b. If the **Claim Code** field is displayed, type the claim value ID associated with the package.
  - c. Click **Next**.
6. In the Legal Service Agreement page, scroll the legal service agreement and read it. Do the following:
  - a. To download the agreement as a pdf file, click the **Download** icon . In the pdf file dialog box, either choose to open the pdf or save it and then click **OK**. If open was selected, the pdf opens in Adobe Acrobat Reader.
  - b. Click **I accept & next** to accept the agreement and move to the next step. If you don't agree with the agreement, click **I do not accept**.



7. The Legal Rate Schedule page shows the rate schedule and some additional details. Scroll the page to see the information on the page. The following details are available on the page:
  - a. Name, description, minimum, maximum, frequency, Unit of Measure (UoM), and currency. Point the cursor to the **Frequency Code** icon  to open a box to see information about interpreting the frequency codes. The codes consist of three characters: the first letter represents the frequency, the second character represents if the item is billed at the start or end of the billing cycle, and the third character represents if the item is fixed or variable.
  - b. **Currency switch** : Click the switch to change between USD and EURO. The currency in the Description column is updated based on the switch setting.
  - c. Click the **Download** icon  to download the rate schedule as a PDF.
  - d. After reviewing the information on the page, if you agree with it, click **I accept & next** to accept the agreement and move to the last step in the registration process.
8. The Summary page shows a summary of all the information entered in the previous steps including the legal service agreement and the rate schedule. You can download the legal service agreement and the rate schedule using the Download icons in those sections of the Summary page. Click the **Submit** button after you have carefully read and checked the agreements.

Registration request submitted successfully message is shown. You can close this tab.

After the registration is complete and you are granted the B2B service package, you can use your credentials to log into your newly registered organization in IAM Administration and access the assigned B2B Connect service package. You can grant access to this service package to other users in your organization if needed.

Appropriate administrator of the B2B service package owning organization would receive the service package request and would either approve or decline it as needed. See [“View , approve, or reject service package requests” on page 170.](#)





## 2.1.5 Inviting existing TLO to register for a B2B service package

Exchange Operators can invite existing TLOs to register and request for a B2B Connect service package. The B2B Connect service package has a specific attribute setting to identify it as such.

There are three parts to inviting existing an TLO to register for a B2B Connect service package:

- First, the security administrator of the existing TLO is sent an email invitation to register.
- Second, the security administrator receives the email invitation and proceeds to complete the registration.
- Third, the IAM administration exchange operator receives the security administrator's request for the service package which they can approve or reject.

### To invite a existing TLO security administrator to register for a B2B service package

1. In the IAM Administration home page, click the main menu  to open the navigation pane.
2. Click **Manage Organization**.  
The Home > <top level organization name> page opens.
3. Click the **Service Packages** tab and find the B2B service package on the page.  
The B2B service package is indicated by this icon in the UI .
4. Click the **Invite** icon  in the Action column for the B2B service package.  
The package invitation page opens. To invite a TLO, make the Top level organization option is selected by default.
5. Click **Select Top Organization** under the Top level organization field.
6. In the Top level organization page, click **Search**  to find the organization you want to invite to register for the B2B service package.
  - a. In the Enter keyword field, type the name of the organization you want and click **Search**  
Matching organization names are displayed in the search result.
  - b. Click the organization you want and click **Add**.  
The selected organization name displays in the Top level organization field.
7. Click **Select User** under the Security admins field.

- In the User List page, select the security administrator to whom you want to send the invite and click **Add**.

The selected security administrator's name displays in the Security admins field.

8. Click **Send Invitation**.

Invitation sent successfully message displays.

**What happens next?**

- The security administrator of the TLO would receive the email invite and then using the link in the email would proceed to complete B2B service package request process. See [“\(For invited TLO security administrator\) To register for the requested DOD service package” on page 30](#).
- The security administrator of the owning organization will receive an email regarding the organization's pending request after the TLO submits the request. The administrator can approve or decline the user request. See [“View , approve, or reject service package requests” on page 170](#).

**(For invited TLO security administrator) To register for the requested B2B service package**

In your Microsoft Outlook, you would receive an invitation email with a link to initiate the request for B2B service package.

1. In the email, click the link to initiate the request process.

An instance of the IAM Administration opens in your browser. You are informed that you are about to request for invite-based package. The B2B service package name is shown with an asterisk \* and an arrow > .

2. Click the arrow > .


The page to start the package request process opens. It displays a progress bar to show different stages of the request process. In the Application Packages stage, the B2B service package details are shown, such as service package and owning organization name, package description and associated attributes.




3. In the field with the asterisk \* , enter the claim ID associated with the package.
4. In **Request Reason** box, enter a reason for requesting the service package.
5. If applicable, click the **Accept the terms and conditions** button, and then in the terms and conditions box, click **I Accept**.

I have read and accepted terms and conditions message displays.

6. Click **Next** to move to the next stage in the process.

The Legal Service Agreement page opens.

7. In the Legal Service Agreement page, scroll the legal service agreement and read it. Do the following:
  - a. To download the agreement as a pdf file, click the **Download** icon . In the pdf file dialog box, either choose to open the pdf or save it and then click **OK**. If open was selected, the pdf opens in Adobe Acrobat Reader.
  - b. Click **Accept & Next** to accept the agreement and move to the next step. If you don't agree with the agreement, click **Do Not Accept**.

The Legal Rate Schedule page opens.
8. The Legal Rate Schedule page shows the rate schedule and some additional details. Scroll the page to see the information on the page. The following details are available on the page:
  - a. Name, description, minimum, maximum, frequency, Unit of Measure (UoM), and currency description. Point the cursor to the **Frequency Code** icon  to open a box to see information about interpreting the frequency codes. The codes consist of three characters: the first letter represents the frequency, the second character represents if the item is billed at the start or end of the billing cycle, and the third character represents if the item is fixed or variable.
  - b. **Currency switch** : Click the switch to change between USD and EURO. The currency in the Description column is updated based on the switch setting.
  - c. Click the **Download** icon  to download the rate schedule as a PDF.
  - d. After reviewing the information on the page, if you agree with it, click **Accept & Next** to accept the agreement and move to the last step in the registration process.
9. The Summary page shows a summary of all the information entered in the previous steps including the legal service agreement and the rate schedule. You can download the legal service agreement and the rate schedule using the Download icons in those sections of the Summary page. Click the **Submit** button after you have carefully read and checked the agreements.

Registration request submitted successfully message is shown. You can close this tab.

After the registration is complete and you are granted the B2B service package, you can grant access to this service package to other users in your organization if needed.

### What happens next?





Appropriate administrator of the B2B service package owning organization would receive the B2B service package request and would either approve or decline it as needed. See ["View , approve, or reject service package requests"](#) on page 170.

## 2.1.6 Inviting TLO to register for a DOD service package

A supplier organization may request for a DOD service package. The service owner or the exchange operator of the organization with the DOD service package can invite a security administrator of the supplier organization to register for the requested DOD service package.

The exchange operator and security administrator can also invite a division to register for a DOD service package.

### To invite a TLO security administrator to register for a DOD service package

1. In the IAM Administration home page, click the main menu  to open the navigation pane.
2. Click **Manage Organization**.  
The Home > <top level organization name> page opens.
3. Click the **Service Packages** tab and find the DoD service package on the page.  
The DOD service package is indicated by this icon in the UI .
4. Click the **Invite** icon  in the Action column for the DOD service package.  
The package invitation page opens. To invite a TLO, make sure the Top level organization option is selected. Its the default selection in this case.
5. Click **Select Top Organization** under the Top level organization field.
6. In the Top level organization page, click **Search**  to find the organization you want to invite to register for the DOD service package.
  - a. In the Enter keyword field, type the name of the organization you want and click **Search**  
Matching organization names are displayed in the search result.
  - b. Click the organization you want and click **Add**.  
The selected organization name displays in the Top level organization field.
7. Click **Select User** under the Security admins field.
  - In the User List page, select the security administrator to whom you want to send the invite and click **Add**.  
The selected security administrator's name displays in the Security admins field.
8. Click **Send Invitation**.  
Invitation sent successfully message displays.

### What happens next?

- The email recipient would receive the email invite and then using the link in the email would proceed to complete DOD service package request process. See “(For invited TLO security administrator) To register for the requested DOD service package” on page 30.
- Appropriate administrator of the DOD service package owning organization would receive the DOD service package request and would either approve or decline it as needed. You will need to click the **Attestation Content** button and accept the attestation as part of approving request for the DOD service package. See “View , approve, or reject service package requests” on page 170.

### **(For invited TLO security administrator) To register for the requested DOD service package**




In your Microsoft Outlook, you would receive an invitation email with a link to initiate the request for DOD service package.

1. In the email, click the link to initiate the registration process.  
An instance of the IAM Administration opens in your browser. You are informed that you are about to request for invite-based package. The DOD service package name is shown with an asterisk \* and an arrow > .
2. Click the arrow > .  
The page to start the package request process opens. It displays a progress bar to show different stages of the request process. In the Application Packages stage, the service package name and owning organization name are shown. You can click **Show Attributes** to see the related attributes for organization and user.
3. In **Request Reason** box, enter a reason for requesting the service package.
4. If applicable, click the **Accept the terms and conditions** button, and then in the terms and conditions box, click **I Accept**.  
I have read and accepted terms and conditions message displays.
5. Click **Next** to move to the next stage in the process.  
The Attestation page opens. It shows the DOD package attestation agreement. Read the agreement and take the next step as needed.
6. Click **Accept & Next** to accept the attestation agreement and then move to the next stage in the process.  
The summary page opens summarizes the previous steps in the process. Review the content on this page and then take the next step.
7. Click **Submit**.  
Request submitted successfully message is shown. You can close this tab.
8. Click **OK**.

## 2.1.7 Inviting user to register for DOD service package

After a supplier organization is granted access to a DOD service package, it can invite its users to request for the package. The service owner or exchange operator and security administrator of the organization with the DOD service package grant can invite users.

### To invite a user to register for a DOD service package

1. In the IAM Administration home page, click the main menu  to open the navigation pane.
2. Click **Manage Organization**.  
The Home > <top level organization name> page opens.
3. Click the **Service Packages** tab and find the DoD service package on the page.  
The DOD service package is indicated by this icon in the UI .
4. Click the **Invite** icon  in the Action column for the DOD service package.  
The package invitation page opens.
  - To invite a user, click the **User** option.  
The Organization Name field shows the current organization name.
5. Click **Select User** under the Users list field.
  - In the User List page, using the Filter icon, find and select the user to whom you want to send the invite and click **Add**.  
The selected user's name displays in the Users list field.
6. Click **Send Invitation**.  
Invitation sent successfully message displays.


### What happens next?

- The email recipient would receive the email invite and then using the link in the email would proceed to complete DOD service package request process.
- Appropriate administrator of the DOD service package owning organization would receive the DOD service package request and would either approve or decline it as needed. You will need to click the **Attestation Content** button and accept the attestation as part of approving request for the DOD service package. See [“View, approve, or reject service package requests from users” on page 182.](#)

## 2.2 Walk-in Registration

### 2.2.1 Walk-in Organization Registration

You can submit a request to register your organization as a new top level organization (TLO) in IAM Administration using its walk-in registration feature. As the first person to register your organization, you would be automatically designated as the security administrator for your organization.

 **Note:** Before starting the registration process, the registrant should know which portal, organization, or service they are registering for. If the service requires supplier codes or site codes, the registrant should have this information available.

#### To register your organization as a new TLO organization in IAM Administration

1. Open the IAM Administration in a supported browser window using the URL provided by your customer.
2. Click the **New User? Register Here** link.

The OpenText Identity and Access Management page opens. The new account creation wizard displays the Welcome message and will take you through all the steps of registering your organization as new.

3. On the Organization Information page, click **Search**.

To select a different language, click  and select another language from the list.

The page displays a list of organizations. On this page, you can start to create a new organization.

4. Provide information related to the organization you want to register. Do the following:

- a. Click **Create Organization**.

A message confirms if you want to continue with creating a new organization. Click **Yes**.

Part of the page displays a message that you are registering as the security administrator of the new organization that you are creating and the responsibilities of the role.

- b. Read the information provided about the Security Administrator role and if you want to accept the role and responsibilities, click **I Accept**. To decline, you can click **Do Not Accept**.



To select a different language, click  and select another language from the list.



On accepting the role, the Organization Information page is updated and displays fields to gather organization-related information. Do the following:

- i. In the **Organization Name** field in the Organization Details section, type a unique name for the new organization.
  - ii. In **Address**, provide the organization address using all the address boxes if needed.
  - iii. In **Country, State, City, and Postal Code** fields, provide the names of the country, province, city, and postal code that comprise the new organization's address.
  - iv. Click **Next**.
5. On the Login and Personal Information page, provide the login details and personal details for the security administrator user being registered along with your new organization.

All the required fields are marked with an asterisk.

- a. In the Login Details section, provide the following information:
    - **User ID:** Provide a unique user ID and click on **Check for availability** to see if the name is available for use.  
A check mark with the word **Available** indicates you can use this name for your organization.
  - b. **Password:** Provide a password according to the password rules. To see the rules, point the mouse cursor to the  icon adjacent to **Retype Password**.
  - c. **Retype Password:** Type your password again.
  - d. In the Personal Details section, provide your first and last name, address, city, province, country, postal code, email address, and phone number.  
Point the mouse cursor to the  icon to see helpful additional information.
  - e. Click **Next**.
6. On the Select Packages page, select the service packages to request for your organization.

The page displays a list of requestable service packages and following details about the service packages: Name, Owner Organization, Category, and description about the service package. The list of the service packages can be sorted by clicking the Name column name. Do the following:

 **Tip:** All the required fields are marked with an asterisk.

If you don't know additional details such as claim value ID (site code/location code) about the requested service packages, you can skip selecting them on this page. Service packages can be requested after the registration is complete.

- a. Click the check box adjacent to the service package name to select it.

The number of selected service packages **Selected 4** is shown in the heading of the list of service packages on the page.

- b. You can also click the check box adjacent to the **Name** column name to select all the service packages on the Select Packages page.
7. Click **Next**.
  8. On the Application Packages page, you need to provide details about the service packages selected in the previous step. The page lists all the selected service packages in individual sections that you can collapse or expand by clicking the arrow in each section. If service packages were not selected on the previous page, this page informs the user about that and asks to provide a reason for the request.



**Tip:** All the required fields are marked with an asterisk.

Do the following on the page:

- a. In the required field for each listed service package, provide the required value. For example, if the required field is **Claim Code**, then provide the claim value ID in the fields for each listed service package.

A claim value ID (site code/location code) is needed to forward your request to the appropriate administrator for review and approval. If you do not know the claim value ID number for the requested service package, inquire about it in your organization such as sales staff, finance staff, or your customer organization that issues the claim value ID.

Some requested service packages require user agreement to their terms & conditions. You would need to accept the terms & conditions in order to proceed. If you do not want to accept, you will need to clear the selection for such a service package on the previous page.
  - b. In the **Request Reason** box, provide a reason for making this request for registering the new organization and the user. Provide enough details to assist the approving administrator in processing your request.
  - c. Click **Next**.

If there are errors in your input, an error message is shown and the fields with error are marked. Fix the errors in order to move forward in the registration process.

Click **Previous** to go back to the previous page to make changes or deselect any or all of the service packages you had selected.
9. On the Summary page, you can see and verify all the information you provided in all the previous pages. You can click **Previous** to go back to previous pages and make changes if needed.
  10. Click **Submit** to submit your registration request.

A message informs that your registration request was successfully submitted.

If the requested service packages and services are approved, they are granted and assigned to the organization but are not automatically granted to the organization's security administrator. To access and use these services, the newly approved administrator can grant the approved services to anyone in the organization, including themselves.



The Exchange operator for IAM Administration would receive the request for registration and would either approve or decline it as needed. See [“Managing walk-in organization registration request” on page 35](#).

You can also check the status of your registration request using the registration status link located on the IAM Administration login page.

## 2.2.2 Managing walk-in organization registration request

As the administrator of a portal, you would receive email notifications about the pending walk-in registration requests from users who want to register their organization and themselves as the security administrator of that organization. You can review the request and then either approve or decline the requests as needed. To manage the requests in IAM Administration, use the following procedure:

### To manage the registration request

1. Log into the IAM Administration as an exchange operator for TLO registration requests or as a security administrator for division registration requests.
2. On the home page, on the **Organization Requests** tile, click **New Organizations**.  
Alternatively, you could click the main menu  > **My Tasks**. See [“My Tasks Module – Manage Organization and User Requests” on page 165](#).
3. In the Home > My Tasks page for organization requests, open the Refine by pane by clicking the Filter icon  and use one or more of the options on the pane to find the new organization request that you want to manage. See [“Filter new organization requests” on page 167](#).  
The new organization request displays in the page.
4. Click the organization name in the list on the page.  
The Request: New Organization dialog box opens and displays the details of the new organization request and the requesting administrator details. See [“View, approve, or reject new organization requests” on page 168](#).
5. To approve the request, the **Approve** action needs to be selected. In this case it is selected by default. If you want to decline the request, just click **Reject**.
6. In the **Reason** box, provide the reason for approving. In case of request rejection, provide a reason for rejecting the request.
7. If the new organization registration request also includes service packages, they are available in the Included requests section. Approve or reject as needed and provide a reason.

8. Click **Submit**.



You have successfully submitted your decision message displays. The new organization request also no longer displays on the page.

The user who submitted the request for registration would receive an email notification informing them if their request was approved or rejected.

### 2.2.3 Managing walk-in user registration request

As the administrator of a portal, you would receive email notifications about the pending walk-in registration requests from users who want to register themselves as a user in an existing organization. You can review the request and then either approve or decline the requests as needed. To manage the requests in IAM Administration, use the following procedure:

#### To manage the user registration request

1. Log into the IAM Administration as an exchange operator.
2. On the home page, on the **User Requests** tile, click **New Users**. Alternatively, you could click **Menu**  > **My Tasks**. See “[My Tasks Module – Manage Organization and User Requests](#)” on page 165.
3. In the Home > My Tasks page for user requests, open the Refine by pane by clicking the Filter icon  and use one or more of the options on the pane to find the new user request that you want to manage. See “[Filter new user requests](#)” on page 178.  
The new user request displays in the page.
4. Click the user name in the list on the page.  
The Request: New user dialog box opens and displays the personal details of the new user and the request details. See “[View, approve, or reject new user requests](#)” on page 179.
5. To approve the request, the **Approve** action needs to be selected. In this case it is selected by default. If you want to decline the request, just click **Reject**.



**Note:** Selecting Reject for the request would also reject all the included requests from the request queue.

6. In the **Reason** box, provide the reason for approving. In case of request rejection, provide a reason for rejecting the request.
7. If the Included requests section has additional packages or claims, click **Approve** or **Reject** as needed, and provide a reason for rejecting the package or claim.
8. Click **Submit**.



You have successfully submitted your decision message displays. The new user request also no longer displays on the page.

The user who submitted the request for registration would receive an email notification informing them if their request was approved or rejected.

## 2.3 Post registration

After users' request for registration is approved, users need to activate their account by logging in to the application using their credentials and completing their personal information section if needed, security configurations, and email preferences.

### To access the Profile module

1. Log into the IAM Administration application using your credentials.  
You are logged into the IAM Administration application but before you can begin to use the application, you are required to complete your personal information, configure the security settings, and email preferences in a new page. Sections with complete information display a check mark  and the sections that need to be completed display an asterisk .
2. Click the section with the asterisk to open and complete it. Clicking any of the sections opens the related tab on the My Profile page.  
After you have completed all the sections, you are shown the Home button.
3. Click **Home** to begin to use the application.



## Chapter 3

# Managing your profile details

## 3.1 Managing my personal information

You can manage your personal information, change your password, and set up language, time zone, and email preferences using the My Profile option in IAM Administration. You can also see the roles granted to your profile.



**Note:** What you see in the user interface is determined by the role and permissions assigned to your profile. The user interface elements, such as fields, labels, and tooltips, that you see in IAM Administration for your organization might be different from the descriptions in the Help and the guide because this application can be configured to suit the needs of any organization.

### To access my profile in IAM Administration


1. Click the my profile icon in the header area of the Home page. The icon shows first letters of your first and last name.
2. Click **My Profile** in the list.

The My profile page opens and displays the following tabs: Account Info, Security, Preferences, and Roles.

### 3.1.1 Account Info tab

The Account Info tab in the My Profile page displays personal details of the currently logged in user:

- **Account Status:** Indicates the status of your account, Active or otherwise.
- **Last Login:** Shows the date and time for your last login in IAM Administration.
- **Password Change Log:** Click **Open** to view your password change history. Password Change Log opens in a new page and lists the following information for every time your password was changed: date and time of password change, event type, user who performed this action, and any notes if available. Click **X** to close the page and go back to Account Info tab.
- **Organization Name:** Displays the name of the organization you belong to. The value in the field cannot be edited.
- **Personal Details** area: Displays your First and Last Names, User Id, Address, City, State, Country, Postal code, Email address, and Phone number. All the fields with asterisk \* are required. The value in the User Id field cannot be

edited. Point to  besides the Phone field to see additional information about the field.





### To edit personal details

- Modify your personal details as needed and click **Save**.  
Clicking **Reset to default** does the following based on certain conditions:
  - If the fields were empty and the user provided data for the first time, then clicking the **Reset to default** button clears the values from the fields.
  - If the fields already contained saved data and the user modified the data but did not save, then clicking the **Reset to default** button would revert the fields to the previously saved data.


## 3.1.2 Security tab

Use the Security tab to reset your password, select security questions and answers, and set 2–step verification for the account.

### To manage your security settings

1. Open the My Profile page using the instructions in *“Managing my personal information” on page 39*.
2. Click the **Security** tab in the My Profile page.  
The tab displays three areas: Password, Security Question, and 2–step verification. The Password area shows the date of last password change.
3. To change your current password, do the following:
  - a. Click the arrow  in the **Password** area to expand it.
  - b. Type your current password in the **Current Password** box.
  - c. Type your new password in the **New Password** field. Point to  besides the **Retype New Password** field to see password requirements.
  - d. Again type your new password in the **Retype New Password** field and click **Submit**.  
Data updated successfully message displays. The Password area shows the current date of password change.
4. To manage security questions, do the following:
  - a. Click the arrow  in the **Security Question** area to expand it.
  - b. To select your first question, click the arrow  in the **Question 1** field and from the list, select an existing question.
  - c. Type the answer for the first question in the **Answer 1** field.




 **Note:** To see the values in the answer fields, click the **Unmask security answers** check box.


- d. To select your second question, repeat the above steps for Question 2.
- e. Click **Save**.

Data updated successfully message displays.


5. To manage 2-step verification, do one of the following configurations:

 **Notes**

- If 2FA (two factor authentication) is configured for an organization, then users of the organization must choose one of the modes described below for their 2-step verification.
- If the 2-step verification is already configured for a user account, the switch is set to ON .

- a. Click the arrow  in the **2-step verification** area to expand it.

The expanded area displays four modes of implementing 2FA: SMS, Phone, Email, and Google Authenticator. You would need to configure one mode for your user account.

 **Note:** You can use only one mode for your profile.

- b. To use the **SMS** mode, see [“SMS mode for 2-step verification”](#) on page 42.
  - c. To use the **Phone** mode, see [“Phone mode for 2-step verification”](#) on page 43.
  - d. To use the **Email** mode, see [“Email mode for 2-step verification”](#) on page 44.
  - e. To use the **Google Authenticator** (GA) mode, see [“Google Authenticator mode for 2-step verification”](#) on page 45.
  - f. Click **Save** after you configure one of the modes to save the settings.
6. If you click **Save** without registering any 2-step verification mode, the system displays the message that you need to select an MFA mode and register it. In this case, click **OK** to close the message and then follow above steps to register any of the four modes to be used for 2-step verification.

### 3.1.2.1 SMS mode for 2-step verification

#### To use the SMS mode

1. With **SMS** selected, click the switch  in the 2-step verification area to enable the SMS option.

The switch moves to the ON state and the SMS area becomes available.


2. As step one, you have to enter a phone number if it is not already shown on the screen and verify the number.

The first **Mobile number** box displays the same phone number from the Phone field on the Account Info tab if the field is populated. If the first **Mobile number** box is empty, enter the phone number where you want the verification code to be sent.

3. Click **Send Passcode** to verify the phone number. The verification code is sent to your phone as a text message.

The **Send Passcode** button changes to **Resend Passcode**. Step 2 for the SMS process displays where you have to enter the OTP (one time password) you received on your phone in the box in step two.


4. To verify your phone number, enter the OTP you received on your phone in the box in Step 2 and click **Validate**.

After the OTP is validated, SMS mode registered successfully messages displays. Verified  and **Remove** are shown next to the phone number. This phone number becomes the primary phone number for this account.

This means that you have set the SMS mode as the chosen 2FA mode for this account.


5. To provide a different number in the first **Mobile number** box, click **Remove** which clears the field and then do the following:

- a. Type the new number in the first **Mobile number** box.
- b. Click **Send Passcode**.

 **Note:** If you change a phone number that was already verified and registered for your account, the system displays a warning that the new phone number is different from the previously registered number and that you need to verify and register this new number.

- c. To proceed with the change, click **Yes** in the warning.

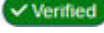
Mobile number updated successfully message displays.

 **Note:** The mobile number is also update on the Account Info tab in the Phone field.

- d. Click **Send Passcode** to verify the new phone number.

The verification code is sent to the new phone number as a text message.

- e. If the code expired, click **Resend Passcode** to receive another verification code on the phone.
- f. After you receive the verification code, enter it in the box in Step 2 on the screen and click **Validate**.

After the OTP is validated, SMS mode registered successfully messages displays. Verified  and **Remove** are shown next to the phone number. This new phone number becomes the primary phone number for this account.

6. To add another phone number to receive the verification code, click **Add Phone number**.

A second mobile number box along with the Send Passcode button is added on the screen.

7. In the second **Mobile number** box, enter an alternate phone number where you would like to receive the verification code, and click **Send Passcode**.

The system displays a message that you have added another phone number which you need to verify and register.


8. Click **Yes** to proceed.

Mobile number updated successfully message displays.

9. Verify the number by clicking **Send passcode** and entering the received OTP and then validating it.

### 3.1.2.2 Phone mode for 2–step verification

#### To use the Phone mode

1. Click **Phone** and then click the switch  in the 2–step verification area to enable the Phone option

The switch moves to ON state and the Phone area becomes available.

2. Configuring the Phone mode is similar to the SMS mode except that the verification code is sent to the verified primary phone number or the alternate phone number as a call.




**Note:** Use the steps in the “SMS mode for 2–step verification” on page 42 to configure the phone mode.

### 3.1.2.3 Email mode for 2-step verification

Users can configure 2-step verification area to implement multi-factor authentication (MFA) for authenticating the user identity during the login process. There are four MFA modes: SMS, Phone, Email, and Google Authenticator. Users can enable only one of the modes for their profile.

#### To use the Email mode

1. Click **Email** and then click the switch  in the 2-step verification area to enable the Email option.  
The switch moves to ON state and the Email area becomes available.
2. If the **Email Id** box is populated, it displays the same email address from the Email field on the Account Info tab. Do the following:
  - a. Click **Send Passcode** to verify the email address.  
The verification code is sent to the email address.
  - b. Go to [Step 6](#).

3. If the **Email Id** box is empty or you want to use a different email address to receive the verification code, enter the email address in the box.
4. Click **Send Passcode** to verify the email address.  
If you change the email address to a value that does not match the email address on the Account Info tab, then a message displays and informs you that this email is different from the registered email address. You will need to regenerate the pass code and verify it. If you want to proceed, click **Yes**.  
Email address updated successfully message displays.



**Note:** The Email address is also updated on the Account Info page.

5. Click **Send Passcode** again to verify the new email address.  
The system emails the verification code to the new email address.
6. Enter the verification code from the email into the **Verify the email id** box and click **Validate**.


Email mode registered successfully messages displays. Verified  and **Remove** are shown next to the email address. This means that you have set Email as the 2FA mode for your profile.

7. Click **Remove** to change the email address.  
The Email Id box is cleared. You can provide another email address for 2-step verification. Follow the above steps to register the new email address for 2FA.  
If you click **Save** to save your changes without verifying and registering the email address, the system displays the message that you need to select an MFA mode and register it. In this case, click **OK** to close the message. Click **Send**

**passcode** and then follow the above steps to verify the code using the verification code.

### 3.1.2.4 Google Authenticator mode for 2–step verification






#### To use the Google Authenticator (GA) mode

1. Click **Google Authenticator** and then click the switch  in the 2–step verification area to enable the GA option  
The switch moves to ON state and the Google Authenticator area becomes available.
2. Follow the onscreen instructions for step 1.
3. Follow the onscreen instructions for step 2 and then click **Validate**.  
GA mode registered successfully message displays. The Google authenticator area shows **Device successfully registered** message and a **Remove** button.
4. Click **Remove** to unregister your device and register another one.  
Device removed successfully message displays.
5. Follow above steps 1 and 2 to register another device for GA mode 2FA.

### 3.1.3 Preferences tab

Use the Preferences tab to configure your language, time zone, and email settings.

#### To configure your preferences

1. Open the **My Profile** page using the instructions in [“Managing my personal information” on page 39](#).
2. Click the **Preferences** tab.
3. In the **Language** field, click the arrow  and select the language of your choice.
4. In the **Time Zone** field, click the arrow  and select the time zone as needed.
5. In the **Email preferences** area, click the arrow  to expand the area and see the various settings. Turn the switch on  or off  for each setting as needed.
6. Click **Save**.
7. Click **X** to close the My profile page.

### 3.1.4 Roles tab

The Roles tab in the My profile page lists the roles granted to the currently logged in user. The page shows the role ID, role name, description, and role grant date.



## Chapter 4

# Reports

Administrators can use this module to access IAM Analytics to create different types of reports.



An exchange operator can upload report templates. See [“To upload a report template” on page 47](#).

### To open IAM Analytics

1. Access IAM Administration application.
2. Click the main menu  to open the navigation pane.
3. Click **Reports** or click the arrow  adjacent to the **Reports** module to expand the menu and then click **Administration Reports**.

IAM Analytics opens in a new browser window.

### To upload a report template

1. Click the main menu  to open the navigation pane.
2. Click the arrow  adjacent to the **Reports** module to expand the menu, and then click **Upload Report Template**.

App Buyer Configuration UI opens in a new browser window.

## 4.1 IAM Analytics

The IAM Analytics window displays reports in following categories: User, Organization, Package, Federation, and Custom. To see reports types in each category, select the category name in the header.



**Note:** Based on your role, you may or may not see all the categories and report types mentioned in the Help.

## 4.1.1 User Reports

User reports consist of the following types:

Report type	Description
User Summary	<p>This report lists all organizations under the realm with number of pending, rejected, active, suspended, inactive, locked, expired, and unactivated users.</p> <p>You can filter the list of users for all the organizations in the realm by user statuses.</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria.</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p>
User Information	<p>This report lists all users in the organization and their basic information. Users can be filtered based on their service package and subpackage grants.</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p> <p>Service administrators can get data from their realm, own organization and its divisions based on the packages they manage.</p>
User Detail	<p>This report lists all users in the organization and their basic information. In addition, the report also provides information about user attributes. Users can be filtered based on their service package and subpackage grants.</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p> <p>Service administrators can get data from their realm, own organization and its divisions based on the packages they manage.</p>



Report type	Description
User Role	<p>This report lists all users with roles based on their personas in the organizations. Users can be filtered based on their service package and subpackage grants and supplier code (claim Id).</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p> <p>Service administrators can get data from their realm, own organization and its divisions based on the packages they manage.</p>
User Service Summary By Organization	<p>This report lists number of users who have access to service packages by organizations.</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p> <p>Service administrators can get data from their realm, own organization and its divisions based on the packages they manage.</p>
User Package Grants	<p>This report lists all users with packages granted to them based on their persona in the organizations.</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p> <p>Service administrators can get data from their realm, own organization and its divisions based on the packages they manage.</p>
User Package Grant Detail	<p>This report lists all users with package grant attributes, package claims, and package claim values granted to them based on their persona in the organizations.</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p> <p>Service administrators can get data from their realm, own organization and its divisions based on the packages they manage.</p>

Report type	Description
User Audit	<p>This report (quarterly user auditor) lists the organizations that have not completed an audit in the last 90 days (based on personas).</p> <p>This report (annual user grant auditor) lists the organizations that have not completed a user grant audit in the last 365 days (based on personas).</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can get package and its grants data for their realm.</p>
Weekly User Status	<p>This report lists all users, in the organizations, whose status changed from last week (based on personas).</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p>
Password Changes	<p>This report lists password change details for all the users whose password changed.</p> <p>You can use the filter criteria Period to specify the date range during which passwords were changed.</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p>

### 4.1.2 Organization Reports

Organization reports consist of the following types:

Report type	Description
Organization Details	<p>This report lists organization details such as organization ID, organization name, address, claims, T&amp;C acceptor, user ID, T&amp;C accepted date for a package (based on personas).</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p> <p>Service administrators can get data from their realm, own organization and its divisions based on the packages they manage.</p>

Report type	Description
Organization Package Grant Details	<p>This report lists organization package grant details such as organization ID, organization name, address, package grant status, granted date and granted by, application name, application ID and claims (based on personas).</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p> <p>Service administrators can get data from their realm, own organization and its divisions based on the packages they manage.</p>
Weekly Organization Status	<p>This report lists organization details such as organization name, top-level organization name and address, where the status of the organizations changed since last week (based on personas).</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p>

### 4.1.3 Package Reports

Package reports consist of the following types:

Report type	Description
Service Summary	<p>This report lists number of users, organizations, and parent supplier codes for a specific or all packages (based on personas).</p> <p>Service Owners can get package and its grants data for their realm.</p> <p>Service administrators can get data from their realm, own organization and its divisions based on the packages they manage.</p>
Registered User Count	<p>This report gives a count of registered users and suppliers depending on the period selected and organization option.</p> <p>Exchange administrators can retrieve data from their realm based on the specified report criteria</p> <p>Security administrators can access data from their own organization and its divisions based on the specified report criteria</p> <p>Service administrators can get data from their realm, own organization and its divisions based on the packages they manage.</p>

## 4.1.4 Federation Reports

Federation reports consist of the following types:

Report type	Description
Federation Count	This report lists number of federations for the selected provider (based on personas).  All types of administrators with access to reports have access to this report type.
Federated User Details	This report lists federated user details for the selected provider (based on personas).  All types of administrators with access to reports have access to this report type.
Federated Process Details	This report lists federated process details for the selected provider (based on personas).  All types of administrators with access to reports have access to this report type.


## 4.1.5 Custom Reports


Based on configuration, some users will also see Custom reports category. Custom reports consist of the following types:

Report type	Description
Affiliated Org Non SAO Administrators Report	This report lists number of federations for the selected provider (based on personas).  All types of administrators with access to reports have access to this report type.
Affiliated Org Non SAO Service Packages Report	This report lists federated user details for the selected provider (based on personas).  All types of administrators with access to reports have access to this report type.
GMSP Weekly Request Report	This report lists federated process details for the selected provider (based on personas).  All types of administrators with access to reports have access to this report type.

## 4.1.6 Working with reports

This section provides generic instructions for creating and exporting or scheduling and downloading different types of reports.

If reports are small and would not take a long time to be generated, use the **Export** option  to download the report if the option is available for the selected report type.

If the reports are big and might take long time to get generated, you have the option to schedule it using the **Schedule** icon  and then when the report is completed and ready to be downloaded, you will get an email notification. You can then proceed to download your report.

### 4.1.6.1 Creating and exporting a report

Use this procedure if you want to create and export a report right away and the Export option is available for the selected report type.

#### To create and export a report

1. Make sure a report category, for example **User Reports** is selected in the header. Also, make sure to select a report type, for example **User Information**, in the first panel.

**Organization Option** is a global filter and is by default set to **All Organizations** for an Exchange operator. The selection in the global filter is applied to all the report types.

The listing page displays information related to the selected report type. The listing page also might show instructions about what you need to do next, such as first use the report filter to filter the information using the specified criteria and schedule the report generation or export the displayed information in a CSV file.




2. For a security administrator, the global filter **Organization Option** can be set to the following options: **My immediate organization only**, which is the logged in security administrator's parent organization and **include all organizations below**, which are all the divisions under the parent organization. Select the option you want from the list and click **Apply**.

The content of the listing page updates based on the organization option selected.

3. Click the **Filters** icon  in the toolbar.


The Filter By pane opens. You can specify criteria to filter the information that you want to include in the report.

4. In the Filter By pane, do the following:

- a. Click the  icon in each category to open a popup to specify criteria as needed. After specifying criteria, click the  icon again to close the popup. Your selections display in the appropriate category box.  
To delete your selections for a category, click **Clear** for that category.
  - b. Provide required values in other fields as needed.
5. Click **Apply** or to set your selection as the default setting, click the arrow  on the Apply button and select **Apply and set as default**.

The listing page is updated and displays the information based on the specified criteria in the Filter By pane..

 **Tips**

- Use **Clear All** to clear out all the selected filters.
  - Click the **Filters** icon again to hide the Filter By pane or click anywhere else in the page.
6. Click the **Export** icon  and then **CSV Document** to export this list into a CSV file.

For some report such as Registered User Count type package report, you can export the report in XLSX and PDF formats.



#### 4.1.6.2 Scheduling report creation

If reports are big and might take long time to get generated, use this procedure to schedule generating reports if the Schedule option is available for the selected report type.

##### To schedule report generation

1. Select the report category in the header area of IAM Analytics page and then in the reports type panel, select the report you want to schedule.
2. (For Security Administrator) In the **Organization Option**, select one of the following options: **My immediate organization only** and **include all organizations below** and then click **Apply**.

The content of the listing page updates based on the organization option selected.

3. Apply the filters as needed using the **Filters** icon  in the action bar.
4. Click the **Schedule** icon  in the action bar.

The Analytics Scheduler dialog box opens. It has the following three tabs:

- **Schedule New Job:** Use this tab to schedule a report creation job for now or set how frequently you want to create the report. You can also specify the format of the report.
  - **Scheduled Job:** Use this tab to see all the scheduled jobs.
  - **Completed Job:** Use this tab to see the completed jobs and download the reports.
5. On the Schedule New Job tab, do the following:
- a. In **Scheduling Format**, select the format in which you want the report created.
  - b. Click **Right now** to create the report right away. Go to [Step 5.d.](#)
  - c. Click **Schedule** and select the option you want to configure the frequency of report creation. You can set the frequency to once, daily, weekly, monthly, and quarterly.
    - i. If the **Once** option is selected, then also select a **Timezone** from the list, set the **time** in hh:mm:ss format and the **date** to when you want the report to be created, and in **Period**, specify the date range from which you want to include the information in the report by selecting from date and to date.
    - ii. If the **Daily** option is selected, then also select a **Timezone** from the list, set the **time** in hh:mm:ss format to when you want the report to be created, and for **Period**, specify a number for the day prior to today for which you want the daily report to be created. For example, if the period is 5 and the date of the scheduled job is 29th Oct, then the report would contain full day data for 24th Oct only. The daily option is to generate one day's data only.
    - iii. If the **Weekly** option is selected, then also select the day of the week when the report creation should occur every week in the **On** field, select a **Timezone** from the list, set the **time** in hh:mm:ss format to when you want the report to be created, and in **Period**, specify the day of the week in past up to which data should be included in the report. For example, if Every Friday is selected in the On field, then the Period field should have Last Friday to create a weekly report.
    - iv. If the **Monthly** option is selected, then also specify the day of every month the report should be created, select a **Timezone** from the list, set the **time** in hh:mm:ss format to when you want the report to be created, and for **Period**, specify the day of the previous month when the monthly report creation cycle should start. For example, if 30th Oct is the specified day for report creation and cycle starts on 30th day of the previous month, then the report would contain data for one month that is October in this case.
    - v. If the **Quarterly** option is selected, then also select the day of the month the report should be created, select a **Timezone** from the list, set the **time** in hh:mm:ss format to when you want the report to be created, and for **Period**, specify when the quarterly report creation

cycle should start. For that, enter a day that was 3 months ago from the day of report creation. The report would be generated every 3 months one time and will contain 3 months data. For example, if 30th Oct is the specified day for report creation and cycle starts on 1st day of the month that was 3 months ago, then it means that cycle starts on 1st day of August and the report would contain data from past 3 months, August, September, and October.

d. Click **Submit**.


A message displays that the job is scheduled and an email is sent to the recipient. The scheduled job displays on the Scheduled Job tab. If the report being generated is small, it might become available on the Completed Job tab immediately. For information about using the Completed Job tab, see [“To check the completed job and download a report” on page 57](#).

The job names indicate the report frequency such as Now, Once, Daily, Monthly and Quarterly, report type, and date and time the report job was scheduled. For example, `Once-User Information-2021/09/15 14:32:19`, `Monthly-User Information-2021/08/13 18:35:23`, and `Quarterly-User Information-2021/08/25 12:25:33`.

### 4.1.6.3 Managing scheduled report creation jobs

Use this procedure to check all the scheduled jobs and manage them if needed.

#### To check the scheduled jobs

1. Click the **Schedule** icon  in the action bar.  
The Analytics Scheduler dialog box opens.
2. In the Analytics Scheduler dialog box, click the **Scheduled Job** tab.  
The tab displays all the scheduled, cancelled, and expired report jobs. You can use the << and >> arrow buttons to navigate the list of scheduled jobs. You can do the following on this tab:  
Use **View Summary** to see the summary of a selected job.

- Click any job whose summary you want to see and then click **View Summary**.

The summary of the selected job displays information such as status of the job which could be scheduled, cancelled, or expired, and details of the schedule job such as when is the next day for report creation depending on the specified frequency. It also shows the name and type of the output document.

- Click **Back to Scheduled Job** to go back to the list of scheduled jobs.

Use **View Completed** to see the completed reports for weekly, monthly, or quarterly type of scheduled report jobs.

- Click a scheduled report job of weekly, monthly, or quarterly type and then click **View Completed**.



The Completed Job tab opens and displays the completed reports for the previous period for the selected job.

- Click **Back to Scheduled Job** to go back to the list of scheduled jobs.

You can filter the displayed jobs by their status, which could be scheduled, cancelled, or expired and frequency.


- Click the **Scheduled** check box to see only scheduled jobs and then from the list of report creation frequency  , select the option you want. For example, to see all the scheduled jobs to be generated every week, click the Scheduled check box and then select Weekly from the list. Clear the **Cancelled** and **Expired** check boxes. Go to [Step 5](#).
  - Click the **Cancelled** check box to see only the jobs that were cancelled and clear the **Scheduled** and **Expired** check boxes. Go to [Step 5](#).
  - Click the **Expired** check box to see only the jobs that expired and were not completed and clear the **Scheduled** and **Cancelled** check boxes. Go to [Step 5](#).
  - Click **Reset** to clear your selections and go back to the original selections on the page to see all the scheduled jobs.
3. (optional) To cancel a scheduled job, select it and then click **Cancel Job** and then click **Ok** to confirm cancelling the job.
  4. (optional) To delete a canceled job, select it and then click **Delete Job** and then click **Ok** to confirm deleting the job.
  5. Click **Apply** after you have selected the check boxes you need.  
Clicking apply displays the results based on your selections. The result displays the job name and job status.

After the scheduled jobs are completed, the appropriate user is notified by email. User can then download the report from the Analytics Scheduler dialog box. See [“To check the completed job and download a report” on page 57](#).

#### 4.1.6.4 Downloading completed reports


Use this procedure to download completed reports.

##### To check the completed job and download a report

1. Click the **Schedule** icon  in the action bar.
2. In the Analytics Scheduler dialog box, click the **Completed Job** tab.

The tab displays all the completed report jobs that succeeded, failed, were cancelled, are running, or pending. You can use the << and >> arrow buttons to navigate the list of completed scheduled jobs. You can do the following on this tab:

You can filter the displayed jobs by their status, which could be scheduled, failed, cancelled, running or pending, and frequency.

- Click the **Succeeded** check box to see only the scheduled jobs that were completed successfully and then from the list of report creation frequency , select the option you want. For example, to see all the successfully completed jobs to be generated every month, click the Succeeded check box and then select Monthly from the list. Clear other status check boxes. Go to [Step 3](#).

- Click the **Failed** check box to see only the jobs that failed and were not completed, and clear other status check boxes. Go to [Step 3](#).
- Click the **Cancelled** check box to see only the jobs that were cancelled and clear other status check boxes. Go to [Step 3](#).
- Click the **Running** check box to see only the jobs that are still running and clear other status check boxes. Go to [Step 3](#).
- Click the **Pending** check box to see only the jobs that are still pending and clear other status check boxes. Go to [Step 3](#).
- Click **Reset** to clear your selections and go back to the original selections on the page to see all the listed jobs.

3. Click **Apply** after you have selected the check boxes you need.

Clicking apply displays the results based on your selections. The results show the job name, output file name, output file size, date and time when the job was completed, result to indicate if the job succeeded or not, and the downloadable report.

4. Click **Report** in the Download column for any completed job to download the report in the CSV format.

Clicking the downloaded report opens it.

The length of the time for which the completed reports are retained on the Completed Jobs tab is configurable.

5. (optional) To delete any job on the Completed Job tab, click the job to select it and then click **Delete Completed Job**. Click **OK** to confirm deletion or click **Cancel** to cancel out the deletion.

Job is deleted message displays, and the deleted job does not display on the Completed Job tab.

## Chapter 5


# Manage Organization

Administrators can use this module to manage users, service packages, pending requests, history, and administrators of their own organization.


### To open the Manage Organization page

1. Click the main menu  to open the navigation pane.
2. Click **Manage Organization**.

The Home > <top level organization name> page opens.

 **Note:** What you see in the user interface is determined by the role and permissions assigned to your profile. The user interface elements, such as fields, labels, and tooltips, that you see in IAM Administration for your organization might be different from the descriptions in the Help and the guide because this application can be configured to suit the needs of any organization.

## 5.1 Contents of the manage organization page




 **Note:** The contents of this page change based on user role and permissions. Based on your role, you might see all the following information or just a subset of it.

The manage organization page displays a metadata section and six tabs to manage information for the currently logged in organization.

### Metadata section




The metadata section is the area above the tabs.

The metadata section of the manage organization page for the current organization displays the following information:

- The top level organization (TLO) name, phone number, and organization ID
- Number of users, administrators, and pending requests of the organization.
- Displays a flag icon to indicate the current status of the organization, whether the organization is active , inactive, or in any other state.
- Displays the arrow  to expand the metadata section to view additional information such as organization creation date, organization type, TLO URL. Click the  to revert to the original view of the metadata section.



### Tabs section



The tabs section of the manage organization page for the current organization displays the following information:

- Six tabs: Overview, Users, Service Packages, Pending Requests, History, and Administrators.
- Organization Hierarchy icon  to view the organization tree. See [“Organization hierarchy” on page 60](#).
- Icons **Add User**  and **Add Division**  to add users and divisions, respectively, to your organization. See [“To add a new user to an organization” on page 62](#) and [“To add a new division to an organization” on page 63](#).



## 5.1.1 Organization hierarchy


Clicking the **Organization Hierarchy** icon  opens the currently open organization’s hierarchy tree in a panel. You can use this hierarchy tree to navigate to different divisions of the organization to perform division-related tasks. To come back to the parent organization, just click the parent organization name in the hierarchy tree panel.

If the currently open organization is a top-level organization (TLO), it displays at the top level of the hierarchy and is represented by the root . All the divisions, represented by the icon , that are part of the top-level organization are listed under the root. If divisions have subdivisions, they are listed under the division.

Clicking the arrow icon  next to a division name or subdivision name expands the tree further. Clicking the arrow  next to the root organization either expands or collapse the hierarchy tree.

Pointing to any division or organization name in the hierarchy tree displays a group

of inline icons  to view profile details, users details, and administrators for the division or organization, respectively. Clicking on any of the inline icons for any division in the organization hierarchy opens that division in the Manage Organization page. In the organization hierarchy, the open division is shown as selected and your location in the hierarchy is indicated by the location icon  next to the division name. If TLO is the currently open organization, no location icon is shown next to its name in the hierarchy.

 **Note:** The group of inline icons does not appear for the organization or division whose information currently displays in the Manage Organization page.

See [“Managing divisions of your organization” on page 99](#) for detailed information about managing divisions-related tasks.

## 5.2 Overview tab on the manage organization page

The Overview tab displays the following information about the currently open TLO in IAM Administration: Organization name, full address including city, province, country, and postal code, phone number, fax number, company URL, and other information configured for the organization. The password and authentication policies used are also displayed.

The **password policy** contains rules about the kind of passwords, such as minimum and maximum password length, characters that can be used, lifetime of a password and so on, that are acceptable to log into the application.

The **authentication policy** contains rules to verify the identity of the user who is attempting to log into the application. The authentication policy contains rules such as number of invalid login attempts permitted within a certain amount of time before the account is locked, multi-factor authentication policy used and so on.



### Notes

- The information on this tab can be edited by the Exchange operator and Security Administrator for the organization. See [“To edit the contents of the Overview tab” on page 61](#).
- What you see in the user interface is determined by the role and permissions assigned to your profile. The user interface elements, such as fields, labels, and tooltips, that you see in IAM Administration for your organization might be different from the descriptions in the Help and the guide because this application can be configured to suit the needs of any organization.



### To edit the contents of the Overview tab

1. Click **Edit** on the Overview tab page.  
The fields switch to the editable mode.
2. Modify the contents of the fields as needed. Fields marked with an asterisk \* are mandatory and require a value.
3. In the **Password Policy** field, select another policy from the list if needed.
4. In the **Authentication Policy** field, select another policy from the list if needed.
5. Click **Save**.




## 5.2.1 Adding a new user to your organization

To add a new user to your organization from the Overview tab in the Manage organization page, use the following procedure:

### To add a new user to an organization

1. Click the **Add User** icon  on the Overview tab page.
2. In the **Select Division** page, select the division of the organization where you want to add the new user. For divisions with subdivisions, click the  to expand and see the subdivisions. Click the subdivision if that is where you want to add the user.



The selected organization, division, and subdivision are shown as breadcrumb trail under the dialog box name. The selected division or subdivision name is also shown.

3. Click **Next**.  
The user account creation wizard opens and displays the login and personal information page.
4. In the Login and personal information page, provide the following details. The required fields are marked with an asterisk .
  - a. In the Login Details section, provide the following information:  
**User ID:** Provide a unique user ID and click on **Check for availability** to see if the name is available for use.  
A check mark with the word Available indicates you can use this name for your organization.
  - b. **Password:** Provide a password according to the password rules. To see the rules, hover the mouse cursor over the  icon adjacent to **Retype Password**.
  - c. **Retype Password:** Type your password again.
  - d. In the Personal Details section, provide user's first and last name, user's address, city, province, country, postal code, email address, and phone number. Point the cursor to the  icon to see helpful additional information.
  - e. Click **Next**.  
The Summary page shows a summary of all the information entered in the previous steps.
5. Click **Submit** after you have checked all the information on the summary page. User created successfully message displays.

## 5.2.2 Adding a new division to your organization

To add a new division to your organization from the Overview tab in the Manage Organization page, use the following procedure:

### To add a new division to an organization

1. Click the **Add Division** icon  on the Overview tab page.
2. In the **Select Division** page, select the division of the TLO where you want to add the new division. For divisions with subdivisions, click the  to expand and see the subdivisions. Click the subdivision if that is where you want to add the user.

The selected organization, division, and subdivision are shown as breadcrumb trail under the dialog box name. The selected division or subdivision name is also shown.



3. Click **Next**.  
Part of the page displays a message that you are registering as the security administrator of the new division (organization) that you are creating and the responsibilities of the role.
4. Read the information provided about the Security Administrator role and if you subpackage to accept the role and responsibilities, click **I Accept**. To decline, you can click **I do not accept**.

On accepting the role, the wizard to create a new division account opens and displays the first step in the process, the Organization Information page. The page displays the name of the parent organization under which you are creating the new division. The page also displays the fields to gather organization-related information for the new division. Do the following:

- a. In the **Organization Name** field in the Organization Details section, type a unique name for the new division and click on **Check for availability** to see if the name is available for use.  
A check mark with the word Available indicates you can use this name for your division.
  - b. In **Address**, provide the organization address using all the address boxes if needed.
  - c. **Country, State, City, and Postal Code**: Provide the names of the country, province, city, and postal code that comprise the new division's address.
  - d. Click **Next**.
  - e. Organization created successfully message displays.
5. In the Login and Personal Information page, provide the following details. The required fields are marked with an asterisk.
    - a. In the Login Details section, provide the following information:

**User ID:** Provide a unique user ID and click on **Check for availability** to see if the name is available for use.

A check mark with the word Available indicates you can use this name for your organization.

- b. **Password:** Provide a password according to the password rules. To see the rules, point the cursor to the  icon adjacent to **Retype Password**.
- c. **Retype Password:** Type the password again.
- d. In the Personal Details section, provide user's first and last name, email address, and phone number. Point the cursor to the  icon to see helpful additional information.
- e. Click **Next**.  
The Summary page shows a summary of all the information entered in the previous steps.
- f. Click the **Submit** button after you have checked the information.  
Organization created successfully message displays.  
The administrator receives an email that a new division is added to the organization.

## 5.3 Users tab







The Users tab on the Manage Organization page lists all the users who are associated with the currently organization.

### To open the Users tab

1. Open the **Manage Organization** page using instructions in ["Manage Organization" on page 59](#).
2. Click the **Users** tab on the Manage Organization page.

The Users tab page contains a Filter icon  and a list of users associated with the current organization.

The list of users on the Users tab displays the following details about the users:

- **Name, User Id, Job Title, Email, Phone:** The columns display users' name, user ID, job title, email address, and phone number.
- **Status:** Status of the user indicating whether they are active , inactive , pending , suspended , rejected , or locked .

Clicking a user item would open the user's details in another page. See ["To view the details of a user" on page 66](#).



Use the Filter icon to open a Refine by pane, which provides options to refine the list of users using the provided criteria. See [“To filter or refine the list of users” on page 65](#).

The lower part of the Users page displays the number of items shown on each page **10 per page** which you can change. It also shows the number of pages and the total number of items.

#### To change the number of items listed per page setting


- Point the cursor to the number of items per page and from the popup menu, select the number you want to display.

#### To navigate the list of items on all the pages

1. Click **Next** to go to the next page.
2. Click **Previous** to go to the previous page.
3. Click a page number to directly navigate to that page.

As an administrator, you can filter or refine the list of users to find specific ones or find ones using certain search criteria.

#### To filter or refine the list of users

1. Make sure the Users tab is selected and click **Filter**  on the page.
2. In the Refine By pane, use one, some, or all of the following options to use as criteria to refine the list and only display the matching user records:
  - **User status types, Active, Inactive, Pending, Suspended, Rejected, Locked:** Click one or more status type check boxes to refine the list of users by their status.
  - **First Name:** Enter the first name to find users with matching first name.
  - **Last Name:** Enter the last name to find users with matching last name if first name is not entered or matching combination of first and last name.
  - **User Id:** Enter the user ID of the user you want to find.
  - **Email Id:** Enter the email address of the user you want to find.
  - **Role Id:** Enter the role ID of the user you want to find.
  - Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine By pane.

The matching records are listed in the Users page. The fields used for the search are shown as tokens above the column names on the page.

- Click the **X** in individual tokens to remove that filter and re-run the search and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.

- Click **Close** to close the Refine by pane.

### 5.3.1 Viewing user details

Administrators can view the details of a user.

#### To view the details of a user

- In the Users tab, after refining the listed records if needed, click the user whose details you want to view.

The selected user's details open in another page **Home** > <top level organization name> > <selected user name> and displays the following information: a metadata section with user's name, user ID, email address, phone number, user's status, active or any other. User's status can be changed using the Set Status switch. The metadata section is the area above the tabs.

The page also displays another section with six tabs: **Overview, Service Packages, Open Requests, History, Attributes, and Security Settings.**

#### 5.3.1.1 Suspending a user

A suspended user account is one whose package grants and roles remain intact, but the user is unable to login. For example, organizations may suspend the account of users who are going on extended leave of absence and will not need to log in to their accounts. A reason is required for suspending a user account and is logged and is viewable by other administrators in the organization.


To suspend a user, you need to change the user's status to suspended in the metadata area of the **Home** > <top level organization name> > <selected user name> page. Metadata is the area above the tabs.

#### To suspend a user

1. Click the **Set status** switch.

The Suspend selected user dialog box opens. You are informed that suspending the selected user would prevent the user from logging into the application and the user account would be locked until the suspension is removed.

2. In the **Reason** box, provide a reason to suspend the selected user and then click **Suspend**.

The user is suspended successfully message displays. The **Set status** changes to **Suspended** and the status flag also switches to **Suspended** .

If the switch for PERSON SUSPENDED EVENT is turned on, the suspended user will receive an email notification about the account being suspended and would not be able to log in to the portal. For information about configuring email notifications, see "[Preferences tab](#)" on page 45.

After a user is suspended, it can be re-activated or deleted. To re-activate a user, see [“Activating a suspended user” on page 67](#). To delete a user, see [“Deleting a suspended user” on page 67](#).

### 5.3.1.2 Activating a suspended user

To re-activate a suspended user, you need to change the user’s status to active in the metadata area of the **Home** > <top level organization name> > <selected user name> page. Metadata is the area above the tabs


#### To re-activate a suspended user

1. Display the user details for the suspended user who you want to re-activate. See [“To view the details of a user” on page 66](#). You can refine your search for the suspended user using the procedure [“To filter or refine the list of users” on page 65](#).

2. In the metadata area of the selected user who was suspended, click the **Set status** switch.

The Activate selected user dialog box opens. You are informed that activating the selected user would allow the user to log into the application and would unlock the user account.

3. In the **Reason** box, provide a reason to activate the selected suspended user and then click **Activate**.

The user is activated successfully message displays. The **Set status** changes to **Active** again and the status flag also switches to **Active** .

If the switch for PERSON UNSUSPENDED EVENT is turned on, the suspended user will receive an email notification about the account being unsuspended and would be able to log in to the portal. For information about configuring email notifications, see [“Preferences tab” on page 45](#).

### 5.3.1.3 Deleting a suspended user

Deleting a user is **permanent** and cannot be undone. It forever restricts the user account from being used. Users that are deleted lose all roles, service packages grants, and can never log into their account again.

A user who is the only security administrator of an organization cannot be deleted. To delete such a user, another user first must be assigned the security administrator role for the organization.

If the user you want to delete is the sole security administrator and user of an organization, you can not delete such a user. Exchange administrators can instead delete the organization. And security administrators of an organization can delete the divisions in their organization.

To delete a user, make sure user is already in the suspended state. Administrator also needs the Permanently Remove User privilege enabled.

Typically, a user account is deleted when the user leaves the organization and is not expected to return. A reason for deleting a user account is required and becomes part of user's permanent record and can be seen by all administrators of the organization.


### To delete a suspended user

1. Display the user details for the suspended user who you want to delete. See [“To view the details of a user” on page 66](#). You can refine your search for the suspended user using the procedure [“To filter or refine the list of users” on page 65](#).

2. In the Overview tab of the selected suspended user, click the **Delete** button.  
The Delete selected user dialog box opens. You are informed that deleting the user would permanently remove the user from the system and the user would not be able to access the application. To access the application, user would need to re-register with the application.

3. In the **Reason** box, provide a reason to delete the selected suspended user and then click **Delete**.

The user is deleted successfully message displays.

The Users tab in the **Home** > <user's organization name> page shows the user's status as inactive . The word deleted is appended to the deleted user's User Id.

The user is not able to log into the portal and the user account can not be reactivated. If needed the user can be invited to register for a new user account. For more information, see [“Inviting users to register” on page 20](#).

## 5.3.2 Overview tab for the selected user

Overview tab displays user details such as first and last names, organization name to which the user belongs, user's full address, email address and phone number. Administrators with appropriate privileges can edit user's details. See [“To edit the contents of the Overview tab for the selected user” on page 68](#).



**Note:** Fields marked with an asterisk are mandatory.

### To edit the contents of the Overview tab for the selected user

1. Open the Overview tab for a user using the instructions in [“To view the details of a user” on page 66](#).

2. Click **Edit** on the Overview tab page.

The fields switch to the editable mode. The contents of the Organization Name field cannot be modified.

3. Modify the contents of the fields as needed. Fields marked with an asterisk  are mandatory and require a value.

#### 4. Click **Save**.

You have successfully edited the selected user's details. The user will receive an email notification that their user details were modified by the administrator.


### 5.3.3 Service Packages tab

Administrators can see the list of services currently granted to a specific user on the Service Packages tab.

- **Service Package:** A grantable container that contains at least one application or tool accessed through IAM Administration. By requesting a service package, you can obtain access to additional applications. Some service packages contain subpackages.
- **Sub package:** A grantable container that contains at least one subservice application. A Sub package requires that the parent package be granted first. For example, IAM Administration provides an application called Content Management.
  - Customer A has purchased from Covisint a version of Content Management customized with Customer A's logo.
  - Customer B has purchased from Covisint a version of Content Management customized with Customer B's logo.
  - Customer C has purchased from Covisint a version of Content Management customized with Customer C's logo.

Users must be approved access to the Service Package called "Content Management", and then must request access to the sub package for the appropriate "customer version" of the Content Management Application. Therefore, the user would perform the following process to gain access to a "customer version" of the application:

1. request access to **service package** Content Management Service Package.
2. receive approval for **service package** Content Management Service Package.
3. request access to **sub package** "Customer-C Content Management".
4. receive approval for **sub package** "Customer-C Content Management".

 **Note:** Users can only be approved for service packages that are already granted to their organization. If users request a service or sub package that is not already granted to their organization, an administrator will need to request those services on behalf of the organization before granting them to users.




To view the service packages granted to a user of your organization, click the **Service Packages** tab in the User's details page. See ["To view the details of a user" on page 66](#).

The Service Packages page displays a **Filter** icon  and an **Assign Package** icon . The page also displays the following details about the service packages: name

of the service package granted to the user, category of the service package, granted date which is the date and time the service was granted to the user, and status of the service package whether it is active or in some other state. In the Action column, you can view package information, such as names of the owner organization and organization, services included in the package and required approvers.

As an administrator, you can filter or refine the list of service packages granted to the user to find specific ones or find ones using certain search criteria.

### To filter or refine the list of service packages

1. Make sure the Service Packages tab is selected and click **Filter**  on the page.
2. In the Refine by pane, use one, some, or all of the following options to use as criteria to refine the list and only display the matching requests:
  - **Status:** Click the arrow  to select either **Active** or **Suspended** to refine the list of service packages by their status.
  - **Category:** Click the arrow  to select one of the listed options to refine the list of service packages by their category.
  - Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.

The matching records are listed in the Service packages page. The fields used for the search are shown as tokens above the column names on the page.
  - Click the **X** in individual tokens to remove that filter and re-run the search and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
  - Click **Close** to close the Refine by pane.

#### 5.3.3.1 Viewing service package details

To view the details of a listed service package granted to a user of your organization, use the following procedure:

#### To view the details of a service package

- In the Service Packages tab for a user, click the name of the service package in the list.

The Package Overview dialog box opens. The dialog box displays a metadata area with the following information: package name, package ID, package creation date, and service package status, active or suspended.

The dialog box also displays an **Overview** tab with the following details: **Package Details** area with the package type, parent service, owning organization, and grantee name. The tab also has an **Included Services** area that lists other services that might be part of the service package. The tab also shows tiles to display number of sub packages, included services, and required approvers for the service package.

The service package can be suspended using the set status switch in the metadata area. See [“Suspending a service package granted to a user” on page 71](#).

#### 5.3.3.1.1 Suspending a service package granted to a user

To suspend a service package, you need to change the service package’s status to suspend in the metadata area in the Package Overview dialog box.

##### To suspend a service package


1. In the Service Packages tab for a user, click the name of the service package you want to suspend.

The Package Overview dialog box opens.

2. Turn off the **Set status** switch .

The Suspend selected service package dialog box opens. You are informed that suspending the selected service package would prevent the user from accessing all the services of this service package.

3. In the **Reason** box, provide a reason to suspend the selected service package and then click **Suspend**.

The service package is suspended successfully message displays. The **Set Status** changes to **Suspended** and the status flag also switches to **Suspended** .

The **Delete** button becomes available in the Package Overview dialog box.

Once suspended, service package grants can be re-activated or removed. To re-activate a service package grant, see [“Activating a suspended service package granted to a user” on page 71](#). To remove a service package granted to a user, see [“Remove a suspended service package granted to a user” on page 72](#).




**Note:** Use the same procedure to suspend a subpackage granted to a user.

#### 5.3.3.1.2 Activating a suspended service package granted to a user


To re-activate a suspended service package grant, you need to change the service package’s status to active in the metadata area in the Package Overview dialog box.

##### To re-activate a suspended service package

1. Display the details for the suspended service package that you want to re-activate. See [“Viewing service package details” on page 70](#). You can refine your search for the suspended service package using the procedure [“To filter or refine the list of service packages” on page 70](#).
2. In the metadata area of the selected service package that was suspended, turn on the **Set status** switch .

The Activate selected service package dialog box opens. You are informed that activating the selected service package would allow the user to access all the services of this service package.

3. In the **Reason** box, provide a reason to activate the suspended service package and then click **Activate**.

The service package is activated successfully message displays. The **Set Status** changes to **Active** again and the status flag also switches to **Active** .

### 5.3.3.1.3 Remove a suspended service package granted to a user

To delete a service package, make sure the service package is already in the **Suspended** state. Administrator also needs the **Permanently Remove User Package** permission enabled.

#### To delete a suspended service package

1. Display the details for the suspended service package that you want to delete. See [“Viewing service package details” on page 70](#). You can refine your search for the suspended service package using the procedure [“To filter or refine the list of service packages” on page 70](#).

2. In the Overview tab of the selected suspended service package, click the **Delete** button.

The Revoke selected service package dialog box opens. You are informed that removing the selected service package would revoke the package granted to the user.

3. To confirm deletion, click **Delete**.

The service package grant revoked successfully message displays.

The History tab shows the service package grant as revoked.



**Note:** Use the same procedure to delete a suspended subpackage granted to a user.


### 5.3.3.2 Assigning a service package to a user

Security Administrators for an organization can grant service packages to the users in their organization and its various divisions.




**Note:** Service administrators can only grant service packages for which they are the administrator.


#### To assign a service package to a user

1. In the Service Packages tab for the selected user, click **Assign Package** .


The Assign Service Packages page opens and displays a list of service packages to which your organization has access and that can be assigned to the selected user.




2. To filter the list of service packages, click the **Filter** icon  and in the Refine By pane that opens, do the following:

- **Name:** Enter the name of the service package you want to assign to the user.
- **Category:** Click the arrow  to select one of the listed options to search for the packages by category.
- **Package Id:** Enter the ID of the Service Package you want to assign to the user.
- **Parent Package Id:** Enter the parent ID of the service package to narrow the list of service packages by the ID of the parent.
- Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.

The matching records are listed in the Assign Service Packages page. The fields used for the search are shown as tokens above the column names on the page.

- Click the **X** in individual tokens to remove that filter and re-run the search and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
  - Click **Close** to close the Refine By pane.
3. In the filtered list in the Assign service packages area, click the **Assign** icon  in the **Action** column for the service package that you want to assign to the selected user.

The Assign Service Package dialog box opens and displays the following information about the service package:

- Service Package details such as name of the Owning organization, description of the service package, organization name and organization type.
  - **Required Approvers** area that displays the roles of approvers. Click the arrow  in the area to expand it.
  - **Included Services** area that lists the services that might be included in the service package. The area displays the name, category, description and URL of the included services.
  - **Assign Reason** box to provide a reason for assigning the service package to the selected user.
4. In the **Assign Reason** box, enter a reason for assigning the service package to the selected user and click **Assign**.

Service package assigned successfully message displays. The service package that you just assigned no longer displays in the list in the Assign service packages area.

5. Click **X** to close the Service Packages page.

The Service Packages tab page displays the assigned service package.

### 5.3.4 Open Requests tab

The tab displays the currently pending requests made by the selected user. The approving administrators receive email notifications when a request is submitted by the user.


The Open Requests area displays the following details about requests: Name of the service package requested, phase of approval, request types, reason for request, requested date, and action.

Administrators can send reminders to the approvers to approve user's pending requests or can cancel one or more or all the pending requests if needed.

#### To send a reminder to the approver of the service package pending requests

1. Select all the pending requests by clicking the check box adjacent to the **Package Name** column. Alternatively, you can also just click the check box for one request.

The Action bar displays two new options: **Send Reminder** and **Cancel Request**. The Action bar also shows the number of selected pending requests.

2. To send a reminder for all the selected pending requests, click **Send reminder** in the action bar. To send a reminder for one selected pending request, you can either click the **Send reminder**  in the **Action** column or the **Send reminder** in the action bar.


The Send Reminder dialog box opens. It provides details about the pending requests.

3. In the **Reminder note** box for each pending request, enter a note to help the administrator make a decision about approving the request and click **Send**.

#### To cancel pending requests

1. Select all the pending requests by clicking the check box adjacent to the **Package Name** column. Alternatively, you can also just click the check box for one request.

The Action bar displays two new options: **Send Reminder** and **Cancel Request**. The Action bar also shows the number of selected pending requests.

2. To cancel all the selected pending requests, click **Cancel Request** in the action bar. To cancel one selected pending request, you can either click the **Cancel Request**  in the **Action** column or the **Cancel Request** in the action bar.

The Cancel open request dialog box opens. It provides details about the pending requests you are canceling.



**Note:** If you are canceling pending request for another user, the original requestor receives an email notification about the cancellation.

3. Click **Send**.

### 5.3.5 History tab

Administrators can use the History tab to see which requests were granted to the selected user and all the requests user had made for services except the pending requests.

The History tab contains two subtabs: Grant History and Request History

- **Grant History:** Lists all the requests that were granted to the selected user and displays the following details: Requested package, evaluator, decision date, action, such as granted, suspended, or revoked, and status of the granted service package such as active, suspended, or unactivated.
- **Request History:** Lists all the service requests the selected user had submitted except the requests pending a decision. The following details about the requests are shown: request type, requested package, requested date, evaluator who is the role approving the request, decision date, and status of the requested service.

### 5.3.6 Attributes tab

The tab displays the attributes associated with the selected user such as identifier, region, employee ID, department, and so on. The details shown include attribute ID, attribute name and the attribute value.

### 5.3.7 Security settings tab

Administrators can use the Security Settings tab to Specify User Password and Reset User Password. The Specify User Password method is less secure than the Reset User Password method. The administrator helping reset the user password knows user's entire password which can be a risk and a liability.


Therefore, use the specify user password process to reset the user password in exceptional scenarios only such as when a user is locked out of the account due to multiple attempts to log in using incorrect password. In this scenario, user calls the help desk and asks for assistance to reset the password.

#### To specify user password for the selected user

1. Open the **Manage Organization** page using instructions in "**Manage Organization**" on page 59.
2. Click the **Users** tab.
3. On the Users listing page, click the name of the user whose password you need to reset.

4. Click the **Security Settings** tab in the **Home** > <organization name >> <user name> page.

The Security Settings tab page opens, and the **Specify User Password** option is already selected. This option should be used in exceptional situations, such as when user has lost the password and can not remember it at all, to reset the user password, and the administrator needs to follow a series of steps to reset the user password.

5. To reset the user password using this option, follow the following instructions on the screen:
  - a. Read the challenge question to the user on the phone to confirm the user's identity.
  - b. Wait for the user on the phone to provide an answer to the challenge questions. If the user provides correct answers, then proceed to **Step 5.c**. Ask the user to stay on the phone while you perform **Step 5.c**.
  - c. In the **New Password** box, enter a new password for the user and then enter it again in the **Re-type new password** box. Point to  to see the password rules. Select the **Show Password** check box to unmask the password as you are entering it.
  - d. Click **Submit**.

The password is updated successfully message displays.
  - e. Communicate the new password to the user on the phone and inform them that they will be required to change the password the first time they log into the application.

#### What happens next?

The user receives an email and uses that to log into the application using the new password and then change it when prompted on the login screen for the application.

To reset the user password, use the following procedure:

#### To reset user password for the selected user

1. Open the **Manage Organization** page using instructions in "**Manage Organization**" on page 59.
2. Click the **Users** tab.
3. On the Users listing page, click the name of the user whose password you need to reset.
4. Click the **Security Settings** tab in the **Home** > <organization name >> <user name> page.

The Security Settings tab page opens. To reset the user password, the administrator needs to follow a series of steps.
5. Click the **Reset User Password** option.

6. To reset the user password using this option, follow the following instructions on the screen:
  - a. Read the challenge question to the user on the phone to confirm the user's identity.
  - b. Wait for the user on the phone to provide an answer to the challenge questions. If the user provides correct answers, then click **Reset Password**. proceed to step 3. Ask the user to stay on the phone while you perform step 3.


**Step 3** instructions to reset the password display on the screen. You are informed that the password for the selected user is successfully reset. The first-half of the randomly generated password displays on the screen. Follow the following instructions on the screen to reset the user password.

- i. Provide the user this first-half of the password on the phone.
- ii. Inform the user that the rest of the randomly-generated password is emailed to the user's registered email address.
- iii. Inform the user to combine the first half and the emailed half of the randomly generated password to create the full password and then, use this full password to log into the application. They can change the password after logging in if needed.

### 5.3.8 Assigned roles tab

The Assigned Roles tab lists the roles that are currently assigned to the selected user. The tab might not be available if a role is not assigned to a user.

#### To delete a role assigned to the selected user

1. In the Assigned Roles area, click the Delete Roles icon  for a role to remove the role assignment to the selected user.
2. Click **Remove** in the confirmation dialog box.

Successfully removed the assigned role message displays. The removed role no longer displays on the Assigned Roles tab.



## 5.4 Service Packages tab

Administrators can use the Service Packages tab for the organization to see a list of services that are currently granted to their organization.


#### To open the service package page

1. Open the **Manage Organization** page using instructions in "[Manage Organization](#)" on page 59.
2. Click the **Service Packages** tab in **Home** > *<organization name>*.

The Service Packages list page opens and lists all the service packages and subpackages granted to the currently open organization.

The toolbar in the Service Packages list page contains a **Filter** icon  and the  icon to open a submenu with options to request a package and assign a package.

Use the Filter icon to open a Refine By pane, which provides options to refine the list of service packages using the provided criteria.

The lower part of the Service Packages list page  displays the number of records shown on each page, which you can change. It also shows the number of pages and the total number of records or items.

#### To change the number of items listed per page setting




- Point the cursor to the number of items per page and from the popup menu, select the number you want to display.


#### To navigate the list of items on all the pages

1. Click **Next** to go to the next page.
2. Click **Previous** to go to the previous page.
3. Click a page number to directly navigate to that page.

### 5.4.1 Service Packages list page

The Service Package list page contains a list of all of the service packages and subpackages granted to the currently open organization that an administrator is authorized to view and manage. The page displays the following details:


- **Name:** Name of the service package. If the service package contains subpackages, the arrow  displays adjacent to the package name. Clicking the arrow expands the service package row and displays the list of subpackages.
- **Category:** Category that the service package belongs to such as administration, application, role, and so on.
- **Granted Date:** The date when the service package was granted to the organization.
- **Status:** The status of the service package such as active  or suspended .
- **Action:** Displays icons for actions that are permitted for the service package.



Currently it displays the Package Information icon . Clicking the icon opens a Package Information box and displays details such as organization name, organization type, service package name, additional services included in the package, and approvers required to approve granting of the package to requestors. The package information is non-editable.

Clicking a service package name would open the package details in another page. See [“Viewing service package details” on page 79](#).

You can filter or refine the list of service packages granted to the organization to find specific ones or find ones using certain search criteria.

### To filter or refine the list of service packages

1. Make sure the Service Packages tab is selected and click **Filter**  on the page.
2. In the Refine By pane, use one or both options to use as criteria to refine the list and only display the matching requests:

- **Status:** Click the arrow  to select either **Active** or **Suspended** to refine the list of service packages by their status.
- **Category:** Click the arrow  to select one of the listed options to refine the list of service packages by their category.
- Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine by pane.

The matching records are listed in the Service packages page. The fields used for the search are shown as tokens above the column names on the page.

- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** to close the Refine By pane.

## 5.4.2 Viewing service package details

To view the details of a listed service package granted to your organization, use the following procedure:


### To view the details of a service package granted to your organization

- In the **Service Packages** tab for your organization, click the name of the service package in the list.


The service package opens in another page and displays a metadata area with the following information: package name, package ID, package creation date, and service package status, active or suspended.


The service package can be suspended using the Set Status switch in the metadata area. See [“Suspending a service package granted to an organization” on page 81](#).

The service package page also displays many tabs such as **Overview**, **Sub Packages**, **Claim Codes**, and **Remote Claim** if these are included in the service package. If the selected service package is also terms & conditions enabled, then an additional tab called **Terms and Conditions** is also displayed.

For a service package with SAO (Service Authority Organization) organization, the service package page also displays the **SAO Hierarchy** icon . Security administrators and Service administrators can see the SAO Hierarchy icon so that they can see all the supplier codes (Site Codes) associated to the organizations sharing the same authority Code. See [“SAO Hierarchy” on page 83](#).

- The **Overview** tab displays the following details: Package details area with the package name, package description and approver list. The tab also has an Included Services area that lists other services that might be part of the service package. The tab also shows tiles to display number of sub packages, included services, required approvers for the service package, affiliate

organizations, active and inactive users. Some of the tiles show an arrow  which when clicked takes the user to the respective section in the open package. If the service package includes claim code, UDUNS number is also shown. In case of SAO package, UDUNS Number and Service Authority are also shown. UDUNS is Ultimate Duns.

- The **Sub Packages** tab displays all the subpackages that are part of the selected service package and the following details: sub package name, category, granted date, status, and the Package Information icon  in the Action column. Clicking the icon opens a Package Information box and displays details such as organization name, organization type, additional services included in the subpackage, and required approvers, which shows the role required to approve granting of the subpackage to requestors. The subpackage information is non-editable. See [“Service Packages list page” on page 78](#) to see detailed descriptions.

The subpackages list can be filtered. See [“To filter or refine the list of service packages” on page 79](#).

- The **Claim Codes** only displays if the selected service package includes claim details of type code. The tab displays all the claim values associated with the claim code granted to the current organization.
- The **Remote Claim** only displays if the selected service package includes claim details of type remote.

**For a service package with remote type claim having single claim ID (also called claim code or supplier code)**

For a SAO organization, the tab displays all the claim values associated with the claim code granted for the requested service package with remote type claim. The claim values cannot be deleted and the delete icon is not displayed.

For non-SAO organizations with the same claim code, the tab displays the claim value that is assigned to the current organization for the granted service package with the remote type claim. The listed claim value cannot be deleted. For non-SAO organizations, more claim values can be requested by

clicking the **Request Claim value** icon  and selecting and requesting



individual claim values from the claim values page that opens. If non-SAO organizations have multiple claim value grants, the delete icon becomes available.

**For a service package with remote type claim having multiple claim IDs (also called claim code or supplier code)**

When multiple TLOs request the same service package but use different claim IDs, all these TLOs become a SAO for the claim ID they used while requesting. These TLOs are assigned all the claim values (site codes) associated with that claim ID. These TLOs must be the first ones requesting the same service package but with different claim IDs to become a SAO for each claim ID.

- The **Terms and Conditions** tab displays the description of the terms and conditions for the service package. The page also shows the following:
  - **Initiate Terms & Conditions Review** button: (Only for the Exchange administrator) Click this button if there is a change in the terms and conditions for the service package and you want users to re-accept the terms and conditions. Users granted this service package will be required to re-accept the terms & conditions when they log into the application using single-sign on (SSO).
  - **Export** icon: Use to download the terms and conditions.

### 5.4.2.1 Suspending a service package granted to an organization


To suspend a service package grant, you need to change the service package's status to suspend in the metadata area in the page for the opened service package for the organization.

**To suspend a service package**

1. Turn on the **Set status** switch.

The Suspend selected service package dialog box opens. You are informed about the number of users who are granted this service package and that suspending the selected service package would prevent the users in the organization and divisions from accessing all the services of this service package.

2. In the **Reason** box, provide a reason to suspend the selected service package and then click **Suspend**. This reason is sent to the administrators of all the impacted organizations.

The service package is suspended successfully message displays. The **Set status** changes to **Suspended** and the status flag also switches to **Suspended** .

The **Delete** button becomes available in the lower part of the service package Overview page.

Once suspended, service package grants can be re-activated or removed. To re-activate a service package grant, see "[Activating a suspended service package](#)"

granted to an organization” on page 82. To remove a service package granted to an organization, see “Deleting a suspended service package granted to an organization” on page 82.



**Note:** Use the same procedure to suspend a subpackage granted to an organization.

### 5.4.2.2 Activating a suspended service package granted to an organization


To re-activate a suspended service package grant, you need to change the service package’s status to active in the metadata area in the page for the opened service package for the organization.

#### To re-activate a suspended service package

1. Display the details for the suspended service package that you want to re-activate. See “Viewing service package details” on page 79. You can refine your search for the suspended service package using the procedure “To filter or refine the list of service packages” on page 79.
2. In the metadata area of the selected service package that was suspended, **turn on** the **Set Status** switch.

The Activate selected service package dialog box opens. You are informed about the number of users who are granted this service package and that activating the selected service package would allow all the users in the organization to access all the services of this service package.

3. In the **Reason** box, provide a reason to activate the suspended service package and then click **Activate**. This reason is sent to the administrators of all the impacted organizations.

The service package is activated successfully message displays. The **Set Status** changes to **Active** again and the status flag also switches to **Active** .

### 5.4.2.3 Deleting a suspended service package granted to an organization

To delete a service package grant from an organization, make sure the service package is already in the **Suspended** state. Administrator also needs the **Permanently Remove User Package** permission enabled.

#### To delete a suspended service package grant

1. Display the details for the suspended service package that you want to delete. See “Viewing service package details” on page 79. You can refine your search for the suspended service package using the procedure “To filter or refine the list of service packages” on page 79.
2. In the Overview tab of the selected suspended service package, click the **Delete** button.

The Delete selected service package dialog box opens. You are informed about the number of users who are granted this service package and that deleting the selected service package would prevent the users in the organization and divisions from accessing all the services of this service package.

3. In the **Reason** box, provide a reason to delete the suspended service package and then click **Delete**. This reason is sent to the administrators of all the impacted organizations.

The service package deleted successfully message displays.



**Note:** Use the same procedure to delete a suspended subpackage granted to an organization.

### 5.4.3 SAO Hierarchy

Administrators of IAM Administration need to see the SAO (Service Authority Organization) hierarchy, so that they can see all the supplier codes (also called claim code or claim ID) associated to these organizations in the hierarchy sharing the same authority code.

The IAM application allows companies to create multiple administrative organizations for a single Legal Corporation. For example, a company's European offices may have a completely separate IAM organization from the North American offices' IAM organizations. Most portal packages, such as the Ford and GM Supplier Portals, require relationships between these organizations based on the supplier code. The Service Authority Organization (SAO) is a designation of primary responsibility for all organizations with the same parent supplier code.

SAO is a designation indicating the organization that is ultimately responsible for a parent supplier code. Because supplier codes vary from buyer to buyer, they are associated with partner portal grants to organizations. For each unique partner portal and parent supplier code combination, there is one organization designated as the SAO. This helps the portal owner manage access more easily. Only one portal request per parent supplier code will need to be approved by the Service Administrator of the Portal.


Service Authority Organizations are organizations that have authority over a specific parent supplier code for a specific service.

An organization becomes the SAO by being the first to register and be approved for access with a particular parent supplier code. The SAO designation is valuable when a company has several entities that fall under a single supplier code, but operate as independent top-level organizations (TLO) in OpenText Identity and Access Management. If your organization is the SAO for a service package, you may receive service package and site code (also called claim value IDs) requests from other top-level organizations that share the same parent supplier code.

If your organization is not the SAO for a service package that uses supplier codes, you should be aware that all future requests for subpackages and site codes (also

called claim value IDs) will be routed to the SAO organization's security administrator for evaluation.

A Service Authority Organization has following responsibilities:

 **Tip:** Non-SAO organizations are other top-level organizations that share the same parent supplier code as the SAO organization for a service package.

- Approve requests for the services submitted by non-SAO organizations
- Assign claim value IDs (Site Codes) to non-SAO organizations
- Revoke access to the service from non-SAO organizations

### To view the SAO Hierarchy


1. Log into your organization that has the SAO designation.
2. Navigate to the **Manage Organization** page, open the **Service Packages** tab, and select the service package you want to investigate.

The selected service page opens with the Overview tab as the default page.

For a SAO package, the **Overview** tab displays the **UDUNS Number** and **Service Authority** organization name in addition to other details shown for any other service package. The UDUNS number is the claim code. The organization name shown under Service Authority is the organization with the SAO designation. The **Affiliate Organizations** tile shows the number of organizations associated to the SAO organization through a common authority code.

3. In the Overview page, click the **SAO Hierarchy** icon .

A pane opens with the title **Other Same Authority Organizations** and lists the




SAO organization at the root of the hierarchy indicated by  and other organizations that share the same authority code listed under the root organization. Pointing to the names of the other organizations in the hierarchy

displays inline options to see **Info**  and **Claim Code** . You can use the Claim Code icon to view and assign new claim value IDs. See *"To view and assign claim values for organizations in SAO hierarchy"* on page 85.

Click the  icon to view information about the organization.

### 5.4.3.1 Viewing and assign claim values for organizations in SAO hierarchy

#### To view and assign claim values for organizations in SAO hierarchy

1. Click the inline **Claim Code** icon  for an organization in SAO hierarchy pane.  
A dialog box opens and lists the claim value IDs associated with the organization whose claim code icon you clicked. The dialog box also displays the authorized claim code for the selected service package.
2. To request new claim values for the organization, click the **Assign Claim Values** icon  in the title bar.
3. In the Assign Claim Values of Claim Code <claim code> page, click the **Assign** icon  in the Action column for the claim value ID you want to assign or select multiple claim value IDs and click **Assign** in the Action bar.
4. Click **X** to close the dialog box.

### 5.4.3.2 Changing SAO designation

#### To change SAO designation

When multiple distinct IAM organizations have the same parent claim code (Ultimate DUNS or supplier code) attached to a portal grant, the SAO designation can be switched between those related organizations. The organization that currently has the SAO designation must initiate the process.

The organization with the SAO designation is a top-level organization with the Ultimate DUNS grant. The service package with the same claim authority code should have the attribute *isSaoEnabled* set to *True* in both the SAO and non-SAO organization with the same parent claim code.

1. Log into an SAO organization and navigate to the Manage Organization page.
2. Click the **Service Package** tab and from the listed service packages, select the service package for which you want to change the SAO designation.  
The selected service page opens with the Overview tab as the default page. Notice the current SAO organization name listed as Service Authority. After SAO designation change, the Service Authority information will display the new SAO's name.
3. In the Overview page of the selected service package, click **Change** under **Service Authority**.



**Note:** The Change button only displays for an organization with SAO designation.

The Change button is only available for a SAO organization's Security Administrators and Service Administrators with privilege 20102.



The Change Authority for Application <service package name> dialog box opens and lists other organizations with the same authority code. The dialog box displays the name and address of the organization, and the name of the current application authority. You can filter the contents of the dialog box using the Refine By pane, which shows the Name criteria. Type the name of the organization you want to search for and click **Filter**.


4. Click the organization you want to designate as SAO and click **Submit**.

Successfully requested for change authority message displays.

Name of the new SAO is displayed under the Service Authority label in the Overview page for the selected service package.

5. Click the **SAO Hierarchy** icon .

You will notice that the Other Same Authority Organizations pane now lists the newly designated SAO organization name as the root organization . Point to the organization name and you will see two inline icons: **Info**  and **Claim**

**Code** . You can click the Claim Code icon to view the organization's authorized claim code and associated claim values IDs (also called site codes).


6. Log out of current organization and log into the newly designated SAO organization. Open the **Manage Organization** module and navigate to the Service Packages tab. Select the SAO service package from **Step 2**.

The selected service package in the newly designated SAO organization displays the new SAO's name as the Service Authority. All the claim values IDs that were assigned to the previous SAO are automatically assigned to the new SAO organization. You can see them under the Claim Codes tab.


#### 5.4.4 Assigning a service package to an organization

The Security Administrator of a TLO can assign service packages to users and division that are in its organization's hierarchy

##### To assign a service package to an organization

1. In the Service Packages tab page for the currently open organization, click  and in the list, click **Assign Package**.


The Assign Service Packages page opens and displays a list of service packages that can be assigned to the currently open organization.

2. To filter the list of service packages, click the **Filter** icon  and in the Refine By pane that opens, do the following:

- **Name:** Enter the name of the service package you want to assign.
- **Category:** Click the arrow ▼ to select a category from the listed options such as Administration, Applications, Roles, and so on, to refine the list of service packages by their category.
- **Package Id:** Enter the ID of the Service Package you want to assign to the user.
- **Parent Package Id:** Enter the parent ID of the service package to narrow the list of service packages by the ID of the parent.
- Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine by pane.

The matching records are listed in the Assign Service Packages page. The fields used for the search are shown as tokens above the column names on the page.

- Click the **X** in individual tokens to remove that filter and re-run the search and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** to close the Refine By pane.

3. In the filtered list in the Assign service packages area, click the **Assign** icon  in the **Action** column for the service package that you want to assign to the organization.

The Assign Service Package dialog box opens and displays the following information about the service package:

- Service Package details such as name of the Owning organization, description of the service package, organization name, and organization type.
- **Required Approvers** area that displays the list of approvers. Click the arrow ▼ in the area to expand it.
- **Included Services** area that lists the services that might be included in the service package. The area displays the name, category, description, and URL of the included services.
- **Assign Reason** box to provide a reason for assigning the service package to the organization.

4. In the **Assign Reason** box, enter a reason for assigning the service package to the selected user.
5. If applicable, click the **Terms&Condition** link to read and accept the terms and conditions. Read the information displayed, and click **Accept**.



A check mark shows with the text that I have read and accepted the terms and conditions. The Assign button becomes active.




6. Click **Assign**.  
Service package assigned successfully message displays. The service package that you just assigned no longer displays in the list in the Assign service packages area.
7. Click **X** to close the dialog box.  
The Service Packages tab page displays the assigned service package.


### 5.4.5 Requesting a service package for an organization

Administrators can request service packages for their organizations. After the Organization has access, the administrator can then grant the service packages to the Organization's users.

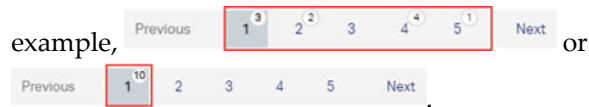
#### To request a service package for an organization

1. In the Service Packages tab page for the currently open top-level organization, click  and in the list, click **Request Package**.  
The Request Service Packages page opens and displays a list of service packages that can be requested for the currently open top-level organization.
2. Follow step 2 onwards in *"To request a service package or subpackage" on page 117*.
3. You can request multiple service packages or a single service package, or a combination of service and subpackages. For multiple packages request, you can select only up to 10 packages. Do one of the following to select packages:
  - To select 10 packages listed on a page, first change the number of items shown on page to 10 per page and then click the check box  adjacent to the **Name** column.
  - Click the check box adjacent to the service packages you want to request. You can only request a maximum of 10 packages at one time.
  - To request one package, just click the **Request** icon  in the Action column for the package you want to request.

The toolbar transforms and shows **Request** and **Selected** with the number of items selected in the list of service packages. You can click the **Show** icon  to expand rest of the page heading area to show the Filter  icon and the page heading. Clicking the **Hide** icon  just shows the Selected and Request options.

Clicking the number of items in Selected **Selected**  displays the names of all of the selected items and provides a **Clear all** option. The page numbers at the bottom of the list also display the number of items selected on each page, for





4. Click **Request** on the Action Bar.
5. In the Request Service Packages dialog box, enter the reason for your request for every package you are requesting to assist the approving administrator make a decision.
6. If applicable, click **Terms&Conditions** link to open the terms and condition for the service package. Click **I Accept** to accept.  
A check mark shows with the text that I have read and accepted the terms and conditions.
7. If requesting a parent service package with claim of type code or remote, you would need to enter the claim ID of the requested service package in the **Claim Code** box.  
After the request is approved, the requested package page would display Claim Code or Remote Claim tab based on the type of the claim for the package you requested. The tab would list the claim value of the parent service package for which you had entered the claim ID during your request submission. In this case, you can not add more claim values.
8. If requesting a subpackage with claim of either type code or remote, then you can select claim values for the parent service package of the requested subpackage.  
After the request is approved, the requested subpackage page would display Claim Code or Remote Claim tab based on the type of the claim for the subpackage you requested. The tab would list the claim value of the parent service package that you had selected during your request submission. You can also add more claim values if they are granted to the parent service package.
9. If requesting a subpackage with claim of type role, then you can select claim values for the parent service package of the requested subpackage.  
After the request is approved, the requested subpackage page would display Claim Roles tab and list the claim ID of the parent service package. On selection of the listed claim ID, another page would open and show the claim values of the parent service package that you had selected during your request submission. You can also add more claim values. See [“To view claim values for a claim ID and request claim values” on page 113.](#)
10. The Send Request button becomes active after all the mandatory fields indicated with an asterisk \* are populated. Click **Send Request**.  
The requested service package no longer displays in the Request Service Packages page.  
The approving administrator for the service package would be notified about your requests. After your request is processed, you would be notified by an email.

- Click the **X** to close the Request Service Packages page.

### Who approves an organization's service package request?

The following table lists the approvers of service package requests based on who the requestor is and who owns the requested service package.

Requestor	Approver
A SAO	Service or Package owner
a top-level non-SAO	SAO Admin
a division	SAO Admin



**Note:** Use the same procedure to request a subpackage for an organization. The parent package of the subpackage must already be granted to the organization.

## 5.5 Pending requests tab for an organization



The tab is only visible to the administrators of the organization.



Administrators can use this tab to view all the pending service package requests by the current organization. The administrators responsible to approve those requests were notified when the requests were submitted. In this tab, current organization's administrator can send reminders to the relevant administrators or delete some of the requests if they are no longer needed.

The Pending Requests list page displays the following details about requests: name of the service package requested, phase of approval, request types, reason for request, and action that can be performed on the listed request such as send reminder to the administrator or cancel request.


Administrators can send reminders to the approvers to approve organizations' pending requests or can cancel one or more or all the pending requests if needed. If the list of pending requests is long, filter the list using the following procedure:

### To filter the list of pending service package requests

- To filter the list, click the **Filter** icon  on the toolbar in the Pending Requests list page.
- In the Refine By pane, do the following to narrow down the list of pending requests:
  - Start Date:** Use the Start Date field to search for requests submitted on a certain date. You can also use the Start Date and End Date fields to search for requests submitted during a specific time frame. Click the calendar icon  and select a date as a start date for the search.


- **End Date:** Click the calendar icon  and select a date as the end date for the search time frame. If no date is selected, the current date is used as the end date.
- **Type:** Click the arrow  in the field to select one of the listed options to filter the list of pending requests by the type of request.
- **Claim ID:** Enter the claim ID of the service package you want to use to filter the list.
- **Claim Value ID:** Enter the claim Value ID of the service package you want to use to filter the list.
- Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine by pane.  
The matching records are listed in the Service packages page. The fields used for the search are shown as tokens above the column names on the page.
- Click the **X** in individual tokens to remove that filter and re-run the search and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** to close the Refine by pane.

#### To send a reminder to the approver of the service package about the pending requests


1. Select all the pending requests by clicking the check box adjacent to the **Service Package Name** column. Alternatively, you can also just click the check box for one request.  
The action bar displays two new options: **Send Reminder** and **Cancel Request**. The action bar also shows the number of selected pending requests.
2. To send a reminder for all the selected pending requests, click **Send Reminder** in the action bar. To send a reminder for one selected pending request, you can either click the **Send reminder**  in the **Action** column or the **Send Reminder** in the action bar.  
The Send Reminder dialog box opens. It provides details about the pending requests.
3. In the **Reminder note** box for each pending request, enter a note to help the administrator make a decision about approving the request and click **Send**.  
The reminder is sent to the approving administrators.

#### To cancel pending requests

1. Select all the pending requests by clicking the check box adjacent to the **Service Package Name** column. Alternatively, you can also just click the check box for one request.  
The action bar displays two new options: **Send Reminder** and **Cancel Request**. The action bar also shows the number of selected pending requests.

2. To cancel all the selected pending requests, click **Cancel Request** in the action bar. To cancel one selected pending request, you can either click the **Cancel Request**  in the **Action** column or the **Cancel Request** in the action bar.

The Cancel pending request dialog box opens. It provides details about the pending requests you are canceling.

 **Note:** If you are canceling pending request for another user, the original requestor receives an email notification about the cancellation.

3. Click **Send**.  
Successfully removed the canceled request message displays.

## 5.6 History tab for an organization

Administrators can use the History tab to see which requests were granted to the currently open organization and all the requests the organization had made for services except the pending requests.

### To open the history tab

1. Open the **Manage Organization** page using instructions in “[Manage Organization](#)” on page 59.
2. Click the **History** tab in the **Home** > <*organization name*> page.  
The History tab opens.

The History tab contains two subtabs: Grant History and Request History

- **Grant History:** Lists all the requests that were granted to the currently open organization and displays the following details: Service ID, Requested package, evaluator who is the approver administrator, decision date, action, such as granted, updated, suspended, unsuspended, or revoked, and status of the granted service package.
- **Request History:** Lists all the service requests the currently open organization had submitted except the requests pending a decision. The following details about the requests are shown: request type, requested package, requested date, evaluator who is the approver administrator, decision date, and status of the requested service.

## 5.7 Administrators tab for an organization

The Administrators tab lists all types of administrators of the currently open organization.






**Note:** The tab is visible to all users of an organization, both administrator type and non-administrator type. But the non-administrator type of users can only see the security administrators for their organization.

### To open the administrator tab

1. Open the **Manage Organization** page using instructions in *OpenText Identity and Access Management - Exchange Operator Help (BNIMCO-H-AGD)*.
2. Click the **Administrators** tab in the **Home** > <organization name> page.

The Administrators tab opens and lists the users of the currently open organization with different types of administrator roles under following five categories:

- **Security Administrators:** Lists the security administrators for an organization.
- **User Account Administrators:** Lists the user account administrators for an organization.
- **Service Administrators:** Lists the service administrators for an organization.
- **Organization Service Administrators:** Lists the organization service administrators for an organization.
- **Individual Service Administrators:** Lists the individual service administrators for an organization.
- In each category, click the arrow  to expand the section to see the name, ID, job title, phone number, and email address of the listed administrators. Click the **Name** column to sort the list by name. Click the arrow  to collapse the section. Point to the  in each section to see a description for the listed administrator role. The title bar shows the number of records in that section.



## 5.8 Quick Search for users and organizations from Home Page

Administrators can use the search option available on the home page to quickly find users or organizations from the home page itself. Use this option for the following searches:


- To search for users in your own organization. See [“Search for users” on page 94](#).
- Use the organization search to search for divisions in your own organization’s hierarchy. See [“Search for organizations” on page 96](#).

### 5.8.1 Search for users

#### To search for users in your own organization


1. On the home page in IAM Administration, click the **Search** icon  in the header area.
2. In the search field, type user name you want to search for. You can use both the first and last name or either the first or the last name.
3. From **Search for**, for user search, select **in Users** option. It is selected by default.
4. Click the **Start Search** icon .

A page opens and displays the results of the user search. The page displays the following:

- Displays all the user names that match the search term. The page shows the following details about the users: name, user name, user ID, organization ID, email address, and user status. You can click the Name column to sort the search results by name.
- **Filter** icon : Use to filter the search results using the criteria on the Refine By pane. See [“To filter or refine the list of users” on page 94](#).
- **Edit Search** icon: Use to edit the search criteria. See [“To edit search criteria” on page 95](#).

You can click the name of an active user to open the details about that user and carry out user-related workflows like assigning service packages and so on. See [“Users tab” on page 64](#).


#### To filter or refine the list of users


1. Click **Filter**  on the page.
2. In the Refine By pane, use one, some, or all of the following options to use as criteria to refine the list and only display the matching requests:

- User status types, **Active, Inactive, Pending, Suspended, Rejected, Locked**: Click one or more status type check boxes to refine the list of users by their status.
- **Username**: Enter both the first and last name or either the first or the last name to find users with matching name.
- **User ID**: Enter the user ID of the user you want to find.
- **Email**: Enter the email address of the user you want to find.
- **Role ID**: Enter the role ID of the user you want to find.
- Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine By pane.  
The matching records are listed in the page. The fields used for the search are shown as tokens above the column names on the page.
- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** to close the Refine By pane.

#### To edit search criteria

After the initial search, you can modify the search criteria from the search results page itself.


1. Click the **Edit search** icon on the toolbar.  
A new area displays under the toolbar and displays the following information:
  - **Users** tab: Displays search fields to search users. It also displays all the user names that matched the initial search for a user.
  - **Organizations** tab: Displays search fields to search organizations. Displays all the organization names that matched the initial search. The page shows the following details about the organizations: organization name, organization ID, organization status, DUNS number, and organization address.
2. You can modify the search in following ways:
  - a. To search for a different user, modify the user name in the **Enter keyword** box and click **Search**.
  - b. In addition to the user name search criteria, you can search for users by the ID of the organization they belong to. To do so, add another row of search criteria by clicking the **Add** icon  next to the Enter keyword box in the first row.  
A new row to provide search criteria is added. Do the following:
    - In the **Search by** field, **Organization Id** is already selected.

- In the middle field, **Contains** is already selected.
  - Provide the organization ID in the **Enter Keyword** field and click **Search**.
- c. In addition to the user name and organization ID search criteria, you can also search for users who are assigned a certain service package and Claim ID. To do so, add another row of search criteria by clicking the **Add** icon  next to the Enter keyword box in the second row.

A new row to provide search criteria is added. Do the following:

- In the **Search by** field, **Claim Id** is already selected.
- In the middle field, select the top level package that is assigned to the user you are searching for. The field lists all the service packages granted to the currently open organization.
- If needed, provide the claim ID value in the **Enter Keyword** field and click **Search**. If you just click the Search without providing a claim ID value, the search would show all the users with matching user name, organization ID, and selected service package.



The search returns all the user names that match the provided name, organization ID, selected service package, and the provided claim ID value.

3. To delete any of the rows, just click the **Delete** icon  for that row.
4. Click **Clear** to reset the fields to default values.

## 5.8.2 Search for organizations

Use the procedures in this section to perform a global search for divisions in your organization.

### To search for divisions in your own organization


1. On the home page in IAM Administration, click the **Search** icon  in the header area.
2. In the search field, type either the full name or a few characters from the name of the division you want to search for.
3. From **Search for**, for organization search, select the **in Organizations** option.
4. Click the **Start Search** icon .

A page opens and displays the results of the organization search. The page displays the following:

- Displays all the organization names that match the search term. The page shows the following details about the organizations: organization name,





organization ID, organization status, DUNS number, and organization address.

- **Filter** icon : Use to filter the search results using the criteria on the Refine By pane. See [“To filter or refine the list of organizations” on page 97](#).
- **Edit Search** icon: Use to edit the search criteria. See [“To edit search criteria for organizations” on page 97](#).

You can click the name of an organization to open the details about that organization and carry out organization-related workflows. See [“Contents of the manage organization page” on page 59](#).


### To filter or refine the list of organizations

1. Click **Filter**  on the page.
2. In the Refine By pane, use one, some, or all of the following options to use as criteria to refine the list and only display the matching requests:
  - **Organization status types, Active, Inactive, Pending, Suspended, Rejected:** Click one or more status type check boxes to refine the list of users by their status.
  - **Package Name:** Enter name of a service package to find organizations that are granted that package.
  - **Package Id:** Enter ID of a service package to find organizations that are granted that package.
  - **isSAO:** Click the arrow  in the field, and from the list, select **No** or **Yes** to find organizations that are either SAO or not.
  - Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine By pane.  
The matching records are listed in the page. The fields used for the search are shown as tokens above the column names on the page.
  - Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
  - Click **Close** to close the Refine By pane.

### To edit search criteria for organizations


After the initial search, you can modify the search criteria from the search results page itself.

1. Click the **Edit search** icon on the toolbar.  
A new area displays under the toolbar and displays the following information:

- **Users** tab: Displays search fields to search users. It also displays all the user names that matched the initial search for a user.
  - **Organizations** tab: Displays search fields to search organizations. Displays all the organization names that matched the initial search. The page shows the following details about the organizations: organization name, organization ID, organization status, DUNS number, and organization address.
2. You can modify the search in following ways:
    - a. To search for a different division, modify the name in the **Enter keyword** box and click **Search**.
    - b. In addition to the name search criteria, you can also search for organizations that are assigned a certain service package and Claim ID value. To do so, add another row of search criteria by clicking the **Add** icon  next to the Enter keyword box in the first row.

A new row to provide search criteria is added. Do the following:

      - In the **Search by** field, **Claim Id** is already selected.
      - In the middle field, select the top level package that is assigned to the organization you are searching for. The field lists all the service packages granted to the currently open organization.
      - If needed, provide the claim value in the **Enter Keyword** field and click **Search**. If you just click the Search without providing a claim value, the search would show all the organizations with matching name and selected service package.

The search returns all the organization names that match the provided name, selected service package, and the provided claim value.
  3. To delete any of the rows, just click the **Delete** icon  for that row.
  4. Click **Clear** to reset the fields to default values.

## 5.9 Unlocking locked user accounts

Exchange operators can unlock locked user accounts.

### To unlock locked user accounts

1. Log into IAM Administration and click the **Locked Accounts** tile on the home page.

The Users tab in the Home > *<current organization name>* opens and lists the users whose accounts are locked.
2. Click the user account that you want to unlock.

The selected user's details open. A lock icon  in the metadata area indicates the user account's locked state.

3. Click **Unlock** on the Overview tab.

If the user's password has not expired, the account is unlocked and is indicated by the unlocked icon in the metadata area.

If the user's password has expired, you would need to reset user's password.

4. On the Security Settings tab, reset user's password. For more information, see ["To reset user password for the selected user" on page 76.](#)

## 5.10 Managing divisions of your organization

Using your organizations hierarchy tree, you can open any of the divisions in the organization and perform the following tasks:

- Viewing the division's profile detail, changing the status of the division such as active or suspended, adding a new user, adding a new division: See ["Viewing a division's profile details" on page 100.](#)
- Viewing the users in the division: See ["Managing users in divisions of your organization" on page 102.](#)
- Managing service packages for the division: ["Managing service packages in divisions of your organization" on page 102](#)
- Viewing the pending requests you made for the division: ["Viewing pending requests for divisions in your organization" on page 103](#)
- Viewing the history of all the requests and the granted requests: ["Viewing service package requests history for divisions in your organization" on page 103](#)
- Viewing the administrators for the division: ["Viewing administrators for divisions in your organization" on page 103](#)

### Notes


- You can also open divisions in your organization using the quick search available in the home page. See ["Search for organizations" on page 96.](#)
- To perform division-related tasks for a certain division in your organization, make sure you have selected and opened that division.

## 5.10.1 Viewing a division's profile details




**Note:** What you see in the user interface is determined by the role and permissions assigned to your profile. The user interface elements, such as fields, labels, and tooltips, that you see in IAM Administration for your organization might be different from the descriptions in the Help and the guide because this application can be configured to suit the needs of any organization.

When a division is selected in an organization's hierarchy tree, it opens in the Home > <Top-Level Organization name> page with the Overview tab selected by default. The page displays the selected division name, organization ID, number of Users and Administrators in the division, and pending requests of the division in the top area of the page which is being referred to as the metadata area. The page also displays an area with six tabs. This is similar to when a top-level organization opens. See ["Contents of the manage organization page" on page 59](#) and ["Overview tab on the manage organization page" on page 61](#) and use this information to work with divisions.

On the Overview tab of a division, the metadata area displays a Set Status switch  to change the status of the division from active to suspended and then back to active if needed.

### To suspend an active division

1. Turn **on** the **Set Status** switch in the metadata area of a division.  
The Suspend selected organization dialog box opens. You are informed about the number of users who are part of this organization and that suspending the organization would prevent the users in the organization from signing into the organization and their accounts would be locked.
2. In the **Reason** box, provide a reason to suspend the organization and then click **Suspend**. This reason is sent to the administrators of all the impacted organizations.


The organization is suspended successfully message displays. The **Set Status** changes to **Suspended** and the status flag also switches to **Suspended** .

The **Delete** button becomes available in the Overview page for the open division.

### Activate the suspended division

1. Display the details for the suspended division that you want to re-activate.
2. Turn **on** the **Set Status** switch in the metadata area of the division.  
The Activate selected organization dialog box opens. You are informed that activating the organization would allow all the users in the organization to sign in the organization again.

3. In the **Reason** box, provide a reason to activate the suspended division and then click **Activate**.

The organization is activated successfully message displays. The **Set status** changes to **Active** again and the status flag also switches to **Active** .

### **To permanently delete a suspended division**

To delete a division, make sure that division is already in the suspended state. Administrator also needs the Permanently Remove User privilege enabled.

1. Display the details for the suspended division that you want to delete.
2. In the Overview tab of the selected suspended division, click the **Delete** button.

The Delete selected organization dialog box opens. You are informed that deleting the organization would remove all users and divisions in the organization.

3. In the **Reason** box, provide a reason to delete the suspended division and then click **Delete**.

The organization deleted successfully message displays.

The deleted division will no longer display in the parent organization hierarchy tree.

### **To add new users to the division**

Divisions are also organizations under a parent organization so the steps to add new users in a division are same as adding users in an organization.

- See [“Adding a new user to your organization” on page 62](#) to add new users in the selected division. You will notice that in the Select Division dialog box, the division name is already selected.

### **To add new subdivisions in the selected division**

Divisions are also organizations under a parent organization so the steps to add subdivisions is same as adding divisions in an organization.

- See [“Adding a new division to your organization” on page 63](#) to add new subdivisions in the selected division. You will notice that in the Select Division dialog box, the division name is already selected.

## 5.10.2 Managing users in divisions of your organization

Divisions are also organizations under a parent organization so you manage the users of a division in similar way as in an organization. See [“Users tab” on page 64](#).

## 5.10.3 Managing service packages in divisions of your organization

Divisions are also organizations under a parent organization so you manage the service packages of a division in similar way as in an organization. See [“Service Packages tab” on page 77](#).

As Security administrator, you are able to manage the service packages for divisions in your organization. You can assign, suspend, and remove service packages from divisions in your organizations.

### 5.10.3.1 Assigning service packages to a division in your organization

Security administrator can assign some service packages and subpackages to divisions in their organization. The division must be at a lower tier in the organization hierarchy, and the parent organization must have access to the service package. Subpackages are designed such that the parent package must be granted before the subpackages become available.

A **service package** is an assignable container that contains at least one service, which is an application or tool, accessed through IAM administration application. Some service packages contain subpackages.

A **subpackage** is an assignable container that contains at least one subservice application.

#### To assign service packages to a division in your organization

- See [“Assigning a service package to an organization” on page 86](#). These instructions also apply to divisions.

### 5.10.3.2 Assigning claim code to a service package in a division

After a service package is assigned to a division, administrator of the division can use the following procedure to assign the initial claim code to the service package.

#### To assign a claim code to a service package

1. Open the division and then open the service package to which you need to assign a claim code in IAM Administration.
2. Click the **Claim Codes** tab.
3. Click **Assign claim code**.

### **5.10.3.3 Suspending, activating, deleting service packages in divisions of your organization**

See “Suspending a service package granted to an organization” on page 81, “Activating a suspended service package granted to an organization” on page 82, and “Deleting a suspended service package granted to an organization” on page 82 for instructions to suspend, activate, and delete service packages for divisions of your organizations. Instructions for a division are the same as for an organization.

### **5.10.4 Viewing pending requests for divisions in your organization**

To view the pending service package requests for any selected division in your organization, see “Pending requests tab for an organization” on page 90. Instructions for a division are the same as for an organization.

### **5.10.5 Viewing service package requests history for divisions in your organization**

To view which service package requests were granted to the selected division of your organization and all the requests the division had made for services except the pending requests, see “History tab for an organization” on page 92. Instructions for a division are the same as for an organization.

### **5.10.6 Viewing administrators for divisions in your organization**

To view all types of administrators of the selected division in your organization, see “Administrators tab for an organization” on page 93. Instructions for a division are the same as for an organization.






## Chapter 6

# My Access Management module

Users can use the My Access Management module to view information about the service packages granted to them and request new service packages, to see all the service package requests they submitted and which are still pending and awaiting approval, and history of package requests granted and history of all requests users had submitted except the ones that are still pending approval.

 **Note:** What you see in the user interface is determined by the role and permissions assigned to your profile. The user interface elements, such as fields, labels, and tooltips, that you see in IAM Administration for your organization might be different from the descriptions in the Help and the guide because this application can be configured to suit the needs of any organization.

### To open the My Access Management page

1. Click the main menu  to open the navigation pane.
2. Click **My Access Management**.


The Home > My Access Management page opens. The page displays a metadata section and three tabs to manage information for the currently logged in user.

- The metadata section displays the user name, phone number, e-mail address, and name of the organization the user belongs to.
- The tabs section displays three tabs: **Service Packages**, **Open Requests**, and **History**.

## 6.1 Service Packages tab

Users can use the Service packages tab to view information about the service packages granted to them and request new service packages.

When the My Access Management page is opened, the Service Packages tab is the first tab on the page and is open by default.

The Service Packages list page displays a Filter icon  and a  icon to show Request Package and Assign Package options. The page also displays details about the service packages. See [“Service Packages list page” on page 106](#).

Users can request one or more service packages. See [“Requesting a service package for yourself” on page 117](#).

The lower part of the Service Packages list page displays the number of records shown on each page **10 per page** which you can change. It also shows the number of pages and the total number of records or items.

#### To change the number of items listed per page setting




- Point the cursor to the number of items per page and from the popup menu, select the number you want to display.


#### To navigate the list of items on all the pages

1. Click **Next** to go to the next page.
2. Click **Previous** to go to the previous page.
3. Click a page number to directly navigate to that page.

### 6.1.1 Service Packages list page

The Service Package list page contains a list of all the service packages and subpackages granted to the currently logged in user and displays the following details:


- **Name:** Name of the service package. If the service package contains subpackages, the arrow  displays adjacent to the package name. Clicking the arrow expands the service package row and displays the list of subpackages.
- **Category:** Category that the service package belongs to such as administration, application, role, and so on.
- **Granted Date:** The date when the service package was granted to the user.
- **Status:** The status of the service package such as active  or suspended .
- **Action:** Displays icons for actions that are permitted for the service package.

Currently it displays the Package Information icon . Clicking the icon opens a Package Information box and displays details such as owner organization name, organization name, organization type, additional services included in the package, and approvers required to approve granting of the package to requestors. The package information is non-editable.

Clicking a service package name would open the package details in another page. See [“Viewing service package details” on page 107](#).

Users can filter or refine the list of service packages to find specific ones or find ones using certain search criteria.

#### To filter or refine the list of service packages

1. Make sure the Service Packages tab is selected and click **Filter**  on the page.



2. In the Refine By pane, use one or both the options to use as criteria to refine the list and only display the matching records:
  - **Status:** Click the arrow ▼ to select either **Active** or **Suspended** to narrow down the list of service packages by their status.
  - **Category:** Click the arrow ▼ to select one of the listed options such as Administration, Applications, Roles and so on to narrow down the list of service packages by their category.
  - Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine By pane.  
The matching records are listed in the Service packages page. The fields used for the search are shown as tokens above the column names on the page.
  - Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
  - Click **Close** to close the Refine By pane.


## 6.1.2 Viewing service package details

To view the details of a listed service package granted to you, use the following procedure:

### To view the details of a service package granted to you

- In the Service Packages tab in the **Home > My Access Management** page, click the name of the service package whose details you want to see.


The service package opens in another page and displays a metadata area with the following information: package name, package ID, package creation date, and Set Status switch to set the service package status to active  or suspended .

The service package can be suspended using the Set Status switch  in the metadata area. Only administrator users with certain permissions can suspend and delete service packages grants. See [“Suspending a service package granted to a user” on page 109](#).

The service package page also displays many tabs based on if it includes sub packages, claim codes, claim roles, remote claim, and so on: **Overview**, **Sub Packages**, **Claim Codes**, **Claim Roles**, **Remote Claim**, and **Service Administrators**.

- The **Overview** tab is always present and displays the following details: Package Details area with the package type, parent service, owning organization and package grantee. If the selected service package has terms and conditions, then the Package Details area also shows a link to open the associated terms and conditions. The tab also has an Included Services area

that lists other services that might be part of the service package. The tab also shows tiles to display number of sub packages, included services, and required approvers for the service package.

- The **Sub Packages** tab displays only if the selected service package includes subpackages. The tab lists all the subpackages that are part of the selected service package. The Sub Packages list page displays the following details: sub package name, category, creation date, approval required, status, and the Package Information icon  in the Action column. Clicking the icon opens a Package Information box and displays details such as owner organization, organization name, organization type, additional services included in the subpackage, and approvers required to approve granting of the subpackage to requestors. The subpackage information is non-editable. See [“Service Packages list page” on page 78](#) to see detailed descriptions.

The subpackages list can be filtered. See [“To filter or refine the list of service packages” on page 79](#).

You can view details of the listed sub package by clicking on a sub package name. The instructions in this procedure also apply to a sub package.



**Note:** For subpackages with certain setting enabled, users can request the subpackage along with the parent service package claim values or claim ID of type role.

For subpackages with certain setting disabled, users can request only the subpackage’s claim values or claim ID of type role.

- The **Claim Codes** tab only displays if the selected service package includes claim details of type code. The tab displays all the claim values associated with the claim code granted to the selected service package for the current user. See [“Claim codes tab” on page 110](#).



**Note:** A service package or subpackage can be granted only one claim of type CODE for a specific user.

- The **Claim Roles** tab only displays if the selected service package includes claim details of type Role. The tab displays all the claim IDs associated with the claim role granted to the selected service package for the current user. See [“Claim Roles tab” on page 113](#).
- The **Remote Claim** tab only displays if the selected service package includes claim details of type Remote. The tab displays the claim value assigned to the current user’s organization for the selected service package with the remote type claim. The user can request more claim values if user’s organization is assigned more claim values by the SAO. See [“Remote Claim tab” on page 115](#).
- The **Service Administrators** tab displays all the users who are assigned the service administrator role in the current organization. See [“Service Administrators tab” on page 116](#).

### 6.1.2.1 Suspending a service package granted to a user


To suspend a service package for the currently logged user, you need to change the service package's status to suspend in the Metadata area in the page for the opened service package.

#### To suspend a service package with active status

1. Turn off the **Set Status** switch for a service package with active status.

The Suspend selected service package dialog box opens. You are informed that suspending the selected service package would prevent you from accessing all the services of this service package.

2. In the **Reason** box, provide a reason to suspend the selected service package and then click **Suspend**.

The service package is suspended successfully message displays. The **Set status** changes to **Suspended** and the status flag also switches to **Suspended** .

The **Delete** button becomes available in the service package Overview page.

After getting suspended, service package grants can be re-activated or removed. To re-activate a service package grant, see [“Activating a suspended service package granted to a user” on page 109](#). To remove a service package granted to a user, see [“Deleting a suspended service package granted to a user” on page 110](#).

### 6.1.2.2 Activating a suspended service package granted to a user

To re-activate a suspended service package grant for the currently logged user, you need to change the service package's status to active in the Metadata area in the page for the opened service package.


#### To re-activate a suspended service package

1. Display the details for the suspended service package that you want to re-activate. See [“Viewing service package details” on page 79](#). You can refine your search for the suspended service package using the procedure [“To filter or refine the list of service packages” on page 79](#).

2. In the metadata area of the selected service package that was suspended, turn on the **Set status** switch.

The Activate selected service package dialog box opens. You are informed that activating the selected service package would allow you access to all the services of this service package.

3. In the **Reason** box, provide a reason to activate the suspended service package and then click **Activate**.

The service package is activated successfully message displays. The **Set status** changes to **Active** again and the status flag also switches to **Active** .

### 6.1.2.3 Deleting a suspended service package granted to a user

To delete a service package grant from a user, make sure the service package is already in the suspended state. Administrator also needs the Permanently Remove User privilege enabled.

#### To delete a suspended service package grant

1. Display the details for the suspended service package that you want to delete. See [“Viewing service package details” on page 79](#). You can refine your search for the suspended service package using the procedure [“To filter or refine the list of service packages” on page 79](#).
2. In the Overview tab of the selected suspended service package, click the **Delete** button.

The Revoke selected service package dialog box opens. You are informed that removing the selected service package would revoke your package grant and you will lose access to all the services of this service package.

3. Click **Delete**.

The service package grant revoked successfully message displays.

### 6.1.2.4 Claim codes tab

The Claim Codes tab lists all the associated claim values for the claim of type code granted to the current user. The Claim Codes tab page displays the authorized claim code for the selected service package.



**Note:** A service package or subpackage can be granted only one claim of type CODE for a specific user.

The page also displays the following details about the associated claim values: claim value ID, claim value name, description, and a set of actions such as **Claim Value**


**Information** icon to see additional information about the claim value and a

**Revoke Claim Value** icon .

#### To delete claim values

1. To delete all listed claim values, click the check box  adjacent to the **Claim Value ID** column name and click **Remove** in the Action bar. Alternatively, to delete just one claim value, click the **Revoke Claim Value** icon in the Action column of the claim value you want to delete.
2. In the Remove dialog box, click **Accept** to confirm removing the claim value.

### To view details of a claim value

1. Click the **Claim Value Information** icon  in the Action column of the claim value whose details you want to view.  
A box opens and displays claim value details such name and address.
2. Click **X** to close the box.

Users can also request new claim values of the claim code. See [“Requesting claim values for claim code” on page 111](#).



#### 6.1.2.4.1 Requesting claim values for claim code

Administrator users can request new claim values for the claim of type code that is granted to them.

For **parent service package** with certain setting enabled, users can request only one claim value.

For **subpackage** with certain setting enabled, users can request the claim values of type code or remote. Users can request the claim values that are granted to the parent service package for an organization.

### To request new claim values

1. Click the **Request Claim Values** icon  in the Claim Codes tab.  
The Request Claim Values of Claim code *<name>* page opens and displays all the claim values that can be requested.
2. In the page, you can select all the available claim values on the page, a few, or just one claim value. Do one of the following as needed:
  - To select all, click the check box  adjacent to the **Claim Value ID** column name.
  - To select a few claim values, click the check box for the claim values you want to request.
  - To request just one claim value, click the **Request** icon  in the Action column for the claim value you want to request.  
One claim value requested successfully message displays.
3. Click **Request** in the Action bar for multiselect request.
4. Click **X** to close the box.

#### 6.1.2.4.2 Requesting ALLACCESS claim value for a claim code

The ALLACCESS claim value is a special type of claim value that when granted to a user for a specific subpackage grants the user access to all claim values for the claim code of the subpackage. Users can request the ALLACCESS claim value. Consider the following prerequisites when requesting the ALLACCESS claim value:



- Can only be requested by a person from an SAO organization and not an organization
- Can only be requested for a subpackage whose parent package is a SAO organization.
- Can be requested along with other claim value IDs under the same claim code but if the ALLACCESS claim value request is approved before the request for other claim value IDs, then the request for other claim value IDs get deleted. The claim code does not need to already have the ALLACCESS claim value for a person to request it. The ALLACCESS claim value is added to the claim code the first time it is requested.
- No additional claim value can be requested under same the claim code if the user is already granted ALLACCESS.



#### Notes

- When the ALLACCESS claim value is granted, pending claim value requests made by the same person requestor under the same claim code of the same sub package are rejected.
- When the ALLACCESS claim value is approved, existing claim values granted to the same person requestor under the same claim code of the same sub package are removed.

#### To request the ALLACCESS claim value

1. Log into an SAO organization with security administrator credentials.
2. Click the  icon > **My Access Management**.
3. In the Service Package tab, click the service package that includes the subpackage where you want to request the ALLACCESS claim value.
4. In the open subpackage page, click the **Claim Codes** tab and click the **Request Claim Value** icon .
5. In the Request Claim Values for Claim Code <code number> page, click the **Select all** check box.  
All the listed claim values on the page are selected and the Request option becomes available on the Action bar.
6. Click **Request** in the Action bar.  
Claim value requested successfully message displays.



- Click **X** to close the box.

Once the claim value is approved, it is listed on the Claim Codes tab listing page in the open selected subpackage page.

### 6.1.2.5 Claim Roles tab


The claim roles tab lists claim IDs associated with the claim of type role that is granted to the selected service package for the current user.

For subpackages with certain setting enabled, users can request the subpackage along with the parent service package claim values or claim ID of type role.


For subpackages with certain setting disabled, users can request only the subpackage's claim values or claim ID of type role.

The page also displays the following details: claim ID, claim type, claim name, description, and a set of actions such as an icon to see additional information about the claim ID and a delete icon.


#### To delete claim IDs

- To delete all listed claim IDs, click the check box  adjacent to the **Claim ID** column name and click **Remove** in the Action bar. Alternatively, to delete just one claim ID, click the **Revoke Claim Id** icon  in the Action column of the claim role to be deleted.
- In the Remove dialog box, click **Accept** to confirm removing the claim ID.

#### To view details of a claim ID

- Click the **Claim Id Information** icon  in the Action column of the claim ID whose details you subpackage to view.  
A box opens and displays claim ID details such name and address.
- Click **X** to close the box.

#### To view claim values for a claim ID and request claim values

- Click a claim ID in the Claim Roles tab listing page.  
The Claim Values <for selected claim ID> page opens. It lists all the claim value IDs for the selected Claim ID that are granted to the current user. Users can perform delete action and can also view details of the claim value ID using the icons in the Action column. See ["To delete claim IDs" on page 113](#) and ["To view details of a claim ID" on page 113](#).
- Administrator users can request claim values by clicking the **Request Claim Values** icon .

The Request claim values of Role Claim <name> page opens and displays all the requestable claim values.


3. In the Request Claim Values page, you can select all the available claim values on the page, a few, or just one claim value. Do one of the following as needed:
  - To select all, click the check box  adjacent to the **Claim Value ID** column name.
  - To select a few claim values or one, click the check box for the claim values you want to request.
4. Click **Request** in the Action bar.  
Claim values requested successfully message displays
5. Click **X** to exit the Request claim values of Role Claim <name> page.

Users can also request new claim values of the claim code. See [“Requesting claim IDs for claim role” on page 114](#).

#### 6.1.2.5.1 Requesting claim IDs for claim role



Administrator users can request new claim IDs for the claim of type Role that is granted to them.

##### To request new claim role


1. Click the **Request Claim Role** icon  in the Claim Roles tab.  
The Request for Claim Roles page opens and displays all the claim IDs that can be requested.
2. In the page, the wizard guides you through steps to request a claim ID. As the first step in the process, select a claim ID by clicking the ID name.
3. Click **Next**.
4. Next, select claim values. You can select all the available claim values on the page, a few, or just one claim value. Click the check box for the claim values to select them.
5. Click **Next**.
6. On the Summary page, review your selections from the previous steps. To make any changes, you can click **Previous** and go back to previous pages and make changes.
7. If you are happy with your selections, click **Submit**.  
Successfully requested claim role message displays. The Request Claim Role page closes and you are back in the Claim Roles tab page. The requested claim role will display here after your request is approved.

### 6.1.2.6 Remote Claim tab


Remote is another type of claim that service packages can have.

The Remote Claim tab page also displays the following details: claim value ID, claim value name, description, and a set of actions such as **Claim Value information** icon  to see information about the claim Value and a **Revoke Claim Value** icon .

#### To revoke claim value

1. To revoke a granted claim value, click the check box  adjacent to the claim value you want to revoke and click **Remove** in the Action bar. Alternatively, you can click the inline icon **Revoke Claim Value**  in the Action column of the claim value to be deleted.
2. In the Remove dialog box, click **Accept** to confirm removing the claim value. Claim value removed successfully message displays.  
User will no longer have access to this package. This happens when the home location code is enabled for a parent package.

#### To view details of the granted claim value


1. Click the **Claim Value information** icon  in the Action column of the claim value whose details you want to view.  
A box opens and displays claim value details such name and address.
2. Click **X** to close the box.


Users can also request new claim values of the remote claim. See [“Requesting claim value for remote claim” on page 115](#).

#### 6.1.2.6.1 Requesting claim value for remote claim

Administrator users can request a claim value for a parent service package with the remote type claim that is granted to them.

#### To request a claim value

1. Click the **Request Claim Values** icon  in the Remote Claim tab.  
The Request claim values of Remote Claim <name> page opens and displays all the requestable claim values that are granted to your organization.
2. On the page, you can select all the available claim values, a few, or just one claim value. Do one of the following as needed:
  - To select all, click the check box  adjacent to the **Claim Value ID** column name.

- To select a few claim values, click the check box for the claim values you want to request.
- To request just one claim value, click the **Request** icon  in the Action column for the claim value you want to request.

One claim value requested successfully message displays. If you request a claim value that is already requested, the application displays a message that the claim value is already requested.


3. Click **Request** in the Action bar for multiple claim values request.
4. Click **X** to exit the page.

### 6.1.2.7 Service Administrators tab





The tab lists all the users with the service administrator role in your organization.

The listing page displays the following details about the service administrator users: name, user ID, job title, email address, phone number and an icon to remove the service administration role from a listed user.

#### To remove the service administrator role from a user

1. To remove the service administrator role from all the listed users, click the check box  adjacent to the **Name** column and click **Remove** in the Action bar. Alternatively, to remove the service administrator role from just one listed user, click the **Delete** icon  in the Action column of the user.
2. In the Remove dialog box, click **Remove** to confirm removing the role from the selected users.


#### To assign the service administrator role to other users

1. Click the **Assign user** icon  in the title bar in the Service Administrators tab.  
The Assign User page opens and lists all the users in your organization with the name, user id, email address, and the Assign this user icon  to assign the user to the role of service administrator.
2. Click the **Assign this user** icon  for the user to whom you want to assign the service administrator role.  
User assigned as service administrator message displays.
3. Repeat the above process as needed.
4. Click the **Back** icon  to go back to previous page.  
The Service Administrators listing page displays the newly assigned user.

### 6.1.3 Requesting a service package for yourself


Users can request service packages and subpackages for themselves from the list of packages that are granted to their organization. Use the same procedure to request subpackages.





#### To request a service package or subpackage


1. Open the My Access Management page. See [“To open the My Access Management page” on page 105](#).
2. On the Service Packages tab, click the  icon and select **Request package** from the list.

The Request Services Packages page opens. It lists the requestable packages that are granted to your organization.

3. You can request multiple service packages or a single service package, or a combination of service and subpackages or just a single subpackage. For multiple packages request, you can select only up to 10 packages. Do one of the following to select packages:

- To select 10 packages listed on a page, first change the number of items shown on page to 10 per page and then click the check box  adjacent to the **Name** column.
- Click the check box adjacent to the service packages you want to request. You can only request a maximum of 10 packages at one time.
- To request one package, just click the  icon in the Action column for the package you want to request.

The toolbar transforms and shows **Request** and **Selected** with the number of items selected in the list of service packages. You can click the **Show** icon  to expand rest of the page heading area to show the Back  and Filter  icons and the page heading. Clicking the **Hide** icon  just shows the Selected and Request options.

Clicking the number of items in Selected **Selected**  displays the names of all of the selected items and provides a **Clear all** option. The page numbers at the bottom of the list also display the number of items selected on each page, for example,



4. Click **Request** on the Action Bar.

5. In the Request Service Packages dialog box, enter the reason for your request for every package you are requesting to assist the approving administrator make a decision.

6. If applicable, click **Terms&Conditions** link to open the terms and condition for the service package. Click **I Accept** to accept.

A check mark shows with the text that I have read and accepted the terms and conditions. The Send Request button becomes active.

7. If requesting a parent service package with claim of type code or remote, you would need to enter the claim value ID of the requested service package in the **Claim Code** box.

After the request is approved, the requested package page would display Claim Code or Remote Claim tab based on the type of the claim for the package you requested. The tab would list the claim value of the parent service package for which you had entered the claim value ID during your request submission. In this case, you can not add more claim values because the user home location flag is enabled for the parent service package.

8. If requesting a subpackage with claim of either type code or remote, then you can select claim values for the parent service package of the requested subpackage. This happens only if certain setting is enabled for the requested subpackage.

After the request is approved, the requested subpackage page would display Claim Code or Remote Claim tab based on the type of the claim for the subpackage you requested. The tab would list the claim value of the parent service package that you had selected during your request submission. You can also add more claim values if they are granted to the parent service package.


9. If requesting a subpackage with claim of type role, then you can select claim values for the parent service package of the requested subpackage. This happens only if certain setting is enabled for the requested subpackage.

After the request is approved, the requested subpackage page would display Claim Roles tab and list the claim ID of the parent service package. On selection of the listed claim ID, another page would open and show the claim values of the parent service package that you had selected during your request submission. You can also add more claim values. See ["To view claim values for a claim ID and request claim values"](#) on page 113.

10. The Send Request button becomes active after all the mandatory fields indicated with an asterisk \* are populated. Click **Send Request**.

The requested service package no longer displays in the Request Service Packages page.

The approving administrator for the service package would be notified about your requests. After your request is processed, you would be notified by an email.

11. Click the **Back** icon  to back to the Service Packages page.
12. Click the **Open requests** tab to see the requested service package or packages listed there.

## 6.2 Open Requests tab

Use the Open Requests tab to see all your currently pending requests.

### To view your pending requests

1. Open the **My Access Management** page. See *“To open the My Access Management page” on page 105.*
2. Click the **Open Requests** tab.


The Open Requests area displays the following details about the pending requests: Name of the service package requested, phase of approval, request types, reason for request, requested date, and action.

Users can send reminders to the approvers to approve their pending requests or can cancel one or more or all the pending requests if needed.

### To send a reminder to the approver of the service package for pending requests

1. Open the My Access Management page. See *“To open the My Access Management page” on page 105.*
2. Click the **Open Requests** tab.
3. Select all the pending requests on one page by clicking the check box adjacent to the **Package Name** column. Alternatively, you can also just click the check box for one request.

The Action bar displays two new options: **Send reminder** and **Cancel request**. The Action bar also shows the number of selected pending requests on the page.

4. To send a reminder for all the selected pending requests, click **Send reminder** in the action bar. To send a reminder for one selected pending request, you can either click the **Send reminder**  in the **Action** column or the **Send reminder** in the Action bar.

The Send Reminder dialog box opens. It provides details about the pending requests.


5. In the **Reminder note** box for each pending request, enter a note to help the administrator make a decision about approving the request and click **Send**.

### To cancel pending requests

1. Open the My Access Management page. See *“To open the My Access Management page” on page 105.*

2. Click the **Open Requests** tab.
3. Select all the pending requests on one page by clicking the check box adjacent to the **Package Name** column. Alternatively, you can also just click the check box for one request.

The Action bar displays two new options: **Send reminder** and **Cancel request**. The Action bar also shows the number of selected pending requests on the page.

4. To cancel all the selected pending requests, click **Cancel request** in the action bar. To cancel one selected pending request, you can either click the **Cancel request**  in the **Action** column or the **Cancel request** in the Action bar.

The Cancel open request dialog box opens. It provides details about the pending requests you are canceling.



**Note:** If you are canceling pending request for another user, the original requestor receives an email notification about the cancellation.

5. Click **Send**.

## 6.3 History tab

Users can use the history tab to see which service package requests were granted to them and all the requests they had made for services except the pending requests.

The History tab contains two subtabs: Grant History and Request History

- **Grant History:** Lists all the service package requests that were granted to you and displays the following details: Requested package, evaluator, decision date, action, such as granted, and status of the granted service package.
- **Request History:** Lists all the service requests the you had submitted except the requests pending a decision. The following details about the requests are shown: request type, requested package, requested date, evaluator who is the role approving the request, decision date, and status of the requested service.



## Chapter 7

# Administration Module



Administrators can use the Administration module to perform the following tasks:

- User group management-related activities such as listing groups, creating groups, and editing groups to add or remove users using the Manage Groups submodule.
- Manage the roles associated with an organization and manage the users assigned to those roles in the IAM Administration application using the Manage Roles submodule.
- View and manage service packages and sub packages that the administrators are authorized to manage for their organization using the Manage Applications submodule.
- Retrieve the user audit and user grant audit history for their organization including divisions using the Audit submodule.



**Note:** What you see in the user interface is determined by the role and permissions assigned to your profile. The user interface elements, such as fields, labels, and tooltips, that you see in IAM Administration for your organization might be different from the descriptions in the Help and the guide because this application can be configured to suit the needs of any organization.

### To access the Administration module

1. Click the main menu  to open the navigation pane.
2. Click the arrow  adjacent to the **Administration** module to expand the menu.

The Administration module contains submodules Manage Groups, Manage Roles, Manage Applications, and Audits. Select any of the submodules to open related pages.

## 7.1 Manage Groups

IAM Administration supports User Group Management (UGM) by providing the ability to create groups of users for locating, contacting, and coordinating cross-community collaboration with other community members. It enables creation of virtual teams and community.

Administrators can use the Administration > Manage Groups module for UGM.


On OpenText Supplier Portal side, User Group Management is a tool within Directed Communications, Core Share, Alerts, and Polls widgets. An administrator can create groups of users, for distributing the information created in these widgets.

Groups in IAM Administration have two visibility types:



- **Private:** Such groups are only visible to the group owner
- **Public:** Such groups are visible to everyone with the same OEM service package

Groups are collection of different types of members such as users of an organization, TLOs of an organization, service packages, applications, service package claims, and groups.

In IAM Administration, groups are of the following types:



 **Note:** The group type is controlled by templates created by APIs on the IAM platform side.

- **Subscription:** A group type to create subscription categories that supplier users can subscribe to on the OpenText Supplier Portal in the Directed Communications widget. If a bulletin is created with distribution to a subscription category that a supplier user subscribes to then that user will receive the bulletin in an email.



Subscription groups can be public or private as depicted with these icons  and , respectively.

Subscription groups can only comprise of organizations and other groups of restricted type.



- **Restricted:** A group type used to create groups of just service packages.



Restricted groups can be either public or private as depicted by these icons  and , respectively.

Restricted groups are used to create subscription groups also. When an organization is added to a restricted subscription group, it is granted all the subpackages that are in the restricted service package group. In addition, the organization loses grants to subpackages that are not in the restricted group. If this is a SAO organization, then all the non-SAO organizations also display the same behavior.


- **All Types:** A group type that can include members of following types: users, organizations, service packages, applications, claims, and groups. All types groups can be either public or private as depicted by these icons  and , respectively.

### To open the Manage Groups page

1. Click the main menu  to open the navigation pane.
2. Click the arrow  adjacent to the **Administration** module to expand the menu.
3. Click **Manage Groups**.  
The Home > Administration: Manage Groups page opens.

The Manage Groups page contains a Filter icon , an Add Group icon , and a list of all of the groups the current user is authorized to view and related details.

Use the Filter icon to open a Refine By pane, which provides options to refine the list of groups using the provided criteria.

The lower part of the Manage Groups page displays the number of records shown on each page , which you can change. It also shows the number of pages and the total number of records or items.

### To change the number of items listed per page setting




- Point the cursor to the number of items per page and from the popup menu, select the number you want to display.

### To navigate the list of items on all the pages

1. Click **Next** to go to the next page.
2. Click **Previous** to go to the previous page.
3. Click a page number to directly navigate to that page.

## 7.1.1 Manage Groups page

The Manage Groups page contains a list of all the groups an administrator type of user is authorized to view and manage, and displays the following details about the groups:


- **Group Name:** Name of a group. Groups are of public and private kind.
- **Description:** Description about the group.
- **Owner:** The name of the organization the group is associated with.
- **Last Updated:** Shows the name of the administrator user who created this group. It also shows the date and time the group was created.
- **Visibility:** Whether the group is public or private. Public groups are visible to all administrators. Private groups are visible only to administrators who created the group.
- **Action:** Displays icons for actions that are permitted for the group such as Add Member  to the group, Remove Member  from the group, and Delete Group .

Clicking a group name would open the group details in another dialog box. See [“View and edit group details” on page 125](#).

### 7.1.1.1 Filter groups

As an administrator, you can filter or refine the list of groups to find specific ones or find ones using certain search criteria.

#### To filter or refine the list of groups

1. In the Manage Groups page, click **Filter** .
2. In the Refine by pane, use one or some or all options to use as criteria to refine the list and only display the matching groups:
  - **Group Name:** Enter the name of a group that you want to filter. You can use the wildcard asterisk \* along with a few characters from a group name to find all groups whose name matches those characters and any other characters represented by the asterisk in the search term.
  - **Type:** Click the arrow and from the list, select either **Unlock** or **Lock**. This option is used to find groups, of locked and unlocked types, that existed in an OEM prior to Administration.
    - **Unlock:** Use Unlock to find all those groups that can be modified or deleted.
    - **Lock:** Use Lock to find all those groups that cannot be deleted.

- **Member Type:** Click the arrow and from the list, select from Organization, Person, Service Package, Application, Service Package Claim, and Group.
  - **Organization:** Use Organization to find all those groups that contain members of this member type.
  - **Person:** Use Person to find all those groups that contain members of this member type.
  - **Service Package:** Use Service Package to find all those groups that contain members of this member type.
  - **Application:** Use Application to find all those groups that contain members of this member type.
  - **Service Package Claim:** Use Service Package Claim to find all those groups that contain members of this member type.
  - **Group:** Use Groups to find all those groups that contain members of this member type.
- Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine by pane.
 



The matching records are listed in the Manage Groups page. The fields used for the search are shown as tokens above the column names on the page.
- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** to close the Refine by pane.

### 7.1.1.2 View and edit group details


Administrators can view the details of a group and can add new members to the group.

#### To view and edit the details of a group

1. In the Manage Groups page, after refining the listed records if needed, click the name of the group whose details you want to view.
2. The Edit Group dialog box opens and displays the following details:
  - **Select Template:** Shows the name of the template used for the group. The value cannot be edited. The template selected in this field controls the group type.
  - **Name** of the group, **Assigned Group Owner**, **Description** of the group, **Group Visibility Type** whether the group is public or private : The values in all these fields can be edited.
    - To edit the name and description, simply type the new name and description in the respective fields.

- To change the group owner, use the **Change** option. See *“To change assigned group owner of a group”* on page 126.
  - To change the group visibility type, click either **Public group** or **Private group**.
  - **Assigned Members:** This section shows the members who are part of the group.
    - You can add more members to the group using the **Assign Members** icon . Based on the group type you are editing, see the steps to assign members in the appropriate procedure: *“Create a restricted group”* on page 130, *“Create a subscription group”* on page 131, or *“Create an all type group”* on page 135.
    - To remove a member from the group, point to that member and then click the Remove icon . Click **Remove** in the confirmation dialog box. Member removed successful message is shown. Click **Save**.
3. Click **Save** if you edited any of the details. Click **Cancel** to ignore the edits and click **X** to close the dialog box.
- A message that the group was updated successfully is shown.

#### To change assigned group owner of a group

1. Click **Change** adjacent to the group owner name in the Edit Group dialog box.
  2. In the Change Owner dialog box, click the row for the member who you want to assign as the new owner to the group.
  3. Click **Assign**. To cancel changing the group owner, click either the **Cancel** or **Back** icon  in the title bar of the Change Owner dialog box.

The Change Owner dialog box closes, and the selected owner is shown in the Assigned Group Owner field in the Edit Group dialog box.
  4. Click **Save**.
- A message that the group was updated successfully is shown.


#### 7.1.1.2.1 Assign group members to a group

Administrators can assign members to an existing group in two ways:


- from the Manage Groups page. See *“To assign members to a group from the Manage Group page”* on page 127.
- from the Edit Group page. See *“To assign members to a group using the Edit Group dialog box”* on page 127.

To assign members to a group, both options use the Member List dialog box.

### To assign members to a group using the Edit Group dialog box

1. In the Manage Groups page, after refining the listed records if needed, click the name of the group whose details you want to view.
2. With the Edit Group dialog box open for a group in which you want to add more members, click **Assign Members** icon . Based on the group type you are editing, see the steps to assign members in the appropriate procedure: [“Create a restricted group” on page 130](#), [“Create a subscription group” on page 131](#), or [“Create an all type group” on page 135](#).
3. Click **Save** in the Edit Group dialog box.

### To assign members to a group from the Manage Group page

1. In the Manage Groups page, if needed filter the list of groups to find the one to which you want to assign members. See [“Filter groups” on page 124](#).
2. After you locate the group record in the list, click the **Add Member** icon  in the **Action** column for that group.

The Member List dialog box opens. Based on the group type you are editing, see the steps to assign members in the appropriate procedure: [“Create a restricted group” on page 130](#), [“Create a subscription group” on page 131](#), or [“Create an all type group” on page 135](#)

- **Adding members to a restricted group:** In the Member list: Service Packages dialog box, select the packages you want to add, adjust their access settings if applicable by clicking the switch on or off in each column. The on or off default settings of the three access settings Auto grant package, Cascade to Divisions, and Auto grant to users, in the Member List dialog box is controlled by the settings of the group level access settings in the Create Group dialog box. For information about access settings, see [Step 3](#).

The access settings may not be available in some cases if the group opened uses a template that did not provide the options for access settings.

- **Adding members to a subscription group:** In the Member List dialog box, to add more organizations, on the **Organizations** tab, select the organizations you want to add as new members to the group, adjust their access settings if applicable by clicking the switch on or off in each column. The on or off default settings of the three access settings Auto grant package, Cascade to Divisions, and Auto grant to users, in the Member List dialog box is controlled by the settings of the group level access settings in the Create Group dialog box. For information about access settings, see [Step 2](#).

The access settings may not be available in some cases if the group opened uses a template that did not provide the options for access settings.



**Note:** A subscription group can include only one restricted group as a member. To add another restricted group to a subscription group, first

remove the existing restricted group from the subscription group, and then add a new restricted group to the subscription group.




3. Click **Assign** in the Member List dialog box.  
Group updated successfully message displays.

#### 7.1.1.2.2 Remove members from a group


Administrators can remove members from a group in two ways:

- from the Manage Groups page. See [“To remove members from a group from the Manage Group page” on page 128.](#)
- from the Edit Group dialog box. See [“To assign members to a group using the Edit Group dialog box” on page 127.](#)

##### To remove members from a group from the Manage Group page

1. In the Manage Groups page, if needed filter the list of groups to find the one from which you want to remove members. See [“Filter groups” on page 124.](#)
2. After you locate the group record in the list, click the **Remove Member** icon  in the **Action** column for that group.
3. In the Remove Members dialog box, click the **Remove** icon  for the member you want to remove.
4. Click **Remove** in the confirmation dialog box.  
1 group member removed successfully message is shown.
5. Repeat [Step 3](#) and [Step 4](#) if needed.
6. Click the **Back** icon  to close the Remove Members dialog box and go back to the Manage Groups page.

##### To remove members from a group using the Edit Group page


1. With Edit Group dialog box open for a group, perform the following steps. See [“View and edit group details” on page 125.](#)
2. In the **Assigned Members** box, to remove a member from the group, point the cursor to the member you want to remove and then click the **Remove** icon .
3. Click **Remove** in the confirmation dialog box.  
Member removed successful message is shown.
4. Click **Save**.  
Group updated successfully message displays.




### 7.1.1.3 Create a new group

Administrators can create new groups of different types and assign members to them.

#### To create a new group

1. In the Manage Groups page, click the **Add Group** icon  in the title bar of the page.
2. In the Create Group dialog box, do the following to populate the fields to create the new group:


All the mandatory fields are marked with an asterisk.


- a. **Select Template:** Click the arrow  in the field, and from the list, select a template to use for the new group. The selected template controls the group type and the some of the fields shown in the dialog box.
  - To create a subscription group, select a subscription template.
  - To create a restricted group, select a template for a restricted group.
  - To create an all type group. select a template for an all type group.
- b. **Name:** Type a unique name for the new group.
- c. **Assigned Group Owner:** Shows the name of the owner of the group.
- d. **Description:** Enter a description about the new group.
- e. **Group Visibility Type:** Click either **Public group** if the group would be visible to all administrators or **Private group** if the group would only be visible to the administrator who is creating the group.
- f. The procedure to add assigned members is different for the various group types. Based on the group you are creating, select the appropriate procedure to see the remaining steps to create a group:
  - For the remaining steps to create a restricted group, see [“To create a restricted group” on page 130.](#)
  - For the remaining steps to create a subscription group, see [“To create a subscription group” on page 131.](#)
  - For the remaining steps to create an all types group, see [“To create an all types group” on page 135.](#)

### 7.1.1.3.1 Create a restricted group

To create a restricted group, use the following procedure:

#### To create a restricted group

1. After following the [Step 2.a](#) to [Step 2.e](#) in “To create a new group” on page 129, follow the steps in this procedure.
2. In **Restriction Setting**, the **Set Restriction** check box is selected by default. Leave this option unchanged.
3. In **Access Settings**, the **Auto grant package**, **Cascade to Divisions**, and **Auto grant to Users** check boxes are selected by default, controlled by how they are configured in the selected group template. These settings are at the group level. You can leave the default settings unchanged or clear the check boxes if you want to stop the automatic grant of subpackages to organizations, divisions, or users at the group level when this restricted group is included as a member in a subscription group. You can control these settings also at member level.
  - **Auto grant package:** If checked, organizations added to the group are automatically granted all the subpackages that are part of the restricted group added to this subscription group.
  - **Cascade to Divisions:** If checked, divisions of the organizations added to the group are also automatically granted all the subpackages that are part of the restricted group added to this subscription group.
  - **Auto grant to Users:** If checked, users of the organizations added to the group are automatically granted all the subpackages that are part of the restricted group added to this subscription group.
4. In **Assigned Members**, click **Assign Members** icon  to add members to the group.

The Member List dialog box opens and lists all the service packages granted to the current organization.
5. Filter the list of service packages if needed using the following steps:
  - a. Click the **Filter** icon  in the title bar.
  - b. In the Refine by pane, use one or more options to use as criteria to refine the list and only display the matching members:
    - i. **Status:** Click the arrow and from the list, select **Active** or **Suspended** to only display either all the packages with active status or packages with suspended status, respectively.
    - ii. **Category:** Click the arrow and from the list, select one of the categories to only display the packages associated with the selected category.
    - iii. Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.


The matching records are listed in the Manage Groups page. The fields used for the search are shown as tokens above the column names on the page.

- iv. Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
  - v. Click **Close** to close the Refine by pane.
6. Select the service packages to include in the restricted group by clicking the check box adjacent to the package name. To include subpackages from parent service packages, expand the parent service package by clicking the arrow near the package name and from the expanded list of subpackages, select the subpackages to include.



**Note:** Maximum of 10 service packages and subpackages can be selected.

7. Click **Assign**. To cancel assigning selected service packages to the new group, either click **Cancel**.

The Member List dialog box closes, and the selected members are assigned to the group and listed in the Assigned Members box. The following columns are displayed for the selected packages: Member ID, access settings: Auto grant package, Cascade to Divisions, and Auto grant to Users, and the Remove option in the Action column. Point to a row to see the Remove icon  in the Action column.

The access settings shown for the member packages in the Assigned Members box are at the member level. Each access setting column displays a switch to change the setting to on or off. For description of these access settings, see [Step 3](#).

8. Repeat [Step 4](#) to [Step 6](#) to add more members to the group if needed.
9. Click **Create** in the dialog box.  
Group created successfully message displays. The newly created group displays on the top in the Manage Groups page.


#### 7.1.1.3.2 Create a subscription group

To create a subscription group, use the following procedure:

##### To create a subscription group


1. After following the [Step 2.a](#) to [Step 2.e](#) in “[To create a new group](#)” on page 129, follow the steps in this procedure.
2. In **Access Settings**, the **Auto grant package**, **Cascade to Divisions**, and **Auto grant to Users** check boxes are selected by default, controlled by how they are configured in the selected group template. These settings are at the group level.

You can leave the default settings unchanged or clear the check boxes if you want to stop the automatic grant of subpackages to organizations, divisions, or users at the group level. You can control these settings also at member level.

- **Auto grant package:** If checked, organizations added to the group are automatically granted all the subpackages that are part of the restricted group added to this subscription group.
  - **Cascade to Divisions:** If checked, divisions of the organizations added to the group are also automatically granted all the subpackages that are part of the restricted group added to this subscription group.
  - **Auto grant to Users:** If checked, users of the organizations added to the group are automatically granted all the subpackages that are part of the restricted group added to this subscription group.
3. In **Assigned Members**, click the **Assign Members** icon  to add members to the group.


The Member List dialog box opens and displays two tabs: **Organizations** and **Groups**.

The **Organizations** tab lists all the top-level organizations (TLO) in the current OEM (original equipment manufacturer).

The **Groups** tab displays all the restricted groups created in the current organization.
  4. Filter the list of organizations if needed using the following steps:
    - a. Click the **Filter** icon  in the Organizations title bar.
    - b. In the Refine by pane, use one or more options to use as criteria to refine the list and only display the matching members:
      - i. **Name:** Enter a few characters or full name of the organization to find matching organizations.
      - ii. **Status:** Click the arrow and from the list, select one of the listed statuses such as **Active**, **Suspended**, **Pending** or **Rejected** to only display all the organizations that match the selected status.
      - iii. **Category:** Click the arrow and from the list, select one of the categories to only display the packages associated with the selected category.
      - iv. Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.

The matching records are listed in the Manage Groups page. The fields used for the search are shown as tokens above the column names on the page.
      - v. Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.

- vi. Click **Close** to close the Refine by pane.
5. Select the organizations to include in the subscription group by clicking the check box adjacent to the organization name. You can select multiple organizations.
6. Click **Assign**. To cancel assigning selected organizations to the new group, click **Cancel**.

The Member List dialog box closes, and the selected organizations are assigned to the group and listed in the Assigned Members box. The following columns are displayed for the organizations: Member ID, access settings: Auto grant package, Cascade to Divisions, and Auto grant to Users, and the Remove option in the Action column. Point to a row to see the Remove icon  in the Action column.

The access settings shown for the member organization in the Assigned Members box are at the member level. Each access setting column displays a switch to change the setting to on or off. Default setting is on for all the three access settings controlled by group-level access settings. If needed, you can change the member-level setting. For description of these access settings, see [Step 2](#).


7. In **Assigned Members**, click the **Assign Members** icon  to add group members to the group.

The Member List dialog box opens and displays two tabs: **Organizations** and **Groups**.

8. Click the **Groups** tab.

The **Groups** tab displays all the restricted groups created in the current organization.

To filter the list of groups, do the following:

- a. Click the **Filter** icon  in the Manage Groups title bar.
- b. In the Refine by pane, use one, more, or all of the options to use as criteria to refine the list and only display the matching members:
  - **Group Name:** Enter the name of a group that you want to filter. You can use the wildcard asterisk \* along with a few characters from a group name to find all groups whose name matches those characters and any other characters represented by the asterisk in the search term.
  - **Active:** Click the arrow and from the list, select either **False** or **True**.
  - **Owner Id:** Enter the group owner ID to find all the groups associated with this owner.
  - **Member Type:** Click the arrow and from the list, select from Organization, Person, Service Package, Application, Service Package Claim, and Group.

- **Organization:** Use Organization to find all those groups that contain members of this member type.
  - **Person:** Use Person to find all those groups that contain members of this member type.
  - **Service Package:** Use Service Package to find all those groups that contain members of this member type.
  - **Application:** Use Application to find all those groups that contain members of this member type.
  - **Service Package Claim:** Use Service Package Claim to find all those groups that contain members of this member type.
  - **Group:** Use Groups to find all those groups that contain members of this member type.
- Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.  
The matching records are listed in the Manage Groups page. The fields used for the search are shown as tokens above the column names on the page.
  - Click the **X** in individual tokens to remove that filter and re-run the search and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
  - Click **Close** to close the Refine by pane.
9. Select the group to include in the subscription group by clicking the check box adjacent to the group name.



**Note:** You can only select one restricted group to add as a member to the subscription group.

10. Click **Assign**. To cancel assigning the selected restricted group to the new subscription group, click **Cancel**.  
The Member List dialog box closes, and the selected restricted group is assigned to the new subscription group and listed in the Assigned Members box.
11. Click **Create** in the dialog box.  
Group created successfully message displays. The newly created group displays on the top in the Manage Groups page.

### 7.1.1.3.3 Create an all type group

To create an all types group, use the following procedure:

#### To create an all types group

1. After following the [Step 2.a](#) to [Step 2.e](#) in “[To create a new group](#)” on page 129, follow the steps in this procedure.


2. In **Assigned Members**, click the **Assign Members** icon  to add members to the group.

The Member List dialog box opens and displays multiple tabs as configured in the template such as:





- The **Users** tab lists all the users in the current organization.
- The **Organizations** tab lists all the top-level organizations (TLO) in the current organization.
- The **Service Packages** tab lists all the service packages granted to the current organization.
- The **Application** tab lists all the services granted to the current organization.
- The **Claims** tab lets you select a parent service package with claim code and claim values granted to the current organization and then assign those claim values to a group.
- The **Groups** tab displays all the restricted groups created in the current organization.

3. To add users to the new all type group, use the Users tab.

To filter the list of users, use the following steps:

- a. Click the **Filter** icon  in the Users title bar.
- b. In the Refine by pane, use one, more, or all of the options to use as criteria to refine the list and only display the matching user records:
  - **User status types, Active, Inactive, Pending, Suspended, Rejected:** Click one or more status type check boxes to refine the list of users by their status.
  - **First Name:** Enter the first name to find users with matching first name.
  - **Last Name:** Enter the last name to find users with matching last name if first name is not entered or matching combination of first and last name.
  - **Username:** Enter the user name of the user you want to find.
  - **Email:** Enter the email address of the user you want to find.
  - **Role Id:** Enter the role ID of the user you want to find.
  - **Attribute Name:** Enter the name of an attribute to find all users who have matching attribute name.

- **Attribute Value:** Enter the value of an attribute to find all users who have matching attribute value.
- **Grant Attribute Value:** Enter the grant attribute value to find all users who have matching grant attribute value.
- Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.  
The matching records are listed in the Users page. The fields used for the search are shown as tokens above the column names on the page.
- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** to close the Refine by pane.




4. Select the users to include in the new all types group by clicking the check box adjacent to the user name. You can select maximum of 10 users.
5. Click **Assign**. To cancel assigning selected users to the new group, click **Cancel**.  
The Member List dialog box closes, and the selected users are assigned to the group and listed in the Assigned Members box.
6. To add organizations as members to the new group, click the **Assign Members** icon  in **Assigned Members** box.  
The Member List dialog box opens. To add TLO to a group, follow [Step 3 to Step 6](#) in [“To create a subscription group” on page 131](#).
7. To add service packages as members to the new all types group, click the **Assign Members** icon  in **Assigned Members** box.  
The Member List dialog box opens. To add service packages to the new all type group, follow [Step 4 to Step 7](#) in [“To create a restricted group” on page 130](#).
8. To add any type of existing groups as members to the new group, click the **Assign Members** icon  in **Assigned Members** box.  
The Member List dialog box opens. To add an existing group to the new all type group, follow [Step 8 to Step 10](#) in [“To create a subscription group” on page 131](#).
9. To add services as members to an all types group, click the **Assign Members** icon  in **Assigned Members** box. Then, click the **Application** tab in the Member List dialog box.




**Note:** Applications are services. The names are being used interchangeably.

To filter the list of services, use the following steps:



- a. Click the **Filter** icon  in the Application title bar.
  - b. In the Refine by pane, use one, more, or all of the options to use as criteria to refine the list and only display the matching user records:
    - **Grant Status:** Click the arrow and from the list, select one of the listed statuses such as **Active**, **Suspended**, or **Unactivated** to only display services with matching grant status.
    - **Category:** Click the arrow and from the list, select one of the categories to only display the services associated with the selected category.
    - **Application Name:** Enter the name of a application that you want to find. You can use the wildcard asterisk \* along with a few characters from an application name to find all services whose name matches those characters and any other characters represented by the asterisk in the search term.
    - **Service Package ID:** Enter the ID of the parent service package to find all the services that have matching parent package ID.
    - Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.  
The matching records are listed in the Users page. The fields used for the search are shown as tokens above the column names on the page.
    - Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
    - Click **Close** to close the Refine by pane.
10. Select the services to include in the new all types group by clicking the check box adjacent to the service name. You can select maximum of 10 services.
  11. Click **Assign**. To cancel assigning the selected services to the new group, click **Cancel**.  
The Member List dialog box closes, and the selected services are assigned to the new group and listed in the Assigned Members box. A service is depicted by this icon .
  12. To add Service Package Claims as members in the new all types group, click the **Assign Members** icon  in **Assigned Members** box. Then, click the **Claims** tab in the Member List dialog box.  
The Claims tab opens and displays a list to Select Parent Package from.
  13. From the list of parent service packages, select one with claim code and claim values.  
The Package Claims table displays and the associated claim value IDs are listed.

14. Select the claim ID to include in the new all types group by clicking the check box adjacent to the claim ID.
15. Click **Assign**. To cancel assigning the selected claim ID to the new group, click **Cancel**.


The Member List dialog box closes, and the selected claim ID is assigned to the new group and listed in the Assigned Members box. Claim ID is depicted by this icon .

16. Click **Create** in the dialog box.  
Group created successfully message displays. The newly created group displays on the top in the Manage Groups page.

#### 7.1.1.4 Delete a group

Administrators with certain privileges can view and delete groups in the Manage Groups page.



##### To delete a group

1. In the Manage Groups page, if needed filter the list of groups to find the one you want to delete. See [“Filter groups” on page 124](#).
2. After you locate the group record to delete in the list, click the **Delete Group** icon  in the **Action** column for that group.
3. Click **Delete** in the confirmation message.  
Group deleted successfully message displays.

## 7.2 Manage Roles


Administrators can manage the roles associated with an organization and manage the users assigned to those roles in the IAM Administration application using the Manage Roles submodule in the Administration module.

Roles can be of the following types:


- **Immutable:** Such roles cannot be modified or deleted. Immutable roles are depicted using this icon .
- **Mutable:** Such roles can be modified or deleted. Mutable roles are depicted using this icon .

##### To open the Manage Roles page

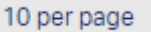
1. Click the main menu  to open the navigation pane.

2. Click the arrow  adjacent to the **Administration** module to expand the menu.
3. Click **Manage Roles**.

The Home > Administration: Manage Roles page opens.

The Manage Roles page contains a Filter icon  and a list of all of the roles associated with the organization and related details. See [“Manage roles page” on page 139](#).

Use the Filter icon to open a Refine By pane, which provides options to refine the list of roles using the provided criteria. See [“Filter roles” on page 140](#).

The lower part of the Manage Roles page displays the number of records shown on each page  which you can change. It also shows the number of pages and the total number of records or items.

#### To change the number of items listed per page setting



- Point the cursor to the number of items per page and from the popup menu, select the number you want to display.

#### To navigate the list of items on all the pages

1. Click **Next** to go to the next page.
2. Click **Previous** to go to the previous page.
3. Click a page number to directly navigate to that page.

### 7.2.1 Manage roles page

The Manage Roles page contains a list of all of the roles associated with an organization and displays the following details about the roles:


- **Role Name:** Name of a role.
- **Role Type:** Type of a role.
- **Owning Organization:** The name of the organization the role is associated with.
- **Action:** Displays icons for actions that are permitted for the role such as Add Users  and Remove Users . For immutable roles, the column does not show any icons because these roles cannot be modified or deleted.

Clicking a role name would open the role details in another dialog box. See [“View role details” on page 140](#).

### 7.2.1.1 Filter roles

As an administrator, you can filter or refine the list of roles to find specific ones or find ones using certain search criteria.

#### To filter or refine the list of roles

1. In the Manage Roles page, click **Filter** .
2. In the Refine by pane, use one or both options to use as criteria to refine the list and only display the matching roles:
  - **Role Name:** Type a role name.
  - **Immutable:** Click the arrow and from the list, select either **False** or **True**.
    - **False:** Use False to find all those roles that can be modified or can be deleted.
    - **True:** Use True to find all those roles that cannot be modified or deleted. They are immutable.
  - Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.


The matching records are listed in the Manage Roles page. The fields used for the search are shown as tokens above the column names on the page.
  - Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
  - Click **Close** to close the Refine by pane.

### 7.2.1.2 View role details

Administrators can view the details of a role such as all the users who are assigned that role. They can add new users to that role or remove existing users from that role.

#### To view the details of a role

1. In the Manage Roles page, after refining the listed records if needed, click the role whose details you want to view.
2. A dialog box with the selected role's name opens and displays the following details:
  - **Role Name, Description, Role Type, Role Code:** The name, description, type, and code of the selected role are shown. The values in these fields cannot be edited.

- **Assigned Users:** This section shows the number of users who are assigned this role and, when expanded by clicking the arrow , lists all these users and related details.


### 7.2.1.3 Add users to a role

Both active and inactive users can be added to a role. You can add single or multiple users at the same time, up to a maximum of 20, to a role.

There are two ways to add users to a role:


- From the role details dialog box. See [“To add users to a role from the role details dialog box” on page 141](#).
- From the Manage Roles page. See [“To add users to a role from manage Roles page” on page 142](#)

#### To add users to a role from the role details dialog box


1. Follow the steps in [“View role details” on page 140](#) to open the role dialog box to view the role details.
2. Click the arrow  in the **Assigned Users** section.

3. In the expanded assigned users section, click **Add Users** .

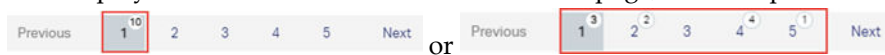
The User List dialog box opens and displays a list of active and inactive users and their details such as user name, user ID, job title, email address, and their status that shows if they are active or inactive.

4. In the User List dialog box, do the following to filter and select one or more users to assign to the role:
  - Click the Filter icon  to open the Refine by pane and refine the list of users using the following criteria or fields:
    - **First Name:** Enter the first name to find users with matching first name.
    - **Last Name:** Enter the last name to find users with matching last name if first name is not entered or matching combination of first and last name.
    - **User Id:** Type the user ID of the user you want to add to the role.
    - **Email:** Type the email ID of the user who you want to add to the role.
    - **Package Id:** Type the package ID associated with the user you want to add to the role.
    - **Claim Id:** Type the claim ID associated with the user you want to add to the role.
    - Click **Filter** to narrow down the list of users using the specified criteria. Click **Close** or the **Filter** icon to close the Refine by pane.

5. Click the check boxes adjacent to the names of the users you want to add to the role or click the check box adjacent to the **User Name** column name to select all the listed users on one page.

 **Note:** Only 20 users can be selected and added to a role at a time. Selecting more than 20 users will display a warning that user selection cannot exceed 20. Click the check box adjacent to the **User Name** column name to clear the check boxes and close the warning message.

The title bar of the dialog box shows the count of the number of users you select, for example **Selected 10**. The page numbers at the bottom of the list also display the number of users selected on each page, for example



- a. To see a list of all the selected users, click **Selected showing the number of selected users** such as **Selected 10** in the title bar of the User List dialog box.





A list of all the selected users is displayed.


- b. To unselect one or more users, point to the user name in the list and click **X** for each user.

The users are unselected and the number of selected users is updated.

- c. To unselect all the users, simply click **Clear all** in the list.

All the users are unselected and the Users List dialog box no longer displays a count of number of selected users.

On user selection, the title bar of the dialog box transforms and shows **Selected** and the Show icon . Clicking the Show icon expands the title bar area to also show the dialog box name, and the Back  and Filter icons . Clicking the Hide icon  hides the dialog box name, and the Back and Filter icons, and only shows Selected and the Show icon.


6. Click **Assign** to add the selected users to the role. Clicking **Cancel** or **Back icon**  in the title bar would close the dialog box without adding any users.


The User List dialog box closes and the selected users are added to the top part of the users' list in the Assign Users section.

7. Click **Save** to add the user to the role.

Role updated successfully message is shown and the Role dialog box closes.

### To add users to a role from manage Roles page

1. In the Manage Roles page, click the **Add users icon**  in the Action column for the role to which you want to add more users.

2. In the User List dialog box that opens, follow the instructions from [Step 4 to Step 5](#) in [“To add users to a role from the role details dialog box” on page 141](#) to add users to the role.
3. Click **Assign** to add the selected users to the role. Clicking **Cancel** or **Back** icon  in the title bar would close the dialog box without adding any users.  
The User List dialog box closes, and a message is shown that the selected number of users are added successfully.



#### 7.2.1.4 Remove users from a role

Administrators with proper permissions can remove a single or multiple users at the same time, up to a maximum of 20, from a role.

There are two ways to remove users from a role:

- Using the role details dialog box. See [“To remove users from a role using the role details dialog box” on page 143](#).
- From the Manage Roles page. See [“To remove users from a role from the manage roles page” on page 144](#)





##### To remove users from a role using the role details dialog box

1. Follow the steps in [“View role details” on page 140](#) to open the role dialog box to view the role details.
2. Click the arrow  in the **Assigned Users** section.  
The Assigned Users section is expanded.
3. If needed, find the user or users you want to remove using the **Filter** icon. See filter instructions in [Step 4](#) in [“To add users to a role from the role details dialog box” on page 141](#). The same filter criteria are also used to narrow the list of users in Assign Users section.
4. Based on if one or multiple users need to be removed, select one of the following steps:
  - To remove **one user** from a role, click the **Remove** icon  in the Action column for that user. Go to step [Step 5](#).
  - To remove **multiple users**:
    1. Select the check box for each of those users or to select all the users listed on a page, click the check box adjacent to the **User Name** column name.





**Note:** Only 20 users can be selected and removed from a role at a time. Selecting more than 20 users will display a warning that user selection cannot exceed 20. Click the check box adjacent to the **User Name** column name to clear the check boxes and close the warning message.

On user selection, the tool bar of the Assigned Users section transforms and shows the count of the number of selected users, for example


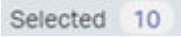
**Selected 10**, **Remove**, and the Show icon . Clicking the Show icon expands the tool bar area to also show the Filter  and Add Users  icons. Clicking the Hide icon  hides the Filter and Add Users icons, and only shows **Selected**, **Remove**, and the **Show** icon..

2. Click **Remove** in the title bar to remove all the selected users together.
5. Click **Remove** in the confirmation message.  
User removed successfully message is shown.
6. Close the role dialog box by clicking **X** or **Save**.





### To remove users from a role from the manage roles page


1. In the Manage Roles page, click the **Remove Users** icon  in the Action column for the role from which you want to remove users.  
The Remove Users dialog box opens and displays a list of users and their details such as user name, user ID, job title, email address, and their status that shows if they are active or inactive.
2. In the Remove Users dialog box, do the following to filter and select one or more users to remove from the role:
  - Click the Filter icon  to open the Refine By pane and refine the list of users using the following criteria or fields:
    - **First Name:** Enter the first name to find users with matching first name.
    - **Last Name:** Enter the last name to find users with matching last name if first name is not entered or matching combination of first and last name.
    - **User Id:** Type the user ID of the user you want to remove.
    - **Email:** Type the email ID of the user who you want to remove.
    - **Package Id:** Type the package ID associated with the user you want to remove.
    - **Claim Id:** Type the claim ID associated with the user you want to remove.
    - Click **Filter** to narrow down the list of users using the specified criteria. Click **Close** or the **Filter** icon to close the Refine by pane.
3. Click the check boxes adjacent to the names of the users you want to remove from the role or click the check box adjacent to the **User Name** column name to select all the listed users on **one** page.



 **Note:** Only 20 users can be selected and removed from a role at a time. The title bar of the dialog box shows the count of the number of users you select, for example .

Selecting more than 20 users will display a warning that user selection cannot exceed 20. Click the check box adjacent to the **User Name** column name to clear the check boxes and close the warning message.


On user selection, the title bar of the dialog box transforms and shows **Selected** and the Show icon . Clicking the Show icon expands the title bar area to also show the dialog box name, and the Back  and Filter  icons. Clicking the Hide icon  hides the dialog box name and the Back and Filter icons, and only shows Selected and the Show icon.

4. Click **Remove** to remove the selected users from the role. Clicking **Back**  in the title bar or **Cancel** would close the dialog box without removing any users from the role.
5. Click **Remove** in the confirmation message.  
Users removed successfully message is shown.  
The Remove Users dialog box closes.



## 7.3 Manage Applications

Only Administrators with Exchange operator, Security Administrator, or Service Administrator role are able to view the Administration > Manage Applications submodule.



Administrators can view and manage service packages and sub packages that they are authorized to manage for their organization using the Manage Applications page.

 **Note:** What you see in the user interface is determined by the role and permissions assigned to your profile. The user interface elements, such as fields, labels, and tooltips, that you see in IAM Administration for your organization might be different from the descriptions in the Help and the guide because this application can be configured to suit the needs of any organization.

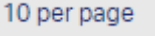
### To open the Manage Applications page

1. Click the main menu  to open the navigation pane.
2. Click the arrow  adjacent to the **Administration** module to expand the menu.
3. Click **Manage Applications**.

The Home > Administration: Manage Applications page opens.

The Manage Applications page contains a Filter icon , an Add Package icon , and a list of all of the service packages and subpackages the current administrator is authorized to view and manage and related details.

Use the Filter icon to open a Refine By pane, which provides options to refine the list of service packages using the provided criteria.

The lower part of the Manage Applications page displays the number of items shown on each page  which you can change. It also shows the number of pages and the total number of items.

#### To change the number of items listed per page setting


- Point the cursor to the number of items per page and from the popup menu, select the number you want to display.

#### To navigate the list of items on all the pages

1. Click **Next** to go to the next page.
2. Click **Previous** to go to the previous page.
3. Click a page number to directly navigate to that page.




### 7.3.1 Manage Applications page

The Manage Applications page contains a list of all of the service packages and subpackages the current administrator is authorized to view and manage, and displays the following details about the service packages:

- **Package Name:** Name of a service package. If the package has subpackages, an arrow  displays adjacent to the package name. Clicking the arrow expands the package list and displays the subpackages.
- **Description:** Description about the service package.
- **Category:** The category such as Administration, Applications, Roles, and so on the service package is associated with.
- **Auto Granted to SAO:** The column displays values **True** or **False**, which indicates if the service package is automatically granted to a SAO (Service Authority Organization) or not.
- **All Access Enabled:** The column displays values **True** or **False**, which indicates if the sub package has the ALLACCESS claim value enabled based on certain settings.

If enabled for a subpackage of a SAO service package, then the subpackage has ALLACCESS claim value for the claim code of the subpackage. The ALLACCESS claim value is a special type of claim value, which when granted to a user for a

specific subpackage, grants the user access to all claim values for the claim code of that subpackage. See [“Requesting ALLACCESS claim value for a claim code” on page 112.](#)


- **Creation Date:** The date when the package was created.
- **Action:** Displays the following icons for actions that are permitted for the service package:
  - **Add Package**  to add subpackages to the selected service package. Subpackages do not have the Add package icon in the Action column.
  - **View Details**  to see the details of the selected package. The details cannot be edited in this view.
  - **Remove Package**  to remove a service package. Clicking the Remove Package icon for a parent service package with subpackages will also remove the subpackages.

Clicking a group name would open the group details in another dialog box. See [“View and edit group details” on page 125.](#)

### 7.3.1.1 Filter service packages

As an administrator, you can filter or refine the list of service packages to find specific ones or find ones using certain search criteria.

#### To filter or refine the list of packages


1. In the Manage Applications page, click **Filter**  on the title bar.
2. In the Refine By pane, use one, some, or all options to use as criteria to refine the list and only display the matching packages:
  - **Parent Package Name:** Enter the name of the parent service package to find matching parent package or subpackages in that parent package.
  - **Category:** Click the arrow in the field and select one of the listed options to find all those packages that belong to the selected category.
  - **Parent Service Id:** Enter the ID of the parent service package to find matching parent package or subpackages in that parent package.
  - Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.

The matching records are listed in the Manage Applications page. The fields used for the search are shown as tokens above the column names on the page.








- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.

- Click **Close** to close the Refine by pane.

### 7.3.1.2 View service package details

Administrators can view the details of a service package and subpackages using the View Details icon  in the Action column in the Manage Applications page. The details in this view cannot be edited.

#### To view the details of a service package

1. In the Manage Applications page, after refining the listed records if needed, click the **View Details** icon  of the service package whose details you want to view.
  - To view the details of a subpackage, first expand the parent service package by clicking the arrow  adjacent to the package name and then from the expanded list of subpackages, click the **View Details** icon  in the Action column for the subpackage.
2. The details box opens and displays the following details:
  - **Parent Service:** It is the ID of the parent service package.
  - **Package Name:** Name of the package or subpackage.
  - **Category:** The name of the category the package belongs to.
  - **Owning Organization:** Name of the organization that is the owner of the service package.
  - **Approval Required:** Name of the role whose approval is needed to work with the service package.
  - **Description:** Description about the service package or subpackage.
  - **Terms and Conditions:** Indicates if the service package includes terms and conditions
  - **Included Services:** Lists the services that are included with the service package. The number of included services is shown in the title bar. Expand the list by clicking the arrow  to view the list of services. The list of services displays the service name, service ID, description, and category of the service. Collapse the list by clicking  in the Included Services title bar.
  - **Access Settings:** Lists the access settings for the package. The total number of settings is shown on the title bar. Expand the list by clicking the arrow  to view the list of access settings. The list of access settings displays the setting name and its on or off status. Collapse the list by clicking  in the Access Setting title bar.
    - **Protected:** Indicates if this package is synched back to the Cleartrust entitlements server, and therefore, protected by the CT web agent.



- **Requestable:** Indicates if this package can be requested by persons or organizations.
- **Grantable:** Indicates if this package can be granted to persons or organizations.
- **Displayable:** Indicates if this package can be displayed in UI.
- **Request Reason Required:** Indicates if package requests must require the requestor to provide a reason for requesting the package.
- **Fast Reg Enabled:** Indicates if this package is synched back to the Cleartrust entitlements server, and therefore, protected by the CT web agent.
- **Person Tac Enabled:** Indicates that the package’s terms and conditions pertinent to package request from a person is enabled.
- **Organization Tac Enabled:** Indicates that the package’s terms and conditions pertinent to package request from an organization is enabled.
- **Service Auto Grant Enabled:** Indicates if the package would be automatically granted to new users in an organization. This setting will also enable grant to existing users during a cascade, as configured by Cascade Enabled setting.
- **Cascade Enabled:** Indicates if a package granted to an Organization would also be automatically granted to all the divisions in that organization.

3. Click X to close the details box.


### 7.3.1.3 Add a new subpackage

Administrators can add new subpackages to existing service packages. Service packages with subpackages are referred to as parent service packages.

There are two ways to add subpackages:

- Using the Add Package icon  in the title bar of Manage Applications page. See [“To add a subpackage using the Add Package icon !\[\]\(01f19d40f03100aa8a158c4891453b0d\_img.jpg\) in the title bar of Manage Applications page” on page 149.](#)
- Using the Add Package icon  in the Action column for a service package listed in the Manage Application page. See [“To add users to a role from manage Roles page” on page 142](#)

**To add a subpackage using the Add Package icon  in the title bar of Manage Applications page**

1. In the Manage Applications page, click the Add Package icon  in the title bar.

2. In the Create Subpackage dialog box, do the following:

Required fields are marked with an asterisk.

- a. In the **Parent Package** field, click the arrow ▼ and from the list, select an existing service package to which you want to add a new subpackage.
  - b. In **Package Name**, type an appropriate name for the new subpackage.
    - Click **supported language(s)** link and in the Translation dialog box, provide localized package name in different languages. Click **Save** when you are done.
  - c. In the **Category** field, click the arrow ▼ and from the list, select an appropriate value from the list such as Administration, Applications, and Roles.
    - **Administration:** Use Administration if the new subpackage is associated with this category.
    - **Applications:** Use Applications if the new subpackage is associated with this category.
    - **Roles:** Use Roles if the new subpackage is associated with this category.
  - d. In **Description**, type a description about the new subpackage.
    - Click **supported language(s)** link and in the Translation dialog box, provide localized description in different languages. Click **Save** when you are done.
  - e. In the **Organization terms and conditions ID** field, click the arrow ▼ and from the list, select a value.


If a value is selected in this field, then in Access Settings, the Organization Tac Enabled setting is automatically set to true.
  - f. In the **Person terms and conditions ID** field, click the arrow ▼ and from the list, select a value.

If a value is selected in this field, then in Access Settings, the Person Tac Enabled setting is automatically set to true.
  - g. **Owning Organization Details** and **Required Approvals:** These two fields are pre-populated based on the selection in the Parent Package field.
  - h. In the **Access Settings** section, click the switch in the Status column for each setting to either on or off as needed. The description field explains what each setting does.
3. Click **Create**.

Package created successfully message displays.

The newly created subpackage is listed on the Manage Applications page under the parent service package. You can use the Refine by pane to search for it.

### To add a subpackage using the Add Package icon in the Action column for a service package

1. In the Manage Applications page, click the **Add Package** icon  in the Action column for a service package to which you want to add a subpackage.

The Create Subpackage dialog box opens. The **Parent Package** field already shows the service package name because you clicked the inline **Add package** icon for this service package.



2. In the Create Subpackage dialog box, provide the other details for the new subpackage using [Step 2 to Step 3 in “To add a subpackage using the Add Package icon !\[\]\(9dc885fa0d6d341860a6e69645e59475\_img.jpg\) in the title bar of Manage Applications page” on page 149.](#)

#### 7.3.1.4 Remove a service package or a subpackage

Administrators with right privileges can remove subpackages from a parent service package or can remove a service package.

##### To remove a subpackage from a parent service package

1. In the Manage Applications page, use the **Filter** option to find the parent service package from which you want to remove a subpackage. See [“Filter service packages” on page 147.](#)

2. Expand the parent service package by clicking the arrow  adjacent to the package name and then from the expanded list of subpackages, click the **Delete Package** icon  in the Action column for the subpackage you want to delete.

The Remove dialog box displays and informs you about the consequences of deleting a subpackage.


3. Click **Remove** to confirm the deletion. If you don't want to delete, click **Cancel**.

A message informs that the subpackage is submitted for deletion, and the deletion might take some time.

After the subpackage is deleted, it is no longer listed under the parent service package on the Manage Applications page.

##### To remove a service package

1. In the Manage Applications page, use the **Filter** option to find the service package you want to delete. See [“Filter service packages” on page 147.](#)

2. Click the **Delete Package** icon  in the Action column for the service package you want to delete.

The Remove dialog box displays and informs you about the consequences of deleting a package or subpackage.

3. Click **Remove** to confirm the deletion. If you don't want to delete, click **Cancel**.  
A message informs that the package is submitted for deletion, and the deletion might take some time.  
After the package is deleted, it is no longer listed on the Manage Applications page.


### 7.3.1.5 View and edit subpackage details

Administrators can open a subpackage to view its details and edit them if needed.



**Note:** All the information in this section also applies to a service package.


#### To view and edit the details of a subpackage

1. In the Manage Applications page, use the **Filter** option to find the parent service package whose subpackage you want to view and edit. See [“Filter service packages” on page 147](#).
2. Expand the parent service package by clicking the arrow  adjacent to the package name and then from the expanded list of subpackages, click the name of the subpackage you want to view and edit.


The subpackage opens in a new page. The breadcrumb trail, Home > Administration: Manage Applications, above the page shows where you are. The page displays the following details:

- the subpackage name and Package ID which cannot be edited.
- **Overview** and **Services** tabs
  - The **Overview** tab displays package details such as parent package name, package name, functional area, description and supported languages, owning organization details, required approvals, and access settings. You can edit any of these fields except Parent Package, Owing Organization Details, and Required Approvals. See [“View service package details” on page 148](#) and [“Add a new subpackage” on page 149](#) for additional information about the fields. Edit the fields as needed and click **Update**. The message data is updated successfully is shown.
  - The **Services** tab lists services associated with the subpackage in the Associated Services section.
    - To add more services to the subpackage, see [“To add services to a subpackage” on page 153](#).
    - To remove a service, see [“To remove an associated service from a subpackage” on page 153](#).
    - To view and edit an associated service, see [“To view and edit an associated service” on page 154](#).





- Click  on the title bar or **Cancel** to close this page and go back to the Manage Applications page.

### To add services to a subpackage

1. Click the **Add Services** icon  in the **Associated Services** title bar on the **Services** tab in an open subpackage.
2. In the Create Service dialog box, do the following:


Required fields are marked with an asterisk .

- a. In **Service Name**, enter a name for the new service you want to add to the subpackage.
  - Click the **supported language(s)** link and in the Translation dialog box, provide localized service name in different languages. Click **Save** when you are done.
- b. In the **Category** field, click the arrow  and from the list, select an appropriate category.
- c. The **Parent Service Id** displays the ID of the parent service package and cannot be edited.
- d. **Description**: Enter a description about the new service.
  - Click the **supported language(s)** link and in the Translation dialog box, provide localized description in different languages. Click **Save** when you are done.
- e. In **Service URL**, click the **Add Service URL** icon  to provide the following details:
  - i. In **Service URL Type**, click arrow and select an appropriate value from the list.
  - ii. In **Service URL Value**, enter the URL for the selected service type starting with http:// or https://.
  - iii. Click **Add**.  
The service URL and service type are added to the Service URL box.
- f. For **Messaging Enabled**, click the switch to turn it on or off.
- g. Click **Create**.


If you are authorized to create a service, the service is created and added to the Associate Services section. If you are not authorized to create a service, you will get the message that you are not authorized.

### To remove an associated service from a subpackage

1. Make sure you are in the **Associated Services** section on the **Services** tab in an open subpackage.

2. To remove a service, simply click the **Remove Service** icon  in the Action column for the service you want to delete.  
The Remove dialog box displays and informs you about the consequences of deleting a service.
3. Click **Remove** to confirm the deletion. If you don't want to delete, click **Cancel**.  
A message informs that the service is submitted for deletion, and the deletion might take some time.  
After the service is deleted, it is no longer listed in the Associated Services section.

#### To view and edit an associated service

1. Make sure you are in the **Associated Services** section on the **Services** tab in an open subpackage.
2. Click the name of the associated service you want to view and edit.  
The service opens in a new page. The breadcrumb trail, Home > Administration: Manage Applications, above the page show where you are. The page displays the following details:
  - the service name, Package ID, and Package Name, which cannot be edited.
  - The page also displays details such as service name, category, parent service ID, parent service type, description, service url and messaging enabled. You can edit any of these fields except Parent Service ID and Parent Service Type. See [“To add services to a subpackage” on page 153](#) for additional information about the fields. Edit the fields as needed and click **Update**. The message data is updated successfully is shown.
  - Click **Close** or  to go back to the **Services** tab of the open subpackage in which you are viewing and editing an associated service.

## 7.4 Audits




**Note:** What you see in the user interface is determined by the role and permissions assigned to your profile. The user interface elements, such as fields, labels, and tooltips, that you see in IAM Administration for your organization might be different from the descriptions in the Help and the guide because this application can be configured to suit the needs of any organization.

Administrators can use the Audit module to retrieve the user audit and user grant audit history for their organization including divisions.

There are two types of Audits:

- **User Audit:** Also called Quarterly User Audit. Supplier and OEM administrators perform this kind of audit to identify dormant or inactive users in an



organization. For this they would need to identify the last login dates of users of the organization. Once the users in the dormant or suspended state are identified, administrators decide either to suspend active users or permanently remove the already suspended users from the system.

 **Note:** An active user must be first suspended before being permanently removed.




- **User Grant Audit:** Also called Annual User Grant Audit. In this kind of audit, administrators are interested in identifying users based on their package grants. They first list the packages granted under their organization and check each package by accessing the details of each individual package and check the users granted to the specific package. After identifying the users for package grant, administrators will decide which users will continue to have access or to revoke access from users who no longer need access.

After the administrators perform the above audits, the audit details submitted are captured and shown as history in the respective sections.

### To open the Audits page

1. Click the main menu  to open the navigation pane.
2. Click the arrow  adjacent to the **Administration** module to expand the menu.
3. Click **Audits**.

The Home > Administration: Audit page opens.

The Audit page contains a Filter icon , a Run Audit icon , a drop-down field to select an audit type, a Download icon , and a list of all the audits, both user audit and user grant audit, conducted in the past.

Use the audit type drop-down field  to see past audits of a certain type, User or User Grant, or to see all the past audits listed on the page. The field shows the following options: **All**, **User Audit**, **User Grant Audit**.

Use the **Filter** icon to open a Refine by pane, which provides options to refine the list of past audits using the provided criteria.

The lower part of the Audits page displays the number of records shown on each page  which you can change. It also shows the number of pages and the total number of records or items.

### To change the number of items listed per page setting

- Point the cursor to the number of items per page and from the popup menu, select the number you want to display.




**To navigate the list of items on all the pages**

1. Click **Next** to go to the next page.
2. Click **Previous** to go to the previous page.
3. Click a page number to directly navigate to that page.

## 7.4.1 View audit history by different audit types

Administrators can use the audit type field on the title bar to see audit history or past audits for specific audit type. By default past audits of all audit types, user audit and user grant audit, are shown on the page.


**To view past audits of different types and to switch between the audit types**



1. In the Audits page, click the arrow  in the audit type field  to see the list of available audit types.
2. In the list, click **User Audit**.  
The page displays past audits of only user audit type. The following columns are shown: Last User Audit, Admin Name, Admin Username, Organization ID, and Audit Type.
3. To switch to another audit type, click the arrow  in the audit type field again and click **User Grant Audit** in the list.  
The page refreshes and displays past audits of only the user grant audit type.
4. To see all the past audits listed on the Audits page, from the audit type list, select **All**.
5. To filter the list of past audits using the Filter icon, see [“Filter audit history list” on page 156](#).
6. To download the list of past audits, click the **Download** icon  on the title bar.  
The contents of the page are downloaded as a .pdf file and saved in the Downloads folder.

### 7.4.1.1 Filter audit history list


As an administrator, you can filter or refine the list of audit history of past audits to find specific ones or find ones using certain search criteria.

**To filter or refine the list of past audits**

1. In the Audits page, click **Filter**  on the title bar.
2. In the Refine By pane, use one, some, or all options to use as criteria to refine the list and only display the matching past audits:

- **Start Date:** Use the Start Date and End Date fields to search for past audits that were conducted during a specific time frame. Click the calendar icon  and select a date as a start date for the search.
- **End Date:** Click the calendar icon  and select a date as the end date for the search time frame. If no date is selected, the current date is used as the end date.
- **Admin First Name:** Enter the first name of the administrator who conducted the audit.
- **Admin Last Name:** Enter the last name of the administrator who conducted the audit to find users with matching last name if first name is not entered or matching combination of first and last name.
- **Admin Username:** Enter the username of the administrator who conducted the audit.
- Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine By pane.  
The matching records are listed in the Audits page. The fields used for the search are shown as tokens above the column names on the page.
- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** to close the Refine by pane.


## 7.4.2 Perform user audit

 **Note:** What you see in the user interface is determined by the role and permissions assigned to your profile. The user interface elements, such as fields, labels, and tooltips, that you see in IAM Administration for your organization might be different from the descriptions in the Help and the guide because this application can be configured to suit the needs of any organization.

Administrators can perform a user audit to validate that all the listed users are members of the organization. They can review the current status of all the active and suspended users and make changes if needed. Administrators can retrieve all user information for their organization and divisions using the Audits module.

An active user must be first suspended before being permanently removed.

### To run a user audit

1. In the Audits page, click the Run Audit icon  in the title bar and then click **User Audit** in the list.

The User Audit page opens and the User List section lists all active and suspended users of the current organization. Administrators can review the


current status of all the active and suspended users in the current organization and validate if they are members of the organization.

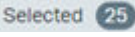
The User List section shows all the active users by default. The User List shows the following information: name of the user, ID of the organization user is member of, user's ID, user's email address, user's status active or suspended, user's last login date, and action that the administrator can apply to the user such as suspend.



2. In the User Audit page, administrators can perform the following as part of the user audit:
  - View the list of active users: The User List section shows all the active users by default.
  - Suspend active users
  - View the list of suspended users
  - Delete suspended users
  - Filter the list of users
3. To filter the list of active or suspended users, click the **Filter** icon in the User List title bar.

The Refine by pane opens. You can use the following search criteria to filter the list of users:

- **Include all divisions** check box: Select the check box to audit an entire organization hierarchy, which means also audit all the divisions within an organization's hierarchy.
  - **Name**: Enter a few characters from the user name or full name to find users with matching name.
  - Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine by pane.

The matching records are listed in the User List section. The fields used for the search are shown as tokens above the column names on the page.
  - Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
  - Click **Close** to close the Refine by pane.
4. To suspend an active user, do the following:
    - a. Click the **Suspend** icon  in the Action column for the user you want to suspend. To suspend all active users listed on the current page of the User List section, click the check box adjacent to the Name column name.


On check box selection, the title bar of the User List section transforms and shows the **Selected** number of users , the **Suspend** button



**Suspend**, and the Show icon . Clicking the Show icon expands the title bar area to also show the name User List, the Filter icon, and the control to select user type . Clicking the Hide icon  hides everything except Selected and the Show icon.


- b. Click **Suspend** in the title bar.
- c. In the Suspend Users confirmation dialog box, provide an appropriate reason in the Reason box and click **Confirm**.



A message indicates that the user status is updated successfully. The suspended user no longer displays in the list of active users. You can check that user listed in the suspended users list.

5. To permanently delete the suspended user, do the following:

- a. In the User Audit page, click the arrow  in the user type field  again and from the list of available options, click **Suspended users**.

The User list section updates and shows all the suspended users. Notice that the Status column shows the suspended icon  and the Action column shows the Delete icon  for all users in this view. All the other columns are same as the Active Users view.

- b. Click the **Delete** icon  in the Action column for the suspended user you want to permanently remove.
  - i. If needed, to remove all suspended users listed on the current page of the User List section, click the check box adjacent to the Name column name.

On check box selection, the title bar of the User List section transforms and shows the **Selected** number of users , the **Delete** button **Delete**, and the Show icon . Clicking the Show icon expands the title bar area to also show the name User List, the Filter icon, and the control to select user type . Clicking the Hide icon  hides everything except Selected, Delete, and the Show icon.

- ii. Click **Delete** in the title bar.
- c. In the Delete Users confirmation dialog box, provide an appropriate reason in the Reason box and click **Confirm**.

A message indicates that the user status is updated successfully. The user who was deleted no longer displays in the list of suspended users.

6. Click **Next**.

The page displays a message that as the administrator of the current organization, you acknowledge your responsibility for user access in your

organization. Review the message and proceed to the next step when you are ready.

7. Click **Submit**.

The Confirm and log user audit page opens. It shows the message that you have reviewed the list of registered users in your organization and by clicking Confirm in the message you are indicating that to the best of your knowledge, all the users are representatives of your company who have business needs to access your organization, and that you have the authority to designate the appropriate individuals for your company.

8. Review the message and click the **Include all divisions** check box to log user audit for users across all divisions of the organization. Then click **Confirm**.

User audit logged successfully message displays. The User Audit page closes.

The user audit you just performed is listed as audit history in the Audits page.


You have successfully performed user audit.

### 7.4.3 Perform user grant audit

Administrators who are interested in identifying users based on their package grants can perform user grant audit. They first list the packages granted under their organization and check each package by accessing the details of each individual package and check the users granted to the specific package. After identifying the users for package grant, administrators will decide to revoke the access to any of these users by identifying the last granted data and last updated date.

#### To run a user grant audit

1. Open the Audits page. See [“To open the Audits page” on page 155](#).


2. In the Audits page, click the Run Audit icon  and then click **User Grant Audit** in the list.

The User Grant Audit page opens and the Service Packages section lists all the service packages and subpackages granted to the current organization. The page shows different steps in the audit process from Application package to Users to Confirmation in a progress bar. As you navigate from page to page, this section shows your progress in the process.




The Service Packages section shows the following information: package name, package category, and last confirmed date and time, which is the last time the package or subpackage was confirmed.

3. To filter the list of service packages, click the **Filter** icon in the Service Packages title bar.

The Refine by pane opens. You can use the following search criteria to filter the list of service packages:


- a. **Category:** Click the arrow  in the Category field and select one of the listed options such as Administration, Applications, Roles and so on.






- b. Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine by pane.  
The matching records are listed in the Service Packages section. The field used for the search is shown as a token above the column names on the page.
    - c. Click the **X** in the token to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
    - d. Click **Close** to close the Refine by pane.
  4. Click the service package or subpackage you want to audit in the Service Packages section. If a service package includes subpackages, it displays this arrow . Click the arrow to expand the service package and see the subpackages.  
Just click the service package or subpackage again to deselect it.
  5. Click **Next**.  
The audit process moves to the Users stage as shown in the progress bar. The page displays the name of the selected package.  
The Users List page opens. It displays all the users who are granted the service package or subpackage you had selected. The Users List section shows the following information: user name, ID of the organization user is member of, user's ID, user's email address, Grant Details icon  to view details of the package grant to a user, and the Remove icon to revoke package grant from the user.
  6. To filter the list of users, click the **Filter** icon in the Users List title bar.  
The Refine by pane opens. You can use the following search criteria to filter the list of active users:
    - **Include all divisions** check box: Select the check box to audit an entire organization hierarchy, which means also audit all the divisions within an organization's hierarchy.
    - **Name**: Enter a few characters from the user name or full name to find users with matching name.
    - Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine by pane.  
The matching records are listed in the User lists section. The fields used for the search are shown as tokens above the column names on the page.
    - Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
    - Click **Close** to close the Refine by pane.
  7. To see the details of the package grant to a user, click the **Grant Details** icon  in the Grant Details column for that user.

The Grant Details box opens and displays the following information about the granted service package: status of the package grant, active or not, date when the user was granted access to the service package, organization name, service package name, services included in the service package, and roles required to approve the package grant.

Click **X** to close the Grant Details box.

8. To revoke package grant from the user, click the Remove icon  in the Remove column for that user.
  - a. If needed, to revoke package grant from all users in the page, select the check box adjacent to the Name column.

On check box selection, the title bar of the User List section transforms and shows the **Selected** number of users **Selected 25**, the **Remove** button , and the Show icon . Clicking the Show icon expands the title bar area to also show the name User List and the Filter icon. Clicking the Hide icon  hides everything except Selected, Remove, and the Show icon.
  - b. Click **Remove** in the title bar.
9. In the Revoke Package Grant confirmation dialog box, provide an appropriate reason in the Reason box and click **Confirm**.

A message indicates that the package grant was revoked successfully from the user. The user whose access was revoked no longer displays in the Users List section.
10. Click **Next**.

The audit process moves to the Confirmation stage as shown in the progress bar.

The page displays a message that as the administrator of the current organization, you acknowledge your responsibility for user access in your organization. Review the message which indicates that you have reviewed all the users in your organization and believe that these users are appropriate members of your organization. After you have reviewed the message, proceed to the next step.
11. Click **Submit**.

The Confirm and Log user grant audit dialog box opens. It shows the message that you have reviewed the list of registered users in your organization and by clicking Confirm in the message you are indicating that to the best of your knowledge, all the users are representatives of your company who have business needs to access your organization, and that you have the authority to designate the appropriate individuals for your company.
12. Review the message, and click the **Include all division** check box, if needed, to confirm and log user grant audit across all divisions of the organization. Then click **Confirm**.

User grant audit logged successfully message displays. The User Grant Audit page closes.

The user grant audit you just performed is listed as audit history in the Audits page.


You have successfully performed user grant audit.




## Chapter 8

# My Tasks Module – Manage Organization and User Requests




Administrators can manage user requests and requests from organizations for registration, service packages, and claims in the IAM Administration application using the My Tasks page.

 **Note:** What you see in the user interface is determined by the role and permissions assigned to your profile. The user interface elements, such as fields, labels, and tooltips, that you see in IAM Administration for your organization might be different from the descriptions in the Help and the guide because this application can be configured to suit the needs of any organization.

### To open the My Tasks page

1. Click the main menu  to open the navigation pane.
2. Click **My Tasks**.

The Home > My Tasks page opens.

The My Tasks page contains a Filter icon , four tabs, and a switch to change from Organization requests  to user requests  and vice-versa. When the switch is set to Organization requests, the page displays the following tabs and the number of pending requests on each tab:

- New Organization Requests: Lists all the new organization registration requests.
- Service Package Requests: Lists all the service package requests from other organizations.
- Claim Code Requests: Lists all the claim code requests from other organizations.
- Claim Value Requests: Lists all the claim value requests from other organizations.

When the switch is set to User requests, the page displays the following tabs and the number of pending requests on each tab:

- New User Requests: Lists all the new user registration requests.
- Service Package Requests: Lists all the service package requests from other users.
- Claim Code Requests: Lists all the claim code requests from other users.
- Claim Value Requests: Lists all the claim value requests from other users.

Use the Filter icon to open a Refine by pane, which provides options to refine the list of requests on each tab page using the provided criteria.

The lower part of the My Tasks page displays the number of records shown on each page **10 per page** which you can change. It also shows the number of pages and the total number of records or items.

### To change the number of items listed per page setting

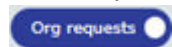
- Point the cursor to the number of items per page and from the popup menu, select the number you want to display.

### To navigate the list of items on all the pages

1. Click **Next** to go to the next page.
2. Click **Previous** to go to the previous page.
3. Click a page number to directly navigate to that page.

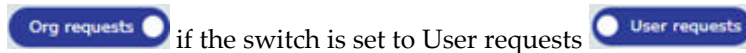
## 8.1 Manage Organization Requests

Administrators can manage different types of requests from different organizations on the My Tasks page. Make sure the switch is set to Organization requests



### To change the switch to Organization requests

- In the **My Tasks** page, click the switch to change to Organization requests



The New Organization Requests tab is selected by default and lists all the organization requests.

### 8.1.1 New organization requests

The New Organization Requests tab lists all the new organization registrations requests and displays the following details about the requests:

- **Requested Organization:** Name of the organization that made the request.
- **Request ID:** ID of the request for the new organization registration. You can click the column name to sort the items on the page in ascending or descending order.
- **Reason:** The reason provided during the request for the new organization registration.
- **Requested Administrator:** ID of the administrator who made the request and is registered along with the organization.




- **Requested Date:** Date and time of the request for the new organization registration. You can click the column name to sort the items on the page in ascending or descending order.

Clicking a request item would open the request details in another dialog box. See [“View, approve, or reject new organization requests” on page 168.](#)

### 8.1.1.1 Filter new organization requests

As an administrator, you can filter or refine the list of new organizations requests to find specific ones or find ones using certain search criteria.

#### To filter or refine the list of new organization requests

1. Make sure the New Organization Requests tab is selected and click **Filter**  on the page.
2. In the Refine by pane, use one, some, or all of the following options to use as criteria to refine the list and only display the matching requests:
  - **Registrant ID:** Enter the ID of the user that is created when a new organization is registered. When a new organization is registered, first a user is created. Registrant ID is the ID of this user. This user is granted the security administrator role for the organization being registered.
  - **Organization ID:** Enter the ID of the organization that made the new organization registration request. This ID is created for the organization during registration.
  - **Organization Name:** Type the name of the organization that made the request to find the organization’s request.
  - **Start Date:** Use the Start Date and End Date fields to search for requests made during a specific time frame. Click the calendar icon  and select a date as a start date for the search.
  - **End Date:** Click the calendar icon  and select a date as the end date for the search time frame. If no date is selected, the current date is used as the end date.
  - Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.  
The matching records are listed in the New Organization requests page. The fields used for the search are shown as tokens above the column names on the page.
  - Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
  - Click **Close** to close the Refine by pane.


### 8.1.1.2 View, approve, or reject new organization requests

Administrators can view the details of the requests they receive from organizations in the Request: New Organization dialog box and then choose to either approve or reject those requests.

#### To view the details of a new organization request

- In the New Organization Requests page, after refining the listed records if needed, click the request whose details you want to view.

The Request: New Organization dialog box displays the following details:

- **Requesting organization details:** details such as name and address of the requesting organization.
- **Requesting administrator details:** details such as name, user ID, address, email address, phone number of the requesting administrator.
- **Organization details:** This section shows the details of the request such as requestor organization name, reason for the request provided by the requestor, actions Approve and Reject options, and a text box to provide the reason for approving or rejecting the request.
- **Included requests:** Displays other requests such as claims, claim code, a reason for the request, and action options Approve and Reject. If there are multiple requests and all need to be either approved or rejected, then click the arrow icon  adjacent to the Action column name and from the list, select either Approve All or Reject All as needed.

Enter a reason for approving or rejecting each included request in the Reason text box.

#### To approve a new organization request

1. In the New Organization requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: New Organization dialog box, click the **Approve** option in the Organization details section to approve the request.
3. In the **Reason** box, type a reason for approving the request.
4. In the Included requests section, if there are other requests such as a claim, click the **Approve** or the **Reject** button to approve or reject the request, respectively. In the **Reason** box, type a reason for approving or rejecting other requests.

If the organization requested a customer-owned service package, the request must be reviewed by a Service Owner Administrator.

5. Click **Submit**.

A message displays that you successfully submitted your decision.

The approved New organization request is no longer listed in the New Organization requests list.



**To reject a new organization request**

1. In the New Organization requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: New Organization dialog box, click the **Reject** option in the Organization details section to reject the request.



**Note:** If you click Reject for the organization request, all the included requests also get rejected and are removed from the request queue.

In the Included requests section, the area with the requests becomes unavailable and cannot be edited.

3. In the **Reason** box, type a reason why you rejected the request.
4. Click **Submit**.

A message displays that you successfully submitted your decision.

## 8.1.2 Service package requests

Security administrators, Exchange operators, and Service administrators need to view all of the service package requests for their organization or across a realm, respectively, so that they can see the details of the requests and take appropriate action to meet the requests.

The Service Package Request tab lists all the service package requests and displays the related details in the following columns:


- **Requested By:** Name of the organization that made the request for the service package.
- **Request ID:** ID of the service package request from the organization.
- **Service Package ID:** ID of the service package that is requested.
- **Service Package Name:** Name of the service package that is requested.
- **Reason:** The reason provided during the request for the service package.
- **Creator ID:** ID of the user (administrator) who made the request.
- **Requested Date:** Date and time of the request for the service package.

Clicking a request item would open the request details in another dialog box. See [“View , approve, or reject service package requests” on page 170](#).

### 8.1.2.1 Filter service package requests

As an administrator, you can filter or refine the list service package requests by organization to find specific ones or find ones using certain search criteria.

#### To filter or refine the list of service package requests

1. Make sure the Service Package Request tab is selected and click **Filter**  on the page.
2. In the Refine by pane, use one or both options to use as criteria to refine the list and only display the matching requests:
  - **Package ID:** Enter the ID of the requested service package.
  - **Requestor ID:** Enter the ID of the **organization** that made the service package request.
  - Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.

The matching records are listed in the Service package requests page. The fields used for the search are shown as tokens above the column names on the page. Nothing is shown if no matching requests are found.

- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** to close the Refine by pane.

### 8.1.2.2 View , approve, or reject service package requests

Administrators can view the details of the requests they receive from organizations in the Request: Service package dialog box and then choose to either approve or reject those requests.

#### To view the details of a service package request

1. In the Service package requests page, after refining the listed records if needed, click the request whose details you want to view.
2. The Request: Service package dialog box displays the following details:
  - **Requester details:** This section shows the details such as name of the user making the request, user ID, requester's organization name, requester email, requester phone number.
  - **Service package details:** This section shows the details of the request such as service package name, reason for the request provided by the requester, actions Approve and Reject buttons, and a text box to provide the reason for approving or rejecting the request.
  - **Included requests:** Displays other requests that could be a part of the service package requests such as claims. The section shows claim value ID, name of

the claim code, a reason for the request, action buttons Approve and Reject, and a text to provide the reason for rejecting the claim request.

### To approve a service package request

1. In the Service package requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: Service package dialog box, click the **Approve** button in the Service package details section to approve the request.
3. In the **Reason** box, type a reason for approving the request.
4. In the Included requests section, if there are other requests such as a claim, click the **Approve** or the **Reject** button to approve or reject the request, respectively. In the **Reason** box, type a reason for rejecting other requests.



**Note:** If the claim is rejected for some reason, on submitting the changes, the application displays a message that the service package must be associated with at least one claim value.

5. Click **Submit**.

If everything is approved, then a message displays that you successfully submitted your decision.

The approved service package request is no longer listed in the Service package requests list.

### To reject a service package request

1. In the Service package requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: Service package dialog box, click the **Reject** button in the Service package details section to reject the request.

A warning displays the message that all the included requests would also get rejected and would be removed from the request queue.

In the Included requests section, the area with the requests becomes unavailable and cannot be edited.

3. In the **Reason** box, type a reason why you rejected the request.
4. Click **Submit**.

A message displays that you successfully submitted your decision.

### 8.1.3 Claim code requests

Security administrators and Exchange operators need to view all of the claim code requests for their organization or across a realm, respectively, so that they can see the details of the requests and take appropriate action to meet the requests.

The Claim Code Requests tab lists the claim code requests for a SAO (Service Authority Organization) package and displays the related details in the following columns:



- **Requested By:** ID of the organization that made the request for the claim code.
- **Request ID:** ID of the claim code request from the organization.
- **Claim Code:** Name of the requested claim code.
- **Claim Value:** ID of the requested claim value.
- **Service Package ID:** ID of the service package related to the requested claim code.
- **Service Package Name:** Name of the service package related to the requested claim code.
- **Justification:** The reason provided during the request for the claim code.
- **Requested Date:** Date and time of the request for the claim code.


Clicking a request item would open the request details in another dialog box. See [“View, approve, or reject claim code requests” on page 173](#).

#### 8.1.3.1 Filter claim code requests

As an administrator, you can filter or refine the list of claim code requests by organization to find specific ones or find ones using certain search criteria.

##### To filter or refine the list of claim code requests

1. Make sure the Claim Code Requests tab is selected and click **Filter**  on the page.
2. In the Refine by pane, use one, some, or all the options to use as criteria to refine the list and only display the matching requests:
  - **Claim ID:** Enter the requested claim code.
  - **Package ID:** Enter the ID of the service package that includes the requested claim code.
  - **Claim Value ID:** Enter the ID of the requested claim value.
  - **Start Date:** Use the Start Date and End Date fields to search for requests made during a specific time frame. Click the calendar icon  and select a date as a start date for the search.

- **End Date:** Click the calendar icon  and select a date as the end date for the search time frame. If no date is selected, the current date is used as the end date.

- Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine by pane.


The matching records are listed in the Claim Code Requests page. The fields used for the search are shown as tokens above the column names on the page. Nothing is shown if no matching requests are found.

- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** to close the Refine by pane.

### 8.1.3.2 View, approve, or reject claim code requests

Administrators can view the details of the claim code requests they receive from organizations in the Request: Claim dialog box and then choose to either approve or reject those requests.

#### To view the details of a claim code request

1. In the Claim Code Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. The Request: Claim dialog box displays the following details:
  - **Requester Details:** This section shows the details such as name of the user making the request, user ID, requester email and phone number, requester's organization ID and name.
  - **Claim Details:** This section shows the details of the claim code request such as claim code, request creation date, service package ID, service package claim ID, service package claim type, and the phase in which the claim request is in such as pending security administrator approval. The section also shows Approve and Reject options, and a text box to provide the reason for approving or rejecting the request.
  - **Included requests:** Displays the claim name which lists the requested claim value ID, a reason for the request, and action options Approve and Reject. If there are multiple requests and all need to be either approved or rejected, then click the arrow icon  adjacent to the Action column name and from the list, select either Approve All or Reject All as needed.  
Enter a reason for approving or rejecting each included request in the Reason text box in Claim Details.

#### To approve a claim code request

1. In the Claim Code Requests page, after refining the listed records if needed, click the request whose details you want to view.

2. In the Request: Claim dialog box, click the **Approve** option in the Claim Details section to approve the request.
3. In the **Reason** box, type a reason for approving the request.
4. In the Included Requests section, if there are other requests such as a claim value ID request, then click the **Approve** or the **Reject** option to approve or reject the request, respectively. In the **Reason** box, type a reason for approving or rejecting the claim value ID requests.
5. Click **Submit**.

A message displays that you successfully submitted your decision.

The approved claim code request item is no longer listed in the Claim Code Requests page.

#### To reject a claim code request

1. In the Claim Code Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: Claim dialog box, click the **Reject** option in the Claim Details section to reject the request.

A warning displays the message that all the included requests would also get rejected and would be removed from the request queue.

In the Included requests section, the area with the requests becomes unavailable and cannot be edited.
3. In the **Reason** box, type a reason why you rejected the request. If a reason is not provided, then on submission, a message displays that a reason is mandatory when you reject a claim code request.
4. Click **Submit**.

A message displays that you successfully submitted your decision.

The rejected claim code request is no longer listed in the Claim Code Requests page.

### 8.1.4 Claim value requests

Organization can request additional claim value ID for claim codes that have already been approved.

Security administrators and Exchange operators need to view all of the claim value requests for their organization or across a realm, respectively, so that they can see the details of the requests and take appropriate action to meet the requests.

The Claim Value Requests tab lists the requests for additional claim value IDs for already approved claim codes for a SAO (Service Authority Organization) package. The tab displays the related details in the following columns:




- **Requested By:** ID of the organization that made the request for additional claim value ID.
- **Request ID:** ID of the claim value request from the organization.
- **Claim Code:** Name of the approved claim code for which additional claim value ID is being requested.
- **Claim Value:** Requested claim value ID.
- **Service Package ID:** ID of the service package related to the requested claim value ID.
- **Service Package Name:** Name of the service package related to the requested claim value ID.
- **Justification:** The reason provided during the request for the claim value ID.
- **Requested Date:** Date and time of the request for the claim value ID.

Clicking a request item would open the request details in another dialog box. See [“View, approve, or reject claim value requests” on page 176.](#)

#### 8.1.4.1 Filter claim value requests

As an administrator, you can filter or refine the list of claim value requests by organization to find specific ones or find ones using certain search criteria.

##### To filter or refine the list of claim value requests

1. Make sure the Claim Value Requests tab is selected and click **Filter**  on the page.
2. In the Refine by pane, use one, some, or all the options to use as criteria to refine the list and only display the matching requests:
  - **Claim ID:** Enter the approved claim code for which claim value ID is being requested.
  - **Package ID:** Enter the ID of the service package that includes the requested claim value.
  - **Claim Value ID:** Enter the requested claim value ID.
  - **Start Date:** Use the Start Date and End Date fields to search for requests made during a specific time frame. Click the calendar icon  and select a date as a start date for the search.
  - **End Date:** Click the calendar icon  and select a date as the end date for the search time frame. If no date is selected, the current date is used as the end date.
  - Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.

The matching records are listed in the Claim Value Requests page. The fields used for the search are shown as tokens above the column names on the page. Nothing is shown if no matching requests are found.


- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** to close the Refine by pane.

#### 8.1.4.2 View, approve, or reject claim value requests

Organization can request additional claim value ID for claim codes that have already been approved.

Administrators can view the details of such claim value requests they receive from organizations in the Request: Claim dialog box and then choose to either approve or reject those requests.

##### To view the details of a claim code request

1. In the Claim Value Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. The Request: Claim dialog box displays the following details:
  - **Requester Details:** This section shows the details such as name of the user making the request, user ID, requester email and phone number, requester's organization ID and name.
  - **Claim Details:** This section shows the details of the claim code request such as claim code, request creation date, service package ID, service package claim ID, service package claim type, and the phase in which the claim request is in such as pending security administrator approval. The section also shows the status of the claim code as Approved.
  - **Included requests:** Displays the claim name which shows the claim value ID being requested for the approved claim code, a reason for the request, and action buttons Approve and Reject. If there are multiple requests and all need to be either approved or rejected, then click the arrow icon  adjacent to the Action column name and from the list, select either Approve All or Reject All as needed.

Enter a reason for approving or rejecting each included request in the Reason text box in Claim Details.

##### To approve a claim value request

1. In the Claim Value Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: Claim dialog box, to approve the requested claim value ID, **Approve** needs to be selected in the Included Requests section. Approve is the default selection.



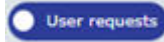
3. In the **Reason** box, type a reason for approving the request.
4. Click **Submit**.  
A message displays that you successfully submitted your decision.  
The approved claim value request item is no longer listed in the Claim Value Requests page.

#### To reject a claim value request


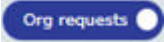
1. In the Claim Value Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: Claim dialog box, to reject the request, click the **Reject** option in the Included Requests section for the listed claim Value ID.
3. In the **Reason** box, enter a reason why you rejected the request. If a reason is not provided, then on submission, a message displays that a reason is mandatory when you reject a claim value request.
4. Click **Submit**.  
A message displays that you successfully submitted your decision.  
The rejected claim value request is no longer listed in the Claim Value Requests page.

## 8.2 Manage user requests

Administrators can manage all of the user requests, associated to the organization requests, such as requests for registration, service packages, and claims on the My Tasks page in IAM Administration. Make sure the switch is set to User requests

 in the My Tasks page.

#### To change the switch to User requests

- In the **My Tasks** page, click the switch to change to User requests  if the switch is set to Organization requests .

When the switch is set to User requests, the page displays the following tabs and each tab displays the number of pending requests:

- New User Requests
- Service Package Requests
- Claim Code Requests
- Claim Value Requests

## 8.2.1 New user requests

The New User Requests tab lists all the new user registration requests and displays the following details about the requests:




- **Name:** The name of the user that is making the registration request. When a new organization is registered, the first user to register the organization is granted the security administrator role for this organization.
- **Requested ID:** Internal unique identifier for the request.
- **Registrant ID:** The ID of the user that is making the registration request. When a new organization is registered, the first user to register the organization is granted the security administrator role for this organization.
- **Reason for request:** The reason provided during the request for the new user registration.
- **Request Date:** Date and time of the request for the new user registration. You can click the column name to sort the items on the page in ascending or descending order.

Clicking a request item would open the request details in another dialog box. See [“View, approve, or reject new user requests” on page 179](#).

### 8.2.1.1 Filter new user requests

As an administrator, you can filter or refine the list of new user requests to find specific ones or find ones using certain search criteria.

#### To filter or refine the list of new user requests

1. Make sure the New User Requests tab is selected and click **Filter**  on the page.
2. In the Refine by pane, use one, some, or all of the following options to use as criteria to refine the list and only display the matching requests:
  - **Registrant ID:** The ID of the user that is making the registration request.
  - **Start Date:** Use the Start Date and End Date fields to search for requests made during a specific time frame. Click the calendar icon  and select a date as a start date for the search.
  - **End Date:** Click the calendar icon  and select a date as the end date for the search time frame. If a date is not selected, the current date is used as the end date.
  - Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine by pane.

The matching records are listed in the New User Requests page. The fields used for the search are shown as tokens above the column names on the page.

- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page again.
- Click **Close** or the **Filter** icon to close the Refine by pane.

### 8.2.1.2 View, approve, or reject new user requests

Administrators can view the details of the user requests in the Request: New user dialog box and then choose to either approve or reject those requests.

In some cases, user requests cannot be approved and are rejected. Following are some of the reasons for rejecting user requests:

- The user has requested a site code or claim code that is not available to the organization anymore.
- The requested service package is removed from the portal and is not available anymore.

#### To view the details of a new user request

1. In the New User Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. The Request: New user dialog box displays the following details:



**Note:** Fields marked with an asterisk are mandatory.

- **Person details:** This section shows details of the user such as name, user ID, phone and email address, status of the request, and creation date and time of the request.
- **Request details:** This section shows the details of the request such as requester name (same as name in the Person details section), reason for the request provided by the requester, action options Approve and Reject, and a text box to provide the reason for approving or rejecting the request.
- **Included requests:** Displays other requests such as service packages, claims, claim code, a reason for the request, and action options Approve and Reject.

#### To approve a new user request

1. In the New user requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: New user dialog box, to approve the request, the **Approve** option in the Request details section needs to be selected. Approve is the default selection.


3. In the **Reason** box, type a reason for approving the request.
4. In the Included Requests section, if there are other requests such as for a service package or a claim, click **Approve** or **Reject** to approve or reject the request, respectively. In the **Reason** box, type a reason for approving or rejecting other requests.
5. Click **Submit**.  
A message displays that you successfully submitted your decision.  
The approved New user request is no longer listed in the New User Requests page.

#### To reject a new user request

1. In the New User Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: New user dialog box, click the **Reject** option in the Request details section to reject the request.  
A warning displays the message that all the included requests would also get rejected and would be removed from the request queue.  
In the Included requests section, the area with the requests becomes unavailable and cannot be edited.
3. In the **Reason** box, type a reason why you rejected the request.
4. Click **Submit**.  
A message displays that you successfully submitted your decision.

## 8.2.2 Service package requests by users

Security administrators, Exchange operators, and Service administrators need to view all of the service package requests from users of their organization so that they can see the details of the requests and take appropriate action to meet the requests.

 **Note:** Users can request a subpackage before their request for the parent service package is approved, but an error message would be shown that the parent package approval is not completed when the administrator tries to approve the subpackage request before approving the parent service package request.

The Service package request tab lists all the service package requests and displays the related details in the following columns:

- **Requested By:** ID of the user who made the request for a service package.
- **Request ID:** ID of the service package request from a user.
- **Service Package ID:** ID of the requested service package.




- **Service Package Name:** Name of the requested service package.
- **Justification:** The reason provided during the request for the service package.
- **Requested Date:** Date and time of the request for the service package.

Clicking a request item would open the request details in another dialog box. See [“View, approve, or reject service package requests from users” on page 182.](#)

### 8.2.2.1 Filter service package requests by users

As an administrator, you can filter or refine the list of service package requests by users to find specific ones or find ones using certain search criteria.

#### To filter or refine the list of service package requests

1. Make sure the Service Package Requests tab is selected and click **Filter**  on the page.
2. In the Refine By pane, use one or all options to use as criteria to refine the list and only display the matching requests:
  - **Package ID:** Enter the ID of the requested service package.
  - **Requestor ID:** ID of the user who made the request for the service package.
  - **Start Date:** Use the Start Date and End Date fields to search for requests made during a specific time frame. Click the calendar icon  and select a date as a start date for the search.
  - **End Date:** Click the calendar icon  and select a date as the end date for the search time frame. If a date is not selected, the current date is used as the end date.
  - Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.  
The matching records are listed in the Service package requests page. The fields used for the search are shown as tokens above the column names on the page. Nothing is shown if no matching requests are found.
  - Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
  - Click **Close** to close the Refine by pane.

### 8.2.2.2 View, approve, or reject service package requests from users

Administrators can view the details of the requests they receive from users in the Request: Service package dialog box and then choose to either approve or reject those requests.

#### To view the details of a service package request by users

1. In the Service Package Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. The Request: Service package dialog box displays the following details:
  - **Requester Details:** This section shows the details such as name of the user making the request, user ID, requester's organization name, requester address and email, and requester phone number.
  - **Service Package Details:** This section shows the details of the request such as service package name, reason for the request provided by the requester, action options Approve and Reject, and a text box to provide the reason for approving or rejecting the request.
  - **Included Requests:** This section displays other requests that could be part of the service package requests, such as claims. The section shows claim value ID, name of the claim code, a reason for the request, and action options Approve and Reject.

#### To approve a service package request by users

1. In the Service Package Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: Service package dialog box, to approve the request, the **Approve** button in the Service package details section needs to be selected. Approve is default selection.
3. In the **Reason** box, type a reason for approving the request.
4. In the Included Requests section, if there are other requests such as a request for a claim value ID, click **Approve** or **Reject** to approve or reject the request, respectively. In the **Reason** box, type a reason for rejecting other requests.



**Note:** If the request for the claim value ID is rejected for some reason, on submitting the changes, the application displays a message that the service package must be associated with at least one claim value.

5. Click **Submit**.

If everything is approved, then a message displays that you successfully submitted your decision.

The approved service package request is no longer listed in the Service Package Requests page.

### To reject a service package request by users

1. In the Service Package Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: Service package dialog box, click **Reject** in the Service package details section to reject the request.

If there are requests in the Included Requests section, a warning displays the message that all the included requests would also get rejected and would be removed from the request queue.

In the Included requests section, the area with the requests becomes unavailable and cannot be edited.

3. In the **Reason** box, type a reason why you rejected the request.
4. Click **Submit**.

A message displays that you successfully submitted your decision.

### 8.2.3 Claim code requests by users

Security administrators and Exchange operators need to view all of the claim code and claim value requests by users for service packages granted to their organization or across a realm, respectively, so that they can see the details of the requests and take appropriate action to meet the requests.

The Claim Code Requests tab lists all the claim code requests for a SAO (Service Authority Organization) package and displays the related details in the following columns:


- **Requested By:** ID of the user who made the claim code request for a service package.
- **Request ID:** ID of the claim code request from the user.
- **Claim Code:** Name of the requested claim code.
- **Claim Value:** ID of the requested claim value.
- **Service Package ID:** ID of the service package related to the requested claim code.
- **Service Package Name:** Name of the service package related to the requested claim code.
- **Justification:** The reason provided during the request for the claim.
- **Requested Date:** Date and time of the request for the claim.

Clicking a request item would open the request details in another dialog box. See [“View , approve, or reject claim code requests by users” on page 184.](#)

### 8.2.3.1 Filter claim code requests by users

As an administrator, you can filter or refine the list of claim code requests by users to find specific ones or find ones using certain search criteria.

#### To filter or refine the list of claim requests

1. Make sure the Claim Code Requests tab is selected and click **Filter**  on the page.
2. In the Refine by pane, use one, some, or all the options to use as criteria to refine the list and only display the matching requests:

- **Claim ID:** Enter the requested claim code name.
- **Package ID:** Enter the ID of the service package that includes the requested claim code.
- **Claim Value ID:** Enter the ID of the requested claim value.
- Click **Filter** to start the process to search for the records that match the criteria your provided in the Refine by pane.

The matching records are listed in the Claim requests page. The fields used for the search are shown as tokens above the column names on the page. Nothing is shown if no matching requests are found.

- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** or the **Filter** icon to close the Refine by pane.

### 8.2.3.2 View , approve, or reject claim code requests by users


Administrators can view the details of the claim code requests they receive from users in the Request: Claim dialog box and then choose to either approve or reject those requests.

#### To view the details of a claim request

1. In the Claim requests page, after refining the listed records if needed, click the request whose details you want to view.
2. The Request: Claim dialog box displays the following details:
  - **Requester Details:** This section shows the details such as name of the user making the request, user ID, , requester email and phone number, requester's organization ID.
  - **Claim Details:** This section shows the details of the claim code request such as claim code, request creation date, service package ID, service package claim ID, service package claim type, and the phase in which the claim request is in such as pending security administrator approval. The section



also shows Approve and Reject options, and a text box to provide the reason for approving or rejecting the request.

- **Included requests:** Displays the claim name which lists the requested claim value ID, a reason for the request, and action options Approve and Reject. If there are multiple requests and all need to be either approved or rejected, then click the arrow icon  adjacent to the Action column name and from the list, select either **Approve All** or **Reject All** as needed.

Enter a reason for approving or rejecting each included request in the Reason text box in Claim Details.

### To approve a claim code request by users

1. In the Claim Code Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: Claim dialog box, click the **Approve** option in the Claim Details section to approve the request.
3. In the **Reason** box, type a reason for approving the request.
4. In the Included Requests section, if there are other requests such as a claim value ID request, then click the **Approve** or the **Reject** option to approve or reject the request, respectively. In the **Reason** box, type a reason for approving or rejecting the claim value ID requests.
5. Click **Submit**.

A message displays that you successfully submitted your decision.

The approved claim code request item is no longer listed in the Claim Code Requests page.

### To reject a claim code request by users

1. In the Claim Code Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: Claim dialog box, click the **Reject** option in the Claim Details section to reject the request.

A warning displays the message that all the included requests would also get rejected and would be removed from the request queue.

In the Included Requests section, the area with the requests becomes unavailable and cannot be edited.
3. In the **Reason** box, type a reason why you rejected the request. If a reason is not provided, then on submission, a message displays that a reason is mandatory when you reject a claim code request.
4. Click **Submit**.

A message displays that you successfully submitted your decision.

The rejected claim code request is no longer listed in the Claim Code Requests page.

## 8.2.4 Claim value requests by users

Users can request additional claim value ID for claim codes that have already been approved.

Security administrators and Exchange operators need to view all of the claim value requests by users for service packages granted to their organization or across a realm, respectively, so that they can see the details of the requests and take appropriate action to meet the requests.

The Claim Value Requests tab lists the requests for additional claim value IDs for already approved claim codes for a SAO (Service Authority Organization) package. The tab displays the related details in the following columns:


- **Requested By:** ID of the user who requested additional claim value ID.
- **Request ID:** ID of the claim value request from the user.
- **Claim Code:** Name of the approved claim code for which additional claim value ID is being requested.
- **Claim Value:** Requested claim value ID.
- **Service Package ID:** ID of the service package related to the requested claim value ID.
- **Service Package Name:** Name of the service package related to the requested claim value ID.
- **Justification:** The reason provided during the request for the claim value ID.
- **Requested Date:** Date and time of the request for the claim value ID.



Clicking a request item would open the request details in another dialog box. See [“View , approve, or reject claim code requests by users” on page 184.](#)

### 8.2.4.1 Filter claim value requests by users

As an administrator, you can filter or refine the list of claim value requests by users to find specific ones or find ones using certain search criteria.

#### To filter or refine the list of claim requests

1. Make sure the Claim Value Requests tab is selected and click **Filter**  on the page.
2. In the Refine by pane, use one, some, or all the options to use as criteria to refine the list and only display the matching requests:
  - **Claim ID:** Enter the approved claim code for which claim value ID is being requested.

- **Package ID:** Enter the ID of the service package that includes the requested claim value.
- **Claim Value ID:** Enter the requested claim value ID.
- **Start Date:** Use the Start Date and End Date fields to search for requests made during a specific time frame. Click the calendar icon  and select a date as a start date for the search.
- **End Date:** Click the calendar icon  and select a date as the end date for the search time frame. If a date is not selected, the current date is used as the end date.
- Click **Filter** to start the process to search for the records that match the criteria you provided in the Refine by pane.  
The matching records are listed in the Claim requests page. The fields used for the search are shown as tokens above the column names on the page. Nothing is shown if no matching requests are found.
- Click the **X** in individual tokens to remove that filter and re-run the search automatically and display the adjusted matching list again or click **Clear All** to remove all the filters and display all the records on the page.
- Click **Close** or the **Filter** icon to close the Refine by pane.

#### 8.2.4.2 View , approve, or reject claim value requests by users

Administrators can view the details of the claim value requests they receive from users in the Request: Claim dialog box and then choose to either approve or reject those requests.

##### To view the details of a claim value request by users

1. In the Claim Value Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. The Request: Claim dialog box displays the following details:
  - **Requester Details:** This section shows the details such as name and ID of the user making the request, requester email and phone number, and requester's organization ID.
  - **Claim Details:** This section shows the details of the claim request such as claim code, request creation date, service package ID, service package claim ID, service package claim type, and the phase in which the claim request is in such as pending security administrator approval. The section also shows the status of the claim code as Approved and a reason text box to provide the reason for approving or rejecting the request.
  - **Included requests:** Displays the claim name column that shows the requested claim value ID, a reason for the request, and action options Approve and Reject.

### To approve a claim value request by users

1. In the Claim Value Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: Claim dialog box, to approve the request claim value ID, the **Approve** option needs to be selected. Approve is the default selection.
3. In the **Reason** box, type a reason for approving the request.
4. Click **Submit**.  
A message displays that you successfully submitted your decision.  
The approved claim item is no longer listed in the Claim Value Requests page.

### To reject a claim value request by users

1. In the Claim Value Requests page, after refining the listed records if needed, click the request whose details you want to view.
2. In the Request: Claim dialog box, to reject the request, click **Reject** in the Included Requests section for the listed claim value ID.
3. In the **Reason** box, type a reason why you rejected the request. If a reason is not provided, then on submission, a message displays that a reason is mandatory when you reject a claim request.
4. Click **Submit**.  
A message displays that you successfully submitted your decision.  
The rejected claim item is no longer listed in the Claim Value Requests list.

## Chapter 9

# Appendix

## 9.1 Administrator Roles

A definition of all Administrator Roles is listed here for informational purposes.

There are several administrator roles available in IAM that can be assigned to users. These roles can be used independently or multiple roles can be combined for a broader variety of administrative options. The available roles include:

---

### Organization Password Administrator

Searches for users' profiles and resets users' passwords

---

### Organization Service Administrator

Administers a specific service package as well as subpackages associated with it

---

### User Account Administrator

Rejects or approves new user requests. (This role is appropriate for someone in a position to confirm that the user should have access to the secured portal)

---

### Security Administrator

A superset of all administrator rights and responsibilities. An organization can have as many or as few administrators as needed.

---

The following section displays roles and privileges in two ways. First, [“Matrix of privileges associated per role” on page 189](#) is comprised of privileges associated per role in a matrix view. Second, [“List of privileges associated per role”](#) is comprised of privileges associated per role in a list view.

**Table 9-1: Matrix of privileges associated per role**

Privileges	General User	Password Admin	User Account Admin	Service Admin	Security Admin
Approve / Reject Division'S Service Package Request	-	-	-	X	X
Approve / Reject New User Registration Requests	-	-	X	-	X

Privileges	General User	Password Admin	User Account Admin	Service Admin	Security Admin
Approve / Reject Organization Service Request	-	-	-	-	X
Approve / Reject Site Codes For Divisions Of Your Org	-	-	-	-	X
Approve / Reject User'S Service Package Requests	-	-	-	X	X
Audit User Grants	-	-	X	X	X
Audit Users In Company (Quarterly & Annually)	-	-	X	-	X
Change Email Preferences For Self	-	X	X	X	X
Change Password Of Self	X	X	X	X	X
Delete A Division In Your Org	-	-	-	-	X
Delete A User Account	-	-	X	-	X
Edit Organization And/Or Division Profile	-	-	-	-	X
Edit Profile Of Others	-	-	X	-	X
Edit Profile Of Self	X	X	X	X	X

Privileges	General User	Password Admin	User Account Admin	Service Admin	Security Admin
Generate A Service Summary Report	-	-	-	-	X
Generate Report Of User Summary By Organization	-	-	-	X	X
Generate Report Of Users Grants Per Service. Package	-	-	-	X	X
Generate Security Administrator Reports	-	-	-	X	X
Grant A Service Package To A Division In Your Org	-	-	-	-	X
Grant A Service Package To A User	-	-	-	X	X
Invite Users To Register	-	-	X	-	X
Modify User Roles	-	-	-	-	X
Remove A Service Package From A Division In Your Org	-	-	-	-	X
Remove Service Package From A User	-	-	-	X	X

Privileges	General User	Password Admin	User Account Admin	Service Admin	Security Admin
Request A Service Package For My Organization	-	-	-	X	X
Request A Service Package For Self	X	X	X	X	X
Reset Password Of Others	-	X	X	-	X
Search /View Details For Divisions In My Organization	-	X	-	X	X
Search For Users In My Organization	-	X	X	X	X
Specify Password For Self	-	X	-	-	X
Specify Password Of Others	-	X	-	-	X
Suspend A Division In Your Org	-	-	-	-	X
Suspend A User Account	-	-	X	-	X
View My Organization al Administrators	X	X	X	X	X
View Organization 'S Hierarchy	-	-	-	-	X
View / Cancel Pending Requests Of Self	X	X	X	X	X



Privileges	General User	Password Admin	User Account Admin	Service Admin	Security Admin
View Request History Of Others	-	-	-	X	X
View Request History Of Self	X	X	X	X	X

### List of privileges associated per role

**Table 9-2: Privileges associated to all registered users (General Users)**

Change password of self	View my organizational administrators
Edit profile of self	View / cancel pending requests of self
Request a service package for self	View request history of self

**Table 9-3: Privileges associated to password administrator**

All of General Users +	Search for users in my organization
Reset password of others	Specify password for self
Search / View details for divisions in my organization	Specify password of others

**Table 9-4: Privileges associated to user account administrator**

All of General Users +	Delete a user account	Search for users in my organization
Approve / Reject new user registration requests	Edit profile of others	Suspend a user account
Audit user grants	Invite users to register	
Audit users in company (Quarterly & Annually)	Reset password of others	

**Table 9-5: Privileges associated to service administrator**

All of General Users +	Generate report of users' grants per svc. package	Search /View details for divisions in my organization
Approve / Reject division's service package request	Generate security administrator reports	Search for users in my organization
Approve / Reject user's service package requests	Grant a service package to a user	View request history of others

Audit users in company (Quarterly & Annually)	Remove service package from a user	
Generate report of user summary by organization	Request a service package for my organization	

**Table 9-6: Privileges associated to security administrator**

All of General Users +	Generate a service summary report	Search / View details for divisions in my organization
Approve / Reject division's service package request	Generate report of user summary by organization	Search for users in my organization
Approve / Reject new user registration requests	Generate report of users' grants per svc. package	Specify password for self
Approve / Reject organization service request	Generate security administrator reports	Specify password of others
Approve / Reject site codes for divisions of your org	Grant a service package to a division in your org	Suspend a division in your org
Approve / Reject user's service package requests	Grant a service package to a user	Suspend a user account
Audit user grants	Invite users to register	View organization's hierarchy
Audit users in company (Quarterly & Annually)	Modify user roles	View request history of other
Delete a division in your org	Remove a service package from a division in your org	
Delete a user account	Remove service package from a user	
Edit organization and/or division profile	Request a service package for my organization	
Edit profile of others	Reset password of others	