opentext™

OpenText™ Identity Manager CE 24.4 (v4.10)

Using the Identity Applications

January 2025

Legal Notice

Copyright 2009 - 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Welcome to OpenText Identity Manager

OpenText Identity Manager enables your organization to manage the user accounts and permissions associated with the wide variety roles and resources available to you.

This application helps you with the following situations:

I want something

If you need an item, whether the item is a piece of equipment like a laptop or something intangible like access to a particular server or application, you can request that item. For more information about making requests, see Request Permissions.

I need to do something

You might need to approve or review someone's request for permissions or other assigned tasks in the OpenText Identity Manager system. You can review all tasks waiting for your action. For more information about managing and addressing pending tasks, see View and Manage Tasks.

What do I have?

You can view all of the roles and resources assigned to you. For more information about your current permissions, see Review Your Permissions.

How did I get it?

You can review requests that you previously made, as well as the status of requests that have not been fulfilled. For more information about viewing your request history, see Review a History of Requests.

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

1 Applications Page

Applications provides a single access point for all users and administrators to the following types of activities in the identity applications:

- Manage your profile settings and password
- Reviewing and completing your tasks, such as approving user requests for access
- Requesting permissions for roles, resources, or processes
- Review the status and history of your requests for permissions
- Find other users in your organization

The **Applications** page might include links to websites and applications that your organization considers important. Also, depending on your role or permission level, you might have access to the following functions:

- Assign roles
- Assign resources
- Create users
- View groups
- OpenText Identity Manager Reporting

However, to create or manage roles and resources, you must use Catalog Administrator. To create or manage groups, use the legacy User Application.

Customize the Applications Page

If you have an administrative role for the identity applications, you can customize **Applications** for all users. You can configure the page to show items and links that your users need to see, organized into categories that make sense for your enterprise. You can include the following items:

- OpenText Identity Manager functions, such as creating groups or running reports
- Permissions that most users need to request
- Links to commonly accessed websites or web-based applications
- REST endpoints
- Badges, such as the number of items of a certain type that a user can access

To configure **Applications**, select ⚙. For more information, see Configure the Applications Page.

To change look and feel of the application, such as logos and localization, see Customize the User Interface.

2 Configure the Applications Page

As an administrator for the identity applications, you can modify the **Applications** page to display all the applications, activities, and permissions that you want users to access. By default, the identity applications provide a **Home items** category, which cannot be deleted.

After you complete your changes, click **Edit done** to return to **Applications**.

Create and Edit Items and Permissions

You can create any number of applications and permissions that you might want to add to the **Applications** page. You do not have to add these items to **Home items** or other **Applications** categories.

1. (Conditional) To create a new item, click **+**.
2. Complete the form for the application or permission.

   NOTE: You must specify a value for all fields that have an asterisk (*), such as the name and description for an application.

3. (Optional) Drag and drop the new application or permission to a category.
4. (Conditional) To modify an existing item, select the edit icon within the tile, then update the values.

Add, Modify, or Delete a Category

You can organize **Applications** items into logical categories. You can create any number of categories that your organization might need. You can also rearrange the tiles within a category or move tiles to a different category.

Add a Category

1. Select **New Category**.

   OpenText Identity Manager adds the category at the end of the category groups. You might need to scroll down to view the added category.
2. Specify the name of the new category.
3. Click **+**, then select **Application** or **Permission**.
4. Complete the form for the application or permission.

   NOTE: You must specify a value for all fields that have an asterisk (*), such as the name and description for an application.

5. Select **+Add**.

Modify a Category

You can modify a category in the following ways:

- Add tiles for applications and permissions by dragging and dropping them from the **New Items** and **Permissions** section on the right side of the page
- Remove an application or permission by selecting the trash icon within the item's tile
- Change the settings for an item
- Change the name of the category
- Reorder the items within the category

Delete a Category

To delete a category, select the trash icon to the right of the category's name.

II Dashboard

The Dashboard provides quick information about your tasks and requests. You can navigate to specific pages or applications with a single click. Additionally, you can add, remove, reposition, and configure widgets on your Dashboard.

- Chapter 3, “Customize Your Dashboard,” on page 11

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

3 Customize Your Dashboard

The identity applications provide many options to change the display of your dashboard and then save it as a personalized view. For example, you can add widgets and reposition them based on your interest. You can also configure the widget fields and personalize them. This document helps you understand the different options to personalize your dashboard.

Manage the Global Dashboard

The global dashboard includes a set of widgets that will appear on the dashboard of every user in the system. Users can view these widgets based on their access provided by an administrator. For more information about provisioning dashboard widgets, see "Manage Dashboard Widgets" on page 147.

The **Manage Dashboard** option allows you to add or modify or remove widgets from the global dashboard. You must be added as trustee to use the **Manage Dashboard** option.

Administrator can add any user/group/container/role as a trustee to manage the global dashboard. To modify trustees to manage dashboard, go to **YourID > Settings > Access** and click **Global Dashboard** from the list. For more information about modifying configuration access, see "Configuring User Access" on page 142.

NOTE: By default, Provisioning Administrator has an access to manage the global dashboard.

Manage Widgets and Layouts

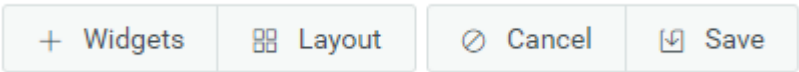
Widgets are Dashboard objects that are designed to provide specific details of a user for particular activity. For example, the Tasks widget provides details about new tasks, claimed tasks, or the tasks that are expected to expire shortly. Similarly, there can be many other widgets which can be configured on your Dashboard.

Administrators who have access to the **Settings** page can provision widgets for a User, Group, Container, or a Role. For more information, see "Manage Dashboard Widgets" on page 147.

To personalize your Dashboard, go to your **Dashboard** and click ∘∘∘.

Use the following are options to personalize your Dashboard:

Figure 3-1 *Personalization Options*



Widgets

Allows you to add Widgets to your Dashboard. See "Add a Widget" on page 12.

Layout

Allows you to change the Dashboard layout. See "Change the Dashboard Layout" on page 16.

Cancel

Cancels all the changes made to your Dashboard.

Save

Saves your changes and applies to your Dashboard.

Add a Widget

To add new widget to your Dashboard, go to **Dashboard** and click ∘∘∘ and select **Widgets**.

Widgets are categorized as **General** and **IDM** based on their features:

Add General Widgets

General category allows you to add widgets to your dashboard outside of OpenText Identity Manager standard widgets. You can specify the REST API URL of the required widget and display the required information in the form of line, pie, or table charts.

1. Select any of the following widget type from the list:
   - **Line Chart:** Displays the requested information for the selected element in the form of line chart.
   - **Links:** Allows you to bookmark frequently used links that helps you to access them quickly.
   - **Pie Chart:** Displays the requested information for the selected element in the form of pie chart.
   - **Table:** Lists the requested information for the selected element in a table form.
2. Click ⚙ to configure the widget added to your dashboard.
3. (Conditional) For **Line Chart**, **Pie Chart**, and **Table** widgets, specify the following details:
   - **Title:** Specifies the widget name that will be displayed on your Dashboard.
   - **URL:** Specifies the REST API URL of the required widget that you want to show on your Dashboard.
   - **Root Element:** Specifies the element from the REST API code for which you want to display a chart. This field is case sensitive. You must enter the exact same name which is mentioned in the REST API code.
   - **Columns:** Specifies the columns that you want to display on your widget. You can add multiple columns. **Title** specifies the display name for a column. **Path** specifies the column name as mentioned in the REST API. **Path** field is case sensitive. You must enter the exact same string from the REST API code.

   The following is a sample REST API code for the **Roles** page:

```
{
    "total": 12,
    "nextIndex": 0,
    "token": "60045d6be10f4419a2da9fa728683b06",
    "assignments": [
        {
            "id":
"cn=aaacccc,cn=level30,cn=roledefs,cn=roleconfig,cn=appconfig,cn=user
application driver,cn=driverset1,o=system",
            "name": "AAAcccc",
            "description": "afasfdsf",
            "entityType": "role",
            "link": "/IDMProv/rest/access/assignments/item",
            "bulkRemovable": "true",
            "categories": [
                {
                    "categoryId": "default",
                    "categoryName": "Default"
                }
```

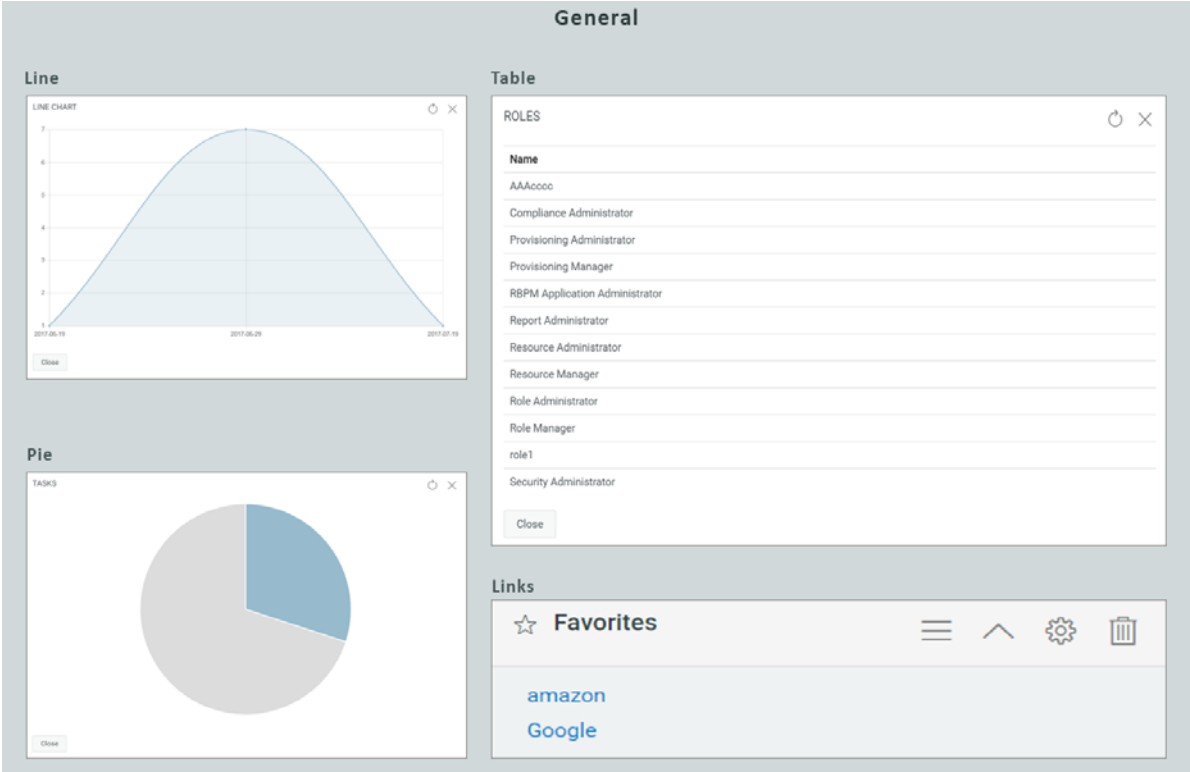

In this sample, assignments is the Root element and name is the selected column to display that will be displayed on the widget. You can also bookmark any URL that you wish to access from your Dashboard

4 (Conditional) For Links widgets, specify the **Title** for the links and add links that you wish to access from the Dashboard.

5 Click **Save** to apply your changes.

The following are sample chart and link widgets that can be added to your Dashboard:

Figure 3-2 Example for General Widgets



Add OpenText Identity Manager Widgets

IDM category allows you to add standard or defined OpenText Identity Manager widgets to your Dashboard.

For example,

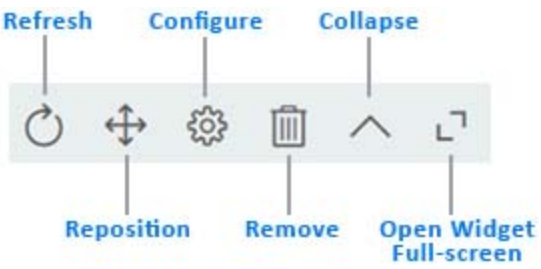
- **Access:** Displays the count of roles and resources, and other information about them.
- **Request For Others:** Displays pending and denied requests for other users and allows you to create request for these users.
- **Self Requests:** Displays the pending and denied requests count and also allows you to create a new request.
- **Tasks:** Displays the count of new or pending tasks, or the tasks that are about to expire.

To configure these widgets, see "Configure a Widget" on page 15.

IMPORTANT: To apply your changes, click Save.

Widget Options

You can perform the following operations on widgets:



Refresh

Updates the widget content with the latest information.

Reposition

Allows you to move the widget across dashboard.

Configure

Allows you to configure the widget properties. For more information, see "Configure a Widget" on page 15.

Remove

Deletes the widget from the dashboard.

Collapse

Hides the widget information and shows only the widget title.

Open Widget Full-screen

Displays the widget information in full-screen mode.

NOTE:

- **Refresh** and **Open Widget Full-screen** options are displayed only for **General** category widgets.
- To apply your changes, click **Save**.

Configure a Widget

You can configure each widget that is added to your dashboard. For example, you can enable or disable the fields of a widget or change the display color of the fields.

1. Click ⚙ on the widget that you wish to configure.
2. Modify the widget properties.

   For example, you can change the title of a widget, or change the color of a label for a widget field. You can also enable or disable a widget field in the properties page.
3. Click **Apply** to view the changes on the dashboard.

To configure **General** widgets, see "Add General Widgets" on page 12.

IMPORTANT: To apply your changes, click **Save**.

Change the Dashboard Layout

The identity applications allow you to modify the layout of the appearance of the widgets on your dashboard.

1. Click ∘∘∘.
2. Select **Layout**.
3. Choose the layout that you wish to see on your dashboard.

IMPORTANT: To apply your changes, click **Save**.

III Tasks

Tasks represents activities assigned to you. You might need to review or approve someone's request for permissions or other tasks in the OpenText Identity Manager system. This application enables you to perform the following activities:

- Chapter 4, "View and Manage Tasks," on page 19
- Chapter 5, "Review the History of Executed Tasks," on page 23
- Chapter 6, "Act as or Assign a Proxy," on page 25
- Chapter 7, "Manage Approvals by Email," on page 27

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

4 View and Manage Tasks

By default, **Tasks** lists requests for permissions that you are responsible for approving or denying. You can take action on these requests one at a time or perform a bulk action for multiple simple requests that do not require detailed information.

Viewing your Tasks

To manage your tasks, select **Task > Tasks**. To view tasks assigned to others, click **Others**.

If you are serving as a proxy or delegate for other's tasks, you can complete tasks that are assigned to someone else. For more information about proxy assignments and delegation assignments, see Act as or Assign a Proxy.

IDM Approvals: *Applies if you have enabled the* **Show IG Approvals in tasks page** *option in the* **Configuration > Identity Governance** *page.*

This tab lists all the OpenText Identity Manager tasks. By default, it lists all the **Self** tasks. To view others tasks with an appropriate role, click **Others**.

- You can search your tasks using **Reassigned Tasks**, **Returned Tasks**, or **Delegated Tasks** filters. Using **Delegated Tasks** filter for the **Self** option displays only the tasks that are delegated to you.
- If you are an administrator, you can also filter tasks using **Assigned to me**, **Recipient as me** filter.
- If you are searching others tasks you can use **Returned Tasks**, **Reassigned Tasks**, or **Delegated Tasks** filter. Using **Delegated tasks** filter for **Others** shows all the tasks that are delegated to other users in the system.
- You can also refine your task search based on tasks occurred in the system:
  1. Select .
  2. (Conditional) To see the tasks created for a certain period, specify the period in **Weeks**, **Days**, or **Hours**.
  3. (Conditional) Specify the task status that you wish to filter.
  4. Click **Filter**.
- If you are a helpdesk user, you can use **Helpdesk Tasks** filter to see the refined list. To manage helpdesk task, see the Dashboard help.
- You can use the Column Customization option to hide or display columns on the Tasks page. Select the check box next to the desired column that you want to view. If you wish to hide columns, uncheck the box next to it. To restore the default columns, first select all the columns by selecting the box next to the search field, then deselect it.

At times, you might have to approve requested items if the Access Request policy specifies you as an approver for requests. These approval requested items are listed in the **Approvals** tab.

IG Approvals: *Applies if you have enabled the* **Show IG Approvals in tasks page** *option in the* **Configuration > Identity Governance** *page.*

This tab lists all the pending approval tasks for Identity Governance. You can reassign the tasks to others using the **Reassign** option.

Approve and Deny Requests

One Request at a Time

1. Click a request that you want to approve or deny.

   Displays a form that provides an information on the selected request.
2. (Optional) Add a comment related to your approval or rejection of the request.
3. Select **Approve** or **Deny**.

Multiple Requests at the Same Time

1. Select the check box for the request(s) that you want to approve or deny.

   NOTE:

   - For a more complex request that requires detailed information, the application does not display a check box. You must approve or deny those requests individually. For more information, see One Request at a Time.
   - When you select a more complex request to approve or deny, the Dashboard might need to open the request form in a separate browser tab.
2. Select **Approve** or **Deny**.
3. Provide a comment explaining why you want to approve or deny the selected requests.
4. Select **Approve** or **Deny**, as appropriate.

Managing Requests for Approval or Denial

In some organizations, a group of people might be responsible for reviewing, approving, and denying requests for access. When this occurs, each member of the group receives the same requests. For example, the IT Services team might be responsible for all requests for telecommunications and computing equipment. When a new employee requests a cellphone, the request gets assigned to all members of the IT Services team. Anyone on the team can complete the request.

You can perform any of the following tasks on the request:

Claim Request

You can **claim responsibility** for a request and act on the required task immediately or later. Regardless of when you act on the task, other members of your group can no longer see that request in their **Tasks**.

To claim a task, select the request, then select **Claim**.

Release Request

If you do not want to act on the request that you have claimed, you can release that request. Select the request that you want to release and click **Release**.

Reassign Request

To reassign a task, select the request under the **Self** tab, then select **Reassign**. The task is automatically reassigned to your manager.

Provisioning Administrator and Provisioning Manager roles can reassign the tasks to any user in the organization.

As a team manager, you can only reassign self tasks to your own manager. However, if you want to reassign a task that is allocated to a member of your team, you can do so using the **Others** tab. Go to **Others** tab, select the required task check box, and then click **Reassign**. In the **Assign to** drop-down menu, select the team member to whom you want to reassign the task, provide a comment for reassignment, and click **Reassign**. The task is reassigned to the team member of choice.

NOTE:

- To reassign a claimed request, first release the request and then reassign it.
- You can reassign a task to the manager who belongs to the defined hierarchy. For more information, go to **Your ID > Settings > Customization > General**. An administrator who can access the **Settings** page has the permission to change the hierarchy. For more information, see Customize the Views.

Return Request

If you do not want to act on a request that is reassigned to you, you can return that request. Select the request that you want to return and click **Return**. The identity applications automatically assigns the returned task to the actual approver.

NOTE: Only a reassigned request can be returned.

Manage Helpdesk Tasks

Helpdesk tasks are generated for every helpdesk ticket raised in the system. If you are a helpdesk user, you can take appropriate actions for your helpdesk tasks.

NOTE: You can **Claim** or **Release** a helpdesk task. If you claim a helpdesk ticket from the list of tasks, helpdesk ticket appears in your **Self** tasks.

---

1. Click the **Helpdesk Ticket** that you want to address.
2. Add a comment that describes your action.
3. Perform any of the following actions for the helpdesk ticket.

   Update

   Updates the helpdesk ticket with the comment added in Step 2.

Complete

Resolves the helpdesk ticket with the comment added in Step 2.

Cancel

Closes the helpdesk ticket with the comment added in Step 2.

5 Review the History of Executed Tasks

Task History keeps track of your executed tasks. It shows the status of actions you completed for the tasks assigned to you, including the requests for permissions that you approved or denied.

Viewing your Task History

By default, the **Task History** displays all **Self** tasks. However, with the appropriate role, you can also access the history of tasks performed by other users.

- To view your history, select **Task** > **Task History**.
- To view others' task history, click **Task** > **Task History** > **Others**.

  You must have one of the following roles:

  - Provisioning Administrator
  - Provisioning Manager
  - User Application Administrator
  - Team Manager
- To update the content in **Task History**, click .
- Under Task History, you can find detailed information about each executed task:
  - **Name:** Displays the name of the workflow associated with the permission.
  - **Requester:** Name of the individual who requested the permission.
  - **Recipient:** Name of the individual to whom the permission has been granted or denied.
  - **Requested Date:** The date and time when the requester made a permission request for themselves or on behalf of the recipient with the appropriate role.
  - **Action Date:** The date and time when you executed the task.
  - **Action Status:** The status of the task you executed.
  - **Final Status:** The final status of the workflow. This column is only visible to the appropriate roles.
- You can search your task history using the recipient and requester name filters. To view the task history for other users, you can search using the name of that user.
- You can also refine your task history search by following these steps:
  1. Select .
  2. (Conditional) To view tasks associated with a specific workflow, enter the date and time when the permission was requested, then select whether you want to filter for tasks before or after the chosen date.
  3. (Conditional) To view tasks that you executed on or before a particular date, enter the date and time, then select whether you want to filter for tasks before or after that date.

4. (Conditional) Specify the task status you wish to filter by. For example, approved or denied.
5. Click **Filter**.

- You can customize the columns displayed on the Task History page by using the **Column Customization** option. To show a specific column, check the box next to it. If you want to hide a column, uncheck the box. To restore the default columns, select the box next to the search field that checks all columns, and then uncheck it.

Review the Details of a Workflow

With the appropriate role, you can view your actions and the full workflow for the permission request. Each step in the process has a timestamp.

The details include the following types of information:

User

Actions that actual users took. These actions might include comments that you or an administrator included with each action.

System

Actions that the application takes to complete the approval process. For example, assigning the request to an individual who can approve the request.

User and System

Actions and comments by both users and the application.

6 Act as or Assign a Proxy

In some organizations, you might be allowed to complete tasks as a **proxy**, or delegate, for someone else. For example, a personal assistant might perform proxy actions for the boss. Also, while a coworker is on maternity leave, you might temporarily be assigned to act on her behalf.

To view your proxy assignments, select **Access > Proxy Assignment**. To create or manage proxy assignments, you must log in as an administrator or a team manager. The team manager can create assignments for team members only. For more information about managing teams, see Teams.

Act as a Proxy

An administrator might assign you to serve as a proxy for another user. When this occurs, the application adds a proxy option to your account menu in the upper right corner.

1. Select ***Your ID*** **> Proxy As**.
2. Enter the name of the person on whose behalf you intend to act.
3. Select **Continue**.
4. Complete any tasks assigned to the person for whom you are the proxy.

   For more information about tasks, see View and Manage Tasks.
5. (Conditional) To act as a proxy for a different individual, complete Step 1 through Step 4.
6. To stop acting as proxy, open the menu then select **Exit Proxy: *name***.

Manage Proxy Assignments

As an administrator or a team manager, you can create, modify, and delete an assignment. For a team manager to manage proxy assignments for a team, you must configure the team appropriately. For more information, see Enable Requesters to Make Proxy Assignments.

1. To add a proxy definition, select **+**.
2. To modify an existing proxy assignment, select the name of the definition in the **Proxy assigned** column.
3. Specify the following values:

   Proxy Assigned

   Specifies one or more users who can perform the proxy actions.

   Proxy as

   Specifies the users, groups, or containers on whose behalf the actions will be taken.

   Expiration

   Specifies the date on which the proxy assignment expires. To maintain the assignment indefinitely, leave the field blank.
4. To complete your changes, select **Create** or **Save**.

7 Manage Approvals by Email

If you are responsible for approving permissions requests, you might receive an email about a pending request. You can respond to the request in one of the following ways, depending on how the email notifications have been configured:

- Select the **Approve** or **Reject** action link in the message.

  After you select the action link, the software creates a new message with the appropriate Subject, To address, and content.
- Reply to the email by adding `approve` or `reject` to the **Subject** line.

Both methods allow you to add comments to the response email. For example, you can explain why you might have rejected a request.

To configure email approvals, select **Administration > Email Based Approval**.

Configuring Email-based Approvals

As an administrator, you can configure the identity applications to send an email that notifies users that they have a pending task to approve or reject a permission request.

NOTE: Before enabling email-based approvals, ensure that you have configured the provisioning request definitions (PRDs) to support notifications and (optional) digital signatures. Also, configure the outgoing mail server. For more information, see the *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications*.

Incoming Email Settings

- **Server Type**

  Specifies the type of server that you want to use for the incoming email notifications.

  If you select **IMAP**, you must also specify a value for **Folder**.
- **Host**

  Specifies the name or IP address of the incoming mail server.

  NOTE: Authentication does not apply to the outgoing mail server. OpenText Identity Manager does not support two-way authentication.

- **Email**

  Specifies the email address that receives the reply messages from users responsible for reviewing permissions requests.

  If the notification includes action links for approving or denying a request, OpenText Identity Manager automatically populates the To: field. Otherwise, users must specify valid email address in this field.

- **Authentication Required**

  Specifies whether the incoming mail server requires authentication.

- **Authentication Type**

  Applies only if you have enabled the **Authentication Required** *option.*

  Select whether you want to connect to your email server using basic authentication or modern authentication.

  - If you select **Basic Authentication**, then you must specify values for the following parameters:

    User ID

    Specifies the account required for server authentication.

    The account for the incoming mail server should be unique and thus not duplicate an account that might receive the email notifications.

    Password

    Specifies the password for the account.

  - If you select **Modern Authentication**, then you must specify values for the following parameters:

    NOTE: This release only supports modern authentication using the Office 365 OAuth authentication service provided by Azure Active Directory (Azure AD) for Microsoft Outlook. You must register your application with Azure AD to get the values for most these parameters. For more information on how to register your application, see Register an application with the Microsoft identity platform (https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app).

    User ID

    Specifies the account required for server authentication.

    The account for the incoming mail server should be unique and thus not duplicate an account that might receive the email notifications.

    Tenant ID

    Specifies the Global Unique Identifier (GUID) for your registered account on Azure Active Directory. Also referred to as the Tenant (Directory) ID.

    Use the Azure portal to obtain the value.

    Client ID

    Specifies the unique ID assigned by Azure Active Directory to your OpenText Identity Manager. Also referred to as the Application (client) ID.

    Use the Azure portal to obtain the value.

    Client Secret

    Specifies a secret string that OpenText Identity Manager uses to prove its identity when requesting an access token. This encrypted value is unique for your application.

    Use the Azure portal to obtain the value.

Scope

Specifies the resource for which the token is granted during token redemption. It defines what OpenText Identity Manager can access on behalf of the user. It should be `https://outlook.office365.com/.default` for SMTP.

The access token issued to the application is limited to the scope granted.

Request URL

Specifies the request URI of your email server, to which OpenText Identity Manager sends authentication requests containing the client secret, scope, grant type, and auth mechanism in the payload.

For example, `https://login.microsoftonline.com/{tenantID}/oauth2/v2.0/token`

Grant Type

Used by OpenText Identity Manager to obtain an access token to access their own resources, not on behalf of a user. The **Grant Type** parameter is set to `client_credentials` by default and cannot be modified.

Auth Mechanism

Specifies the format used by OpenText Identity Manager to encode and transmit the access token to the authentication server. The access token authenticates a user's Outlook account. By default, **Auth Mechanism** is set to X0AUTH2 and cannot be modified.

- **Folder**

  Required for an IMAP server

  Specifies the folder in the email system where you want to store the email notifications.

  The default folder is `INBOX`. For POP3 servers, you cannot change the folder name.

- **Enable SSL**

  Specifies whether you want to use Secure Sockets Layer (SSL) protocol for authentication.

- **Use default port**

  Specifies whether the email process uses the default port for the mail server. Otherwise, specify the port number you want to use to connect to the incoming mail server.

- **Polling Interval**

  Specifies how often you want to poll the incoming mail server for task notifications.

- **Token Expiration**

  Specifies the amount of time that each email-based approval will remain in effect.

  After the token expires, the email recipient cannot use that notification to approve or deny the task.

- **Cleanup Interval**

  Specifies the interval after which the server can clear expired tokens from the database.

- **Email Content Options**

  Specifies the type of information that you want to include in the notification:

Exclude action links

The notification does not include the action links that users can select to approve or deny the request.

To act on the request, users can reply to the email, then add the appropriate keyword, such as `Approve`, to the **Subject**. Alternatively, they can log in to the identity applications to complete the task.

Include action links without digital signature

The notification includes the action links that users can select to approve or deny the request. The email does not require a digital ID for authenticating the message content.

Include action links with digital signature

The notification includes the action links that users can select to approve or deny the request. It also requires a digital ID for authenticating the message content.

- **Approve** and **Reject**

  Specifies the terminology for the links in the email that users select to approve or deny the request.

  You can also modify these terms for all supported languages.

- **Success** and **Failure**

  Specifies the email templates that you want to use for indicating the results of users' actions.

  Success notifications occur after the user successfully approves or denies a task. The software sends a **Failure** notification when an error occurs in the approval process.

- **Enable Socks Proxy**

  Specifies whether you want to use a proxy server to process the approval emails. If not enabled, the server connects directly to the specified Inbox.

  If you enable this setting, you must also specify values for the following parameters:

  Proxy Host

  Specifies the name or IP address of the proxy mail server.

  Proxy Port

  Specifies the port that you want to use for incoming mail to the proxy server.

  Authentication Required

  Specifies whether the proxy server requires authentication for incoming mail.

  If you enable this setting, you must also specify a valid userID and password for the proxy server.

Outgoing Email Settings

- **Notification Template Host**

  Specifies the name or IP address of Tomcat that hosts the identity applications. For example, `myapplication serverServer`.

  This value replaces the $HOST$ token in e-mail templates. The installation program uses this information to create a URL to provisioning request tasks and approval notifications.

- **Notification Template Port**

  Specifies the port number of Tomcat that hosts the identity applications.

This value replaces the $PORT$ token in e-mail templates that are used in provisioning request tasks and approval notifications.

- **Notification Template Secure Port**

  Specifies the secure port number of Tomcat that hosts the identity applications.

  This value replaces the $SECURE_PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.

- **Notification Template Protocol**

  Specifies a non-secure protocol included in the URL when sending user email. For example, `http`.

  This value replaces the $PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications.

- **Notification Template Secure Protocol**

  Specifies the secure protocol included in the URL when sending user email. For example, `https`.

  This value replaces the $SECURE_PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications.

- **Notification SMTP Email From**

  Specifies the email account that the identity applications use to send email notifications.

- **SMTP Server Name**

  Specifies the IP address or DNS name of the SMTP email host that the identity applications use for provisioning emails. Do not use `localhost`.

- **Server requires authentication**

  Specifies whether you want the server to require authentication.

- **Authentication Type**

  Applies only if you have enabled the **Server requires authentication** *option.*

  Select whether you want to connect to your email server using basic authentication or modern authentication.

  - If you select **Basic Authentication**, then you must specify values for the following parameters:

    User name

    Specifies the name of a login account for the email server.

    Password

    Specifies the password of login account for the mail server.

  - If you select **Modern Authentication**, then you must specify values for the following parameters:

    NOTE: This release only supports modern authentication using the Office 365 OAuth authentication service provided by Azure Active Directory (Azure AD) for Microsoft Outlook. You must register your application with Azure AD to get the values for most these parameters. For more information on how to register your application, see Register an application with the Microsoft identity platform (https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app).

User name

Specifies the account required for server authentication.

The account for the incoming mail server should be unique and thus not duplicate an account that might receive the email notifications.

Tenant ID

Specifies the Global Unique Identifier (GUID) for your registered account on Azure Active Directory. Also referred to as the Tenant (Directory) ID.

Use the Azure portal to obtain the value.

Client ID

Specifies the unique ID assigned by Azure Active Directory to your OpenText Identity Manager. Also referred to as the Application (client) ID.

Use the Azure portal to obtain the value.

Client Secret

Specifies a secret string that OpenText Identity Manager uses to prove its identity when requesting an access token. This encrypted value is unique for your application.

Use the Azure portal to obtain the value.

Scope

Specifies the resource for which the token is granted during token redemption. It defines what OpenText Identity Manager can access on behalf of the user. It should be `https://outlook.office365.com/.default` for SMTP.

The access token issued to the application is limited to the scope granted.

Request URL

Specifies the request URI of your email server, to which OpenText Identity Manager sends authentication requests containing the client secret, scope, grant type, and auth mechanism in the payload.

For example, `https://login.microsoftonline.com/{tenantID}/oauth2/v2.0/token`

Grant Type

Used by OpenText Identity Manager to obtain an access token to access their own resources, not on behalf of a user. The **Grant Type** parameter is set to `client_credentials` by default and cannot be modified.

Auth Mechanism

Specifies the format used by OpenText Identity Manager to encode and transmit the access token to the authentication server. The access token authenticates a user's Outlook account. By default, **Auth Mechanism** is set to X0AUTH2 and cannot be modified.

- **Use SMTP TLS**

  Specifies whether you want to secure the contents of email messages during transmission between the mail servers.

- **Email Notification Image Location**

  Specifies the path to the image that you want to include in email notifications.

When the Identity Applications server and the email server are both set to use secure connection, make sure that the following conditions are met:

- The certificate used to establish a secure connection between the Identity Applications server and the email server is a trusted CA certificate
- Use `https` in the image path. For example, `https://localhost:8543/IDMProv/images`

If Identity Applications is operating on a server that uses http for plain text communication, replace `https` with `http` in the image path. An example of the image path: `http://localhost:8080/IDMProv/images`

- **Sign email**

  Specifies whether you want to add a digital signature to outgoing messages.

  If you enable this option, you must also specify settings for the keystore and signature key.

  Keystore Path

  Applies only when you enable **Sign email***.*

  Specifies the full path to the keystore (`cacerts`) file that you want to use for digitally signing an email. You can manually enter the path or browse to the `cacerts` file.

  For example, `/opt/netiq/idm/apps/jre/lib/security/cacerts`.

  Keystore Password

  Applies only when you enable **Sign email***.*

  Specifies the password for the keystore file. For example, `changeit`.

  Alias of signature key

  Applies only when you enable **Sign email***.*

  Specifies the alias of the signing key in the keystore. For example, `idmapptest`.

  Signature key password

  Applies only when you enable **Sign email***.*

  Specifies the password that protects the file containing the signature key. For example, `changeit`.

IV Permissions

Permissions represent the accounts, roles, and resources that you have or might be available to you. This application enables you to perform the following activities:

- Chapter 8, “Review Your Permissions,” on page 37
- Chapter 9, “Request Permissions,” on page 41
- Chapter 10, “Review a History of Requests,” on page 45

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

8 Review Your Permissions

Permissions lists all permissions -- roles and resources -- that have been assigned to you. Your organization might automatically assign you permissions or you might have requested them. For example, you receive a computer as part of your job, but you need to request access to a specific software application. You can also inherit some permissions indirectly through role relationships or if you are a member of a group or a container.

To view your permissions, select **Access > Permissions**. By default, you can see the list of permissions that are assigned or approved to you directly under the **Self** tab. To see the child permissions mapped with the assigned or approved permissions, click .

A team manager or supervisor can see the permissions of their team members in the **Others** tab. For more information, see Find a Permission of Others.

NOTE:

- The type of permissions listed on the permissions page may vary, depending on how the administrator has configured the settings for this page. For more information, see "User Settings" on page 144.
- **Permissions** allows you only to view and revoke permissions assigned to you. To request a role, resource, or PRD, go to **Access > Requests**. To view a history of your requests, go to **Access > Requests History**.

To update the content in **Permissions**, select .

Review the Details of a Permission

For each assigned permission, you can review the details such as the date assigned and who requested the permission. To review the details, select the permission's name.

The following table lists the fields displayed for individual permission:

Field	Description
Description	The description of the role or resource.
Effective Date	The date and time of permission assignment.
Expiration Date	The date after which the permission will no longer be assigned to the user. It is only displayed for the permission that have the expiration option enabled.
Reason	Specifies the reason for assigning the permission to the user.

Field	Description
Assigned Permission via	Specifies who assigned the permission to the user. If a role is assigned to the user directly through an approval process, you can see the list of approver(s) who approved the assignment request under the **View Role Approval Information** option. If a role is inherited by the user through membership to a group or a container, the following details are displayed under the **View Role to Group Assignment Information** option: ◆ **Requested by**: Specifies who requested the permission. ◆ **Request Description**: The description provided while requesting the permission. ◆ **Approver details:** Click the link to see the list of approver(s) who approved the role assignment request.

Find a Permission of Self

By default, **Permissions** lists all of your assigned permissions under **Self** tab. To find a specific permission, you can use any of the following options:

Simple

Enter any permission name, description, or CN. You can change the search criteria to **ROLE** or **RESOURCE** to see a more refined list.

Advanced

To filter the search for **roles**, change the search criteria to **ROLE**, then select . Specify any of the following criteria under **Role Filter(s)**:

- Role category.
- Source of the role, such as the group to which the role belongs. For example, Finance.
- Date the role was assigned.
- Date the role expires.
- Description included with the request for the role.

To filter the search for **resources**, change the search criteria to **RESOURCE**, then select . Specify any of the following criteria under **Resource Filter(s)**:

- Resource category.
- Date the resource was requested.
- Description included with the request for the resource.
- Parameter included with the request for the resource.

Find a Permission of Others

If you are a identity applications Administrator, you can search and view permissions of other team members.

1 On the **Permissions** page, click **Others**.

2 You can search **By User** or **By Permission** names.

   2a (Conditional) If you are searching **By User**, enter the user name.

   2b (Conditional) If you are searching **By Permission**, enter the permission details.

NOTE: Searching by permission details is not supported for a team manager or supervisor user. However, they can see the permissions of their team members by searching for their team name or description. In addition, a search by user name is also provided on the page to allow searching and viewing permissions of a specific team member.

Remove a Permission

On occasion, you might need to request that a permission be revoked because the permission no longer applies to you. For example, you transferred from the Finance department to Technical Support. In your new role, you should not have access to company financial statements so that permission should be revoked.

To revoke any of your permissions:

1 Select the permissions that you want to revoke.

2 Click 🗑.

3 Specify a reason for removing the selected permissions.

4 Click **Revoke Permission(s)**.

You must have necessary administrator rights to revoke any permissions for **Others**. Perform the following steps to remove permissions of others:

1 In **Others**, search for the permissions that you want to revoke. You can search **By User** or **By Permission** names.

   1a (Conditional) If you are searching **By User**, select the permission that you want to revoke.

   1b (Conditional) If you are searching **By Permission**, select the user whose access to be revoked.

NOTE: If you are a team manager, perform the following to revoke permissions.

1. Select the team and search for team members.
2. Select the user permissions that you want to revoke.

---

2 Click 🗑

3 (Optional) If you want revoke permission for multiple users or revoke multiple permissions of a user, click ☰.

You can save your selection in the queue and revoke the permissions anytime. To revoke the permissions in the queue, click .

4 Specify the reason for removing the selected permissions.

5 Click **Revoke Permission(s)**.

Customize Columns

1 Click to customize the columns.

2 (Conditional) Select the check box next to the desired column that you want to display. The selected columns are added simultaneously to the Permissions page.

TIP:

- To choose all columns, select the check box next to the search field.
- To restore the default columns, select the check box next to the search field, then deselect it. It displays the columns set to display by default on this page.

---

3 Click **X** on the Column Customization window to save your preferences.

9 Request Permissions

Your organization might provide a variety of permissions -- roles, resources, and processes (workflows) -- that you can request for yourself. For example, you might be able to request a new computer or access to a specific software application. You can also request permissions on behalf of other individuals. For example, you might be a manager requesting access to software for one of your employees.

Your organization specifies which permissions are listed as **Featured Items**. Usually, these are permissions that are often requested, to make it easier for individuals to request access. However, you can also search for or request permissions not displayed in **Featured Items**.

NOTE: To review requests that you previously made, go to **Access > Requests History**. To review or revoke permissions currently assigned to you, go to **Access > Permissions**.

To request permissions, select **Access > Request**.

Request Permission(s)

When you request a permission, you must specify a reason for the request. You can also specify the date that you need the permission to begin or expire.

You can request permissions in the following ways:

- Select one of the **Featured Items**. You cannot make this request on behalf of another person.

  NOTE: By default, **Helpdesk Ticket** permission appears in the **Featured Items** category. You can raise a helpdesk ticket using this permission.

- Request several permissions at once.
- Request a permission that is not among the **Featured Items**.
- Perform the request on behalf of someone else.

To request only OpenText Identity Manager permissions:

1. (Conditional) To choose a permission from **Featured Items** category, select the permission.
2. (Conditional) To choose a non-featured request or to request several permissions, complete the following steps:
   - **2a** Select **New Request**.
   - **2b** (Conditional) To request access on behalf of other individuals, select **Others**, then specify the individual(s).
   - **2c** For **Permissions**, type the name or description matching the permission.

NOTE: To raise a helpdesk ticket, search **Helpdesk Ticket** in the **Permissions** list.

2d In the displayed list, select the permission(s) that you want.

3 Specify a reason for the request.

4 (Conditional) If you are requesting a role permission, specify the **Effective Date** and **Expiration Date** for the permission.

5 (Conditional) If you are requesting a resource permission, specify the **Expiration Date** for the permission.

NOTE: You can specify the **Expiration Date** only for the resources that have enabled expiration option. Administrators can enable expiration for the resources.

6 (Conditional) If required, specify additional information related to the request:

Secondary forms

Some permissions might have secondary forms that you must complete as part of the request. For example, when requesting a laptop computer, you might need to specify the default operating system or graphics requirements.

Justification for Conflicting Roles

Your organization might have two or more roles that could create security problems when assigned to the same individual. If these types of roles exist, administrators create a separation of duties (SoD) rule to constrain users from gaining access. When a user requests one of these roles while already having a conflicting role or requests two or more conflicting roles, the identity applications respond according to the SoD policies.

Conflicting roles when User is the Recipients If you request for or assign one or more conflicting roles to a user recipients, the application displays an SoD warning. To override the SOD constraint, you must provide the reason for making an exception in the **Justification** field.

Conflicting roles when Groups and/or Containers are the Recipients If you request for or assign one or more conflicting roles to groups and/or container recipients, the application displays a warning with a list of failed roles and SoDs conflicts. A modal window is also displayed that provides you the following information:

- **Recipients:** Select the group or container from the list to view its affected users that are violating the SoD.
- **Select SoD to view details:** Select the SoD from the list to view the conflicting roles and the affected users. Selection is allowed when the request is violating more than one SoD.
- **Conflicting Role 1 and Conflicting Role 2:** Displays the roles violating the selected SoD.
- **Affected Users:** Displays a list of affected user(s) based on the selected recipients and SoD.
- **Remove:** Click to remove the selected recipient from the modal window.
- **Reset:** Click to reset the original list of conflicts displayed in the modal window.
- **Done:** Click to confirm the removal of the selected recipient from the modal window.

7 Select **Request**.

To request OpenText Identity Manager and OpenText Identity Governance permissions:

Applies only when you have enabled the **Show IG Catalog in request page** *option in the* **Configuration > Identity Governance** *page.*

1 Select **New Request**.
   - By default, the request for Self is displayed. The following tabs are displayed:

     IDM Catalogs: Lists all the available OpenText Identity Manager roles, resources, and workflows.

     IG Applications: Lists all the applications collected in the Identity Governance. You can then select the permissions associated with the selected application.

     IG Technical Roles: Lists all the technical roles of the Identity Governance. Select the IG roles that you want to request for and specify a reason for requesting the role.
   - (Conditional) To request access on behalf of other individuals, select **Others**, then specify the recipients (user, group, or team) and the permission associated with the selected recipient.
2 Click **Request** to complete the request.

The Request form displays in the Form Renderer. Based on the designed form (approval,request), and the workflow, the approver needs to login and perform the required actions in **Tasks** tab.

Find a Permission to Request

To find a role or resource that is not featured, select the icon for the magnifying glass. Then type the name or description of the permission that you want to find.

Manage Featured Items

An administrator has access to create a category and add, delete, or edit permissions in that category. To create a category, click ⚙ > ⊞ on the Requests page.

Add a Permission

1 In **New items**, click **+**.
2 Select a **Permission** from the list that you want to add in the featured items list.
3 (Conditional) You can sort permissions by **Closest match** or **Alphabetical**.
4 In **Add to Category**, select a category that you want to add a permission.

   If you do not specify the category, this item appears in the **New items** panel. Drag and drop this item on to any categories that you wish to add.
5 (Conditional) **Select image** for the specified permission, this image appears on the added permission.
6 Click **Add**.

Delete a Permission

Click **Delete** on a permission from the available categories.

Edit a Permission

Click **Edit** on a permission from the available categories.

10 Review a History of Requests

You can review a history of all requests that you have made for yourself or on behalf of others or other's requests. You can also cancel a request that has not been fulfilled.

To update the content in **Requests History**, click ↻.

NOTE: **Requests History** allows you to view the requests for access and cancel requests that are still in progress. To gain permission for a role, resource, or process, go to **Access > Request**. To revoke your access, go to **Access > Permissions**.

To view your history, select **Access > Requests History**.

Review the Details of a Request

For each request, you can view not only your actions but also the workflow involved in approving or denying your request. Each step in the process has a timestamp. Switch to list view to see the workflow and comments related to a request. You can also view the details of a request in the grid view by clicking the link in the Item Requested column.

You can specify whether the details include the following types of information:

User

Actions that actual users take. These actions might include comments that you or an administrator included with each action.

System

Actions that the application takes to complete the approval process. For example, assigning the request to an individual who can approve the request.

User and System

Actions and comments by both users and the application.

Find a Request of Self

By default, **Requests History** lists all of your requests for permissions. Change the search criteria to **Role**, **Resource**, or **Provisioning Request Definition** (process) to find a request quickly.

You can also filter the search. To filter, specify any of the following criteria:

- Item requested
- Type of request: role, resource, or process
- Request State: running, completed, or terminated
- Whether request is granted or revoked

- Confirmation number of the request
- Specific date or range of dates

Find a Request of Others

1. On the **Requests History** page, click **Others**.
2. Search users that you want to see their requests history.
3. (Optional) Change the search criteria to **Role**, **Resource**, or **Provisioning Request Definition** (process) to find a request quickly.

   You can also filter the search. To filter, specify any of the following criteria:

   - Item requested
   - Type of request: role, resource, or process
   - Request State: running, completed, or terminated
   - Whether request is granted or revoked
   - Confirmation number of the request
   - Specific date or range of dates

Raise a Helpdesk Ticket

1. Click icon for which request you want to raise a ticket.
2. Click the **Ticket** icon.
3. Specify values for all fields marked with an asterisk (*).
4. Click **Submit**.

NOTE: You can also raise a helpdesk ticket in the **Request** page. See, Chapter 9, "Request Permissions," on page 41.

Cancel a Request

You can cancel a request that has not been provisioned or is not in an error state. For example, you can cancel a request that indicates **Approval Pending**.

If a request can be canceled, the **Cancel this Request** button is active.

Customize the View

Requests History allows you to view the data in a grid view or as a list. You can sort the data by a column in the grid view. When you change the view, the application maintains that configuration whenever you log in.

To change the displayed columns:

1. Select the grid view and click ⚙.
2. Select the check box next to the desired column that you want to display. The selected columns are added simultaneously to the Request History page.
3. Click **X** on the Column Customization window to save your preferences.

V Users and their Organization Chart

The Organization Chart is a hierarchical representation of relationship between entities such as user, group, or custom entity that are defined in the Directory Abstraction Layer. Organization Chart represents the placement of that entity within an organization hierarchy. By default, the Organization Chart page shows a user entity and its placement within the organizational hierarchy based on `Manager - Employee` relationship.

An administrator defines the default relationship to display in the Organization Chart page from the Settings page. In addition to the default relationships provided with Identity Applications installation package, the administrator can create custom relationship in the Directory Abstraction Layer using Designer. For more information see *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications*.

The application enables you to perform the following activity:

- Chapter 11, "View and Manage Users," on page 51
- Chapter 12, "View and Manage the Organization Chart," on page 53

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

11 View and Manage Users

If you have an administrative role, you can view and manage the user accounts in OpenText Identity Manager. You can view users in a list or as cards. You can also search and filter **Users** to find specific individuals.

To view and manage users, select **People > Users**.

Find a User

By default, **Users** lists all users alphabetically. To find specific individuals, you have the following options:

Simple

Enter any first name, last name, email address, or telephone number.

Filtered

Enter a value on which to filter the search, then select one or more filters. For example, enter `Maria`, then select the **First Name** filter.

Advanced

Select , then specify the search criteria and values. For example, you do not remember the last name of a person but you know the first name (Maria) and department (Customer Relations).

NOTE: The identity applications return duplicate records if a multivalued attribute that has multiple values is used to filter users. For more information, contact your system administrator.

Create a User Profile

If you have an administrative role, you can create the user accounts in OpenText Identity Manager.

1. Select **+**.
2. Specify values for all fields marked with an asterisk (*).

   The password you enter might be a temporary password for the user. This depends on how the administrator configures OpenText Identity Manager. For more information, see the *OpenText™ Identity Manager CE 24.4 (v4.10) Password Management Guide*.
3. (Optional) Specify the user's work and contact information.
4. Select **Create User**.

Modify a User's Profile

You can edit a user's profile and contact information. You can also disable a user account using the **Login Disabled** toggle button. This button will appear on the Users page only when the **Login Disabled** attribute is included as a primary or secondary attribute in the **Card View** and under the **Editable Attributes** option in the **Settings** > **Customization** page.

1. In the list view, select the user whose profile you want to edit.
2. Select the edit icon.
3. Change the profile and contact information as appropriate.
4. (Optional) To disable a user account, enable the **Login Disabled** toggle button.
5. Select **Save**.

View a User's Organization Chart

1. Select a user whose organization chart you want to view.

   Based on your Users page view, you can perform this action in two ways:

   - If you are in the Card View, click .
   - If you are in the List View, click .

   The **Organization** page shows the user's placement in the organization based on the default organization chart relationship configured in the **Settings** page.
2. (Optional) To view more information about the user you selected, such as assigned roles and resources, click on the user's card.

Enabling Login for Disabled User Accounts

If you have an administrative role, you can use the Dashboard to enable login for users whose accounts have been disabled. This option will appear when a user's account has been disabled, either from the edit user page or in the OpenText Identity Console. For more information on how a user's login is disabled from edit user page in Dashboard, see "Modify a User's Profile" on page 52.

To re-enable a disabled user, go to the **Users** page and click the **Enable User Login** icon next to the user's name.

IMPORTANT: Follow these guidelines to make sure that the **Enable User Login** option functions properly:

- In Designer, add the `Login Disabled` attribute to the Directory Abstraction Layer (DAL) and ensure that the edit check box is selected before deployment.
- Go to the **Settings** > **Customization** page in Identity Applications Dashboard and add the `Login Disabled` attribute as the primary or secondary attribute in the **Card View** and under the **Editable Attributes** option.

---

12 View and Manage the Organization Chart

By default, Security Administrator and Provisioning Administrator can view the organization chart for all the users in the system. You can view your own status or search for other users.

You can navigate to the organization chart in one of the following ways:

- Go to **People** > **Organization Chart**. This page displays the organization chart of the logged-in user based on the default organization chart relationship configured in the **Settings** page. A logged-in user can also view their organization chart by clicking the icon provided on the **My Profile**, **Dashboard**, and **Applications** pages.

  To find the organization chart of other users in the system, type the name that user in the search bar.

- Go to **People** > **Users**, select any user from the list and click the icon next to their user name.

NOTE: You should have **Org Chart** access to view the **Organization Chart**. Contact your administrator to provide this access. For more information, see *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications*.

Working With the Organization Chart

In the organization chart, a user, group, or any other entity is represented in a format that resembles a business card. You can use this business card to perform the following tasks:

- "Reset the Root in the Organization Chart View" on page 53
- "Switch to the Organization Chart View" on page 54
- "Choose a Relationship to View" on page 54
- "Navigate to the Next Level in Relationship Hierarchy" on page 54
- "Send Email to Users from the Organization Chart" on page 55
- "View Detailed Information of a User" on page 56

These procedures are applicable to both user entities and custom entities.

Reset the Root in the Organization Chart View

The root is a user entity that is the starting point or orientation point in the organization chart for a relationship. To reset the root entity in your organization chart view,

1. Identify the user that you want to make as the new root.
2. Click .

   The selected user becomes the root entity of the organization chart.

Switch to the Organization Chart View

If you want to view the organization chart of a specific user in the chart view, then perform the following actions:

1. Identify the user whose organization chart you want to view.
2. Click .
3. Select the required relationship that you want to see in the organization chart view of that user.

   The organization chart displays the user's placement in the organization for the selected relationship.

Choose a Relationship to View

1. Identify the user whose relationship you want to view.
2. Click .
3. Select the required relationship that you want to view.

   The relationship is displayed inline in the existing organization chart.

If there is no object for a given relationship, the application will display a warning message. For example, let's say Sara Smith is a team manager with no direct reports assigned to her. If you want to check Sara Smith's organization chart for the Manager - Employee relationship, then you will see the following message:

```
No objects are present for Manager-Employee relationship
```

Navigate to the Next Level in Relationship Hierarchy

To navigate and expand to the next level in the relationship tree, perform the following actions:

1. Identify the user for which you want to view and navigate to the next level in the hierarchy.
2. Click .

   NOTE: Before you perform this step, ensure that you select an appropriate relationship by clicking the icon.

3. Select the user from the list.

   The organization chart of the selected user is displayed.

Send Email to Users from the Organization Chart

You can use the **Send Email** feature to send emails to individual users or to all members of a team within your organization. Additionally, you can share user information, such as email addresses, managers, direct reports, assigned roles, and resources, by including a user profile link in your email.

This section guides you how to:

- "Send User Profile Link on Email" on page 55
- "Send Email to Team" on page 55
- "Send Email to a User" on page 56

Send User Profile Link on Email

1. Identify the user whose details you want to share through email.
2. Click ✉ and select **Email Info** option. A new message template is created in your default email client. The fields in the message are auto-populated with the following text:

This part of the message	Contains
Subject	The text: `Identity information about <username>`
Body	Greetings, message, link, and sender's name. The link (URL) directs the recipient to the **Users** page that displays detailed information about the selected user. **NOTE:** Before you click on the link displayed in the email, ensure that you have appropriate access to the OpenText Identity Manager Dashboard. You must also have the required authorization to view or edit the data.

3. Specify the recipient(s) of the message. Enter any additional details, if required.
4. Click **Send**.

Send Email to Team

In an organization chart with Manager - Employee relationship, you can send email to all the team members using the **Email Team** option. This option is only available to a user who manages a team.

1. Identify the user who manages a team.
2. Click ✉ and select **Email Team** option. A new message template is created in your default email client. The **To** field automatically populates the direct reports (team members) of the manager.
3. Fill in the message content.
4. Click **Send**.

Send Email to a User

1. Identify the user to whom you want to send an email.
2. Click and select **New Email** option. A new message template is created in your default email client. The **To** field automatically populates the email address of the user you selected in Step 1.
3. Fill in the message content.
4. Click **Send**.

View Detailed Information of a User

You must have appropriate access to view the profile of a user. Contact your administrator to provide you the required access. Once you have the access:

1. Identify the user whose information you want to view.
2. Click .

   The **Users** page displays detailed information of the selected user. You might not be authorized to see some of the data or perform some of the actions on the page. Contact your administrator for assistance.

VI Groups

Groups identify users and other accounts that have common characteristics. For example, all employees in the Finance department or all senior managers.

- Chapter 13, “Manage Groups,” on page 59

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

13 Manage Groups

To view the groups to which you belong, select **People > Groups**.

TIP: Refresh **Groups** page to obtain the accurate groups count. To refresh **Groups**, click ↻.

Create a Group

1. Specify the **Name** of the group.
2. Specify the **Description** of the group.
3. Select the container where you want to create this group.

IMPORTANT:

- Do not use these < ; \ " + # / | * ~ special characters in the **Name** field.
- Do not use these | ~ special characters in the **Description** field.

Edit a Group

1. Select the group that you want to edit and click ✎.
2. (Conditional) Change the **Description** and click **Save**.
3. In **Group Members**, you can perform any of the following activities:
   - Searching for a group member by name that you want to add.
   - Adding a member to the group, click + and add the required members.
   - Deleting a member from the group, select the required members that you want to delete and click 🗑.

Delete a Group

Select the group that you want to delete and click 🗑.

You can only delete only one group at a time.

VII Teams

A **team** represents a set of users, groups, or users and groups that can perform provisioning requests and approval tasks associated with the team. Although a team might match a group that exists in the user directory, teams are not the same thing as groups. That is, a group or a member of a group cannot perform team capabilities except when assigned to a team.

Requester

Performs permission requests on behalf of other team members (the recipients). Depending on how the team is configured, a requester can act on an individual provisioning request, one or more categories of requests, or all requests.

Also manages the proxy assignments for team members.

Recipient

Member of the team on whose behalf requesters can act.

Team recipients can be users or groups within the directory. Alternatively, they can be derived through directory relationships. For example, the list of members could be derived by the manager-employee relationship within the organization. In this case, the team recipients would be all users that report to the team manager.

NOTE: The Provisioning Application Administrator can configure the directory abstraction layer to support cascading relationships so that multiple levels within an organization can be included within a team. The number of levels to include is configurable by the administrator.

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

14 View Teams

The **Teams** page lists all teams that you have permissions to view. You might be a member of all listed teams. However, you might also be an administrator with permissions to view, modify, or delete certain teams even though you are not a member.

As a team member, you might be a **requester**, able to make requests on behalf of other team members. Also, others on the team might be able to perform those actions for you, the **recipient**.

To view your teams, select **People > Teams**.

Create a New Team

If your account has administrative permissions, you can manage team functions, such as creating and deleting teams.

To create a new team, select **+**.

After you create the team, you can specify the permissions, such as resources, that might apply to team members. For more information, see Add a Team.

Modify an Existing Team

If your account has administrative permissions, you can modify an existing team, such as adding requesters and recipients, and adding permissions that might apply to team members.

To change an existing team, select the team's name. For more information, see Modify a Team.

15 Add a Team

As an administrator, you can create teams. For each team, you specify the team members (**Recipients**) who receive the team's permissions and those who can take action on recipients' behalf (**Requesters**). After you create a team, you can specify the **Permissions** (resources and provisioning request definitions) that apply to team members. For example, you can add a laptop resource that team members might be required to have.

For more information about teams, see Teams.

Create a New Team

1. On the **Teams** page, select **+**.
2. Specify a name and description for the team.
3. For **Requesters**, specify the users, groups, containers, or resources that can act on behalf of team members.
4. (Conditional) If you want the specified requesters to also be members of the team, select **Include the Requesters in the Recipients list**.

   For example, some requesters might be system administrators who need different resources from members of the team. In this case, the requesters would not necessarily be recipients. However, if the team represents a department in your organization, managers might be both requesters and recipients.
5. For **Recipients**, specify who you want to include as members of the team, according to the following categories:

   All Users

   Includes all user accounts in the directory.

   Relationship

   Includes only users who meet the specified relationship. You must also specify the type of relationship between the requester and recipient. For example, **Manager-Employee**.

   Members

   Includes only the specified users, groups, containers, or resources.
6. Select **Apply**.

Add Permissions to the Team

After you create a team, you can add and remove permissions that apply to team recipients.

- "Add Resources and Roles" on page 66
- "Add Provisioning Request Definitions" on page 67
- "Enable Requesters to Make Proxy Assignments" on page 67

Add Resources and Roles

1. While in the **Create Team** page or when modifying an existing team, select **Add Permission**.
2. Select **Add Resources** or **Add Roles**, as needed.
3. Specify the resources or roles that you want to add:

   All

   Applies only for resources

   Makes all resources available for assignment to team recipients

   Select

   Makes only the selected resources or roles available for assignment to team recipients

   Sub-containers

   Makes only the resources or roles in the specified sub-containers available for assignment to team recipients

   Exclude Roles from Selected Containers

   Applies only when you select the **Role sub-containers** *option and then select a role.*

   Makes the selected roles in the specified sub-containers unavailable for assignment to team recipients

   Exclude Resources

   Applies only for resources

   Makes the selected resources unavailable for assignment to team recipients
4. Select one or more permissions that the team requesters can request on behalf of team members:

   View

   Allows the requester to view the resource or role

   Assign

   Allows the requester to request access to the resource or role for team members

   Revoke

   Allows the requester to request that access for the resource or role be removed

   Assign role to group and container

   Applies only to roles

   Allows the requester to assign the role to the recipient's group and container in the Identity Vault

   Revoke role from group and container

   Applies only to roles

   Allows the requester to request that a role be revoked from the recipient's group and container in the Identity Vault
5. Select **Add**.

Add Provisioning Request Definitions

You might want to allow team managers to initiate PRDs on behalf of their team members. However, the team manager must have trustee rights to the PRD.

1 While in the **Create Team** page or when modifying an existing team, select **Add Permission**.

2 Select **Add Provisioning Request Definitions**.

3 Specify PRDs that you want to add:

All

Makes all PRDs available for assignment to team recipients

Select

Makes only the specified PRDs available for assignment to team recipients

Exclude

Makes the selected PRDs unavailable for assignment to team recipients

4 Select one or more permissions that you want to grant to team managers:

Initiate PRD

Requesters can start a PRD (workflow) on behalf of a team member

Retract PRD

Requesters can stop a PRD on behalf of a team member

Configure Delegate

Requesters can make a team member a delegate for other team members' provisioning requests

Manage Addressee Task

Requesters can claim a task for a team member who is a recipient or addressee (based on the task scope)

Configure Availability

Requesters can reassign a task for a team member who is a recipient or addressee (based on the task scope)

NOTE: If **Manage Addressee Task** and **Configure Availability** are disabled, the team manager cannot view or act on any active requests. Therefore, you must enable at least one of these options.

---

5 Select **Add**.

Enable Requesters to Make Proxy Assignments

You can enable the team's requesters to create proxy assignments for the team's recipients. For example, your organization might want to create teams based on functional departments and allow the department managers to make proxy assignments for their direct reports. For more information about proxy assignments, see Act as or Assign a Proxy.

1 While in the **Create Team** page or when modifying an existing team, select **Add Permission**.

2 Select **Add User Application Driver Permissions**.

3 Select **Configure Proxy**.

4 Select **Add**.

Use Case Example

Sarah Smith is manager of Customer Relations at ABC Financial. Her direct employees are Maria Belafonte and several other individuals. To better manage access requests, ABC Financial created several teams, including *Customer Relations*. On the Customer Relations team, Sarah is the requester and her direct employees are recipients. As the requester, Sarah can view and request permissions, such as laptops and mobile phones, on behalf of her employees. She cannot revoke the permissions.

Sarah also has the ability to create proxy assignments for the members of her team. By doing so, she can assign an employee to act on behalf of other, such as when one is on vacation.

In this scenario, the Customer Relations team has the following settings:

Setting	Value
Requesters	Sarah Smith
Recipients	Maria Belafonte (and other employees who report to Sarah)
Add Resources	Selected Resources: ◆ Mobile phone ◆ Laptop
Add User Application Driver Permissions	Checked
Permissions	◆ View Resource ◆ Assign Resource

NOTE: Users do not need to be a member of a team to request roles, resources, or PRDs. Teams simply make it easier to manage permissions in bulk for users and groups and to assign proxy actions.

16 Modify a Team

As an administrator, you can modify and delete teams. You can modify the following aspects of a team:

- Add Resources and Roles
- Add Provisioning Request Definitions
- Enable Requesters to Make Proxy Assignments

To modify a team, select **People > Teams** then select the team name. For more information about the variables that define a team, see Add a Team.

For more information about teams, see Teams.

VIII Delegation

You can delegate your tasks to other users in your organization. You can also delegate your tasks to multiple users based on categories when you are out of office.

The Provisioning Administrator and Provisioning Manager have the ability to define delegate assignments for any user in the organization.

To create or modify delegation, you must have one of the following roles:

- Provisioning Administrator
- Provisioning Manager
- Team Manager

To view and manage delegations, see Chapter 17, “View and Manage Delegations,” on page 73.

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

17 View and Manage Delegations

To create a delegation for a team, a Team Manager must ensure the following prerequisites are met:

1. Go to **People > Teams**.
2. Select the team from the list that you want to create delegation.
3. (Conditional) If Team Manager wants to create a delegation for self, ensure that **Include the Requesters in the Recipients list** is selected.
4. In **Add Provisioning Request Definition**, ensure that team manager has **Configure Delegate** and **Configure Availability** permissions.

List Delegations

By default, you can see all your delegations in **Self**. To see the delegations of others, select **Others**.

NOTE: The Team Manager can see delegations of other team members in the **Others** tab.

Create a Delegation

1. Select **+**.
2. (Conditional) If you are a team manager, select the team from the list.

   You can see your team members in **Delegate for**.
3. Select a user who needs a delegation from **Delegate for**.

   If you want to create a delegation for self, select your name from the list.
4. Assign delegation by performing one of the following actions:
   - To assign delegation to specific users, select **Assign delegate** and search for the users from the list.
   - To assign delegation by relationship, select **Assign by relationship** and select the relationship from the list.

     The list displays the delegation relationship that was earlier created in Designer. For more information, see *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications*.

   NOTE: The **Assign by relationship** option is disabled for Team Manager. A Team Manager can directly assign delegation to the team members.

   ---
5. Select a time period during which you will be unavailable from **Unavailable From**.

   IMPORTANT: The **Unavailable From** option is displayed only if **Set Availability while creating a Delegation Assignment** is enabled in **Settings > Customization > Navigation Items > General**. In this case, you can provide the availability details while creating the delegation. Alternatively, if

the **Set Availability while creating a Delegation Assignment** is disabled, you must specify the availability details from the **Availability Settings** page after creating the delegation assignment. This ensures that the delegation assignment functions as expected. For more information, see Chapter 18, "Specifying Your Availability," on page 77.

6 (Optional) Enable **Notify other users of these changes** and select the users to notify about this assignment.

7 Set **Effective Date**.

8 (Conditional) To set the expiry date for delegation, select **Specify Expiration** and **Expiration Date**.

Use the same fields for specifying the time period when the unavailability ends.

NOTE: By default, **No Expiration** option is selected.

9 In **Request Type Selection**, select the request type that you want to delegate.

This list displays the delegation relationship that was earlier created in Designer. For more information see *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications*.

All

Delegates all the requests of the selected user to the assigned delegate.

NOTE: This option is displayed only if the administrator has enabled **Allow All Requests** in the **Administration** page.

Attestations

Delegates the requests that are related to the user profile or attestation reports to the assigned delegate.

For example the **Attestation Report** or **Attestation User Profile**

Entitlements

Delegates the requests of the selected entitlement to the assigned delegate.

Groups

Delegates the requests of the selected groups to the assigned delegate.

Roles

Delegates the requests that are related to role assignments, resource assignments, SoD conflicts, or workflows to the assigned delegate.

For example the **Resource Assignment/Revocation Approval**, **Role Assignment/Revocation Approval**, or **SoD Conflict Approval**, **Resource Provisioning/Deprovisioning workflow**

10 Drag and drop the required request type from **Available Requests** to the **Selected Requests** list.

11 Click **Submit**.

Modify Delegations

Select the delegations from the list to modify the delegation attributes.

To delete the delegations, select the delegations from the list and click the **Delete** icon.

IX Availability

You can specify which requests with a delegate assignment you are unavailable to work on during a particular time period. During the time period when you are unavailable for a particular request, the user delegated to act on that request can work on it.

If you prefer not to specify your availability for each request definition individually, you can use the **Not Available for All Requests** from Change Status action.

Before creating availability, you need to have at least one delegate assignment to work on. You need to have your team manager (or the Provisioning Administrator) create delegate assignments for you. The Provisioning Administrator and Team Manager have the ability to define availability delegate assignments for any user in the organization.

You must have one of the following roles to create or modify availability:

- Provisioning Administrator (self or others)
- Provisioning Manager (self or others)
- Team Manager (self or others)
- End-user (self)

To create or modify availability, see Specifying Your Availability.

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

18 Specifying Your Availability

You can create or modify your own availability. To create or modify availability of others, you must be a Provisioning Administrator, Provisioning Manager, or a Team Manager.

To create availability for team members, a Team Manager must have **Configure Delegate** and **Configure Availability** permissions.

1. Go to **People > Teams**.
2. Select the team from the list that you want to create delegation.
3. In **Add Provisioning Request Definition**, ensure that team manager has **Configure Delegate** and **Configure Availability** permissions.

View Availability Status

By default, you can see your availability status in **Self**. The **Status** specifies the existing availability settings.

To see the availability status of others, select **Others**.

NOTE: The Team Manager can see availability of other team members in the **Others** tab.

Change the Availability Status

Select the existing availability settings that you want to change from **Change Status**. If you do not have any existing availability settings, the display list is empty. If no delegates have been assigned for you, a message is displayed indicating that you cannot change your status on the Availability Settings page. If you have one or more availability settings, the display list shows those settings:

Available for All Requests

This is the default status. It indicates that you are globally available. When this status is in effect, requests assigned to you are not delegated, even if you have assigned delegates.

NOTE: The **Available for All Requests** status overrides other settings. If you change the status to one of the other settings, and then change it back to this setting, any selectively available settings previously defined are removed.

Not Available for Any Requests

Specifies that you are globally unavailable for any request definitions currently in the system.

Choosing this status indicates that you are unavailable for all existing delegate assignments. It changes the current status to **Not Available for Specific Requests**. Assignments are effective immediately until the delegate assignment expires. This setting does not affect availability for new assignments created after this point.

Not Available for Specific Requests

Specifies that you are not available for certain resource request definitions. During the time period when you are unavailable for a particular request, the user delegated to act on that request can work on it.

This option takes you to the Create Availability page. It is the same action as clicking the + button.

NOTE: The end user can overwrite the availability setting specified by the Provisioning Administrator, Provisioning Manager, or the Team Manager.

Create an Availability Setting

1. Select +.
2. Specify when the time period during which you will be unavailable by typing the start date and time in **Unavailable From**, or by clicking the calendar button and selecting the date and time.
3. Specify when the time period ends by clicking one of the following options under **Unavailable Until**.
   - **No expiration:** Indicates that this unavailability setting does not expire.
   - **Specify duration:** Lets you specify the time period in weeks, days, or hours.
   - **Specify end date:** Lets you specify the end date and time. You can type the date and time, or click the calendar button and select the date and time from the calendar.

   The end date you specify must be within the time period allowed by the delegate assignment. For example, if the delegate assignment expires on October 31, 2019, you cannot specify an expiration date of November 15, 2019 for the availability setting. If you specify an expiration date of November 15, 2019, it is automatically adjusted when it is submitted to expire on October 31, 2019.
4. In **All Request Types**, select the types of requests not to accept during the time you are unavailable. This has the effect of delegating these requests to other users. This list displays the availability configuration that was earlier created in Designer. For more information see *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications*.
5. Under **Request type selection**, drag and drop the required request type from **Request(s) for selection** to the **Unavailable for the selected requests** list.
6. Click **Create**.

Edit an Availability Setting

Select the user from the list for whom you want to change the availability setting and click the **Edit Availability** icon. In the Edit Availability page that opens, specify the changes and click **Update**.

To delete an availability setting, select the availability setting from the list and click the **Delete** icon.

X Roles and Resource Administration

This application enables you to perform the following activities:

- Chapter 19, “View and Manage Roles,” on page 81
- Chapter 20, “View and Manage Resources,” on page 87

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

19 View and Manage Roles

To create and manage roles, you must have one of the following identity applications roles:

- Role Administrator
- Role Manager

List Roles

You can view roles in a list. You can also search and filter **Roles** to find specific roles.

By default, all roles are displayed on this page. If you want to change the display settings, go to **Your ID** > **Settings** > **Customization** > **General** and select the **Enable Eager Search Results in Roles and Resources Page** as required.

Find a Role

By default, **Roles** page lists all the roles alphabetically. To find the specific roles, you can use any of the following options:

Simple

Enter any role name or description.

Filtered

Specify the role name, description, category or level that you wish to filter and click **Filter**.

You can sort roles based on the columns.

Customize Columns

You can customize columns and reorder the sequence of columns.

1. Click ⚙ to customize the columns.

   On the page, you can only see the columns that are listed in the **Selected Columns** list.
2. (Conditional) Drag and drop the required columns from **Available Columns** to **Selected Columns**.

   By default, **Name** and **Description** columns are displayed.
3. Click **Apply**.

NOTE: If you want to revert your changes and keep the default columns, click **Restore defaults**.

Create a Role

1 Select +.

2 Specify the values for all the fields marked with an asterisk (*).

You can specify **Name** and **Description** for the role in different languages. See, "Change Language" on page 82.

IMPORTANT:

- Do not use these < ; \ " + # = / | * ~ ' ! @ $ % special characters in the **ID** field.
- Do not use these < ; \ " + # = / | * ~ special characters in the **Name** field.
- Do not use these | ~ special characters in the **Description** field.

---

3 (Optional) Specify the **Level**, **Subcontainer**, **Categories**, and **Owners** from the list.

NOTE: You cannot change the specified **Level** and **Subcontainer** details later. To change the display name of role levels, see "Role Settings" on page 111.

---

4 Click **Create Role**.

IMPORTANT: To delete any role from the list, select the role and click icon.

Change Language

By default, user-defined locale is selected.

1 Click **Show Languages**.

2 Specify the value for required language.

3 Click **Apply**.

Edit Roles

Select roles that you want to edit and click **Edit Roles**. You can edit roles in the following ways:

Editing Individual Roles

When you are editing an individual role, you can perform the following actions:

- Modify the role details, owners, and approvals for the selected role.
- Map resource to the selected role.
- Assign the selected role to the required users.
- Check the request status for the selected role.
- Map other roles to the selected role.

Editing Multiple Roles at once

When you are editing multiple roles at once, you can perform the following actions:

- Modify **Categories** and **Owners**, you can **Append** or **Overwrite** these values for the selected roles.
- Modify **Approval Details** for the selected roles.

Change the Approval or Revocation Process

You can modify approval or revocation process for one or more roles at the same time.

1. Select necessary roles from the list that you want to change.
2. Select one of the following options to change the approval process:

   Serial

   Specify the **Approvers** and reorder the selected reviewers to the desired approval hierarchy.

   Quorum

   Specify the **Approvers** and set the required percentage to grant access. You can also use the slide bar to set percentage. The system grants an access if the approvals match or exceed the specified percentage criteria.

   Custom

   Select the customized workflow that you want to use from the list. The list displays the workflows that are defined using Designer. For more information about workflow, see Start Workflow in *OpenText™ Identity Manager CE 24.4 (v4.10) - Using Designer to Create Policies*.
3. (Optional) If you are editing individual roles, enable **Revoke Process Required**. This applies the revocation process as same as the selected approval process.
4. (Conditional) if you are editing multiple roles at once, select one of the following options to change the revocation process.

   Retain Existing Approval Process

   Retains the default process for the selected roles.

   Same as Grant Approval

   Enables the same process that is selected for approval for the selected roles.

   None

   Disables the revocation process for the selected roles.
5. Click **Apply**.

Map Resources to the Role

You can map resources to the role in one of the following places:

- **Edit Roles:** When you select a role to edit, it displays the mapped resources for the selected role under the **Map Resources to Role** tab. You can select the required resources or entitlements from the **Available Resources and Entitlements** list.

- **Roles:** Click icon to map resources to the required roles and perform the following steps:
  1. Select the role from the roles list.
  2. Drag and drop the resources/entitlements that you want to map from the **Available Resources and Entitlements** list to **Mapped Resources**.
  3. Specify the **Mapping Description**.
  4. Click **Apply**.

Assign Role to the Users

1. Select the role from the list that you want to assign.
2. In **Role Assignments**, click **+**.
3. Specify the **Initial Request Description** that describes the purpose of this assignment.
4. Specify the **Recipients** for whom you want to assign the selected role.

   NOTE: In **Recipients**, you can mention users, group, and container from the list.

5. (Conditional) Specify the **Effective Date** and **Expiration Date**.

   If you do not set effective and expiration date, the effective date will be set to the present day and no expiry for this assignment.
6. Click **Assign Role**.

Map Role to Role

This lists the Parent Roles and Child Roles of the selected roles.

Parent Roles

Roles which are higher to the selected role. These roles have all the permissions of the selected role in addition to the permissions specified for these roles.

Child Roles

Roles which are lower to the selected role. The selected role has all the permissions of the child roles in addition to the permissions specified for the selected role.

To add a parent role for the selected role:

1. Click **+**.
2. Specify the **Initial Request Description**.
3. Select **Roles** and click **Map Parent Role**.
4. Click **Apply**.

To add a child role for the selected role:

1. Click **+**.
2. Specify the **Initial Request Description**.

3 Select **Child Roles** and click **Map Child Role**.

4 Click **Apply**.

Add Workflow to Roles

You can add a workflow to the role by using the **Add Workflow** option on the Roles page. The option is enabled by default and displayed when you select a role check box.

To add a workflow, select the check box for the desired role and click **Add Workflow.** For more information, see Adding a Workflow in the *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to the Identity Applications*.

20 View and Manage Resources

To create and manage resources, you must have one of the following identity applications roles:

- Resource Administrator
- Resource Manager

List Resources

The **Resources** page lists all the resources in Identity Applications. You can also search and filter the resources.

By default, all resources are displayed on this page. If you want to change the display settings, go to **Your ID** > **Settings** > **Customization** > **General** and select the **Enable Eager Search Results in Roles and Resources Page** as required.

Find a Resource

By default, **Resources** lists all the resources alphabetically. To find the specific resources, you can use any of the following options:

Simple

Enter the resource name or description.

Filtered

Specify the resource name, description, or category that you wish to filter and click **Filter**.

You can sort the resources based on the columns.

Customize Columns

You can customize the columns and reorder the sequence.

1. Click ⚙ to customize the columns.

   On the page, you can only see the columns that are listed in the **Selected Columns** list.
2. (Conditional) Drag and drop the required columns from **Available Columns** to **Selected Columns**.

   By default, the **Name** and **Description** columns are displayed.
3. Click **Apply**.

NOTE: If you want to revert your changes and keep the default columns, click **Restore Defaults**.

Create a Resource With Entitlement

1 Select +.

2 Select the **With Entitlement** option.

3 In **Entitlement or Driver**, select the driver or entitlement for which you want to create a resource.

4 You can choose to tag an entitlement value during the resource creation or allow the user to select the entitlement values at the time of the request.

- To tag an entitlement value to a resource, specify the necessary entitlement values for the selected driver or entitlement.

  NOTE: For every specified entitlement values, a separate resource will be created.

- To allow the users to choose entitlement values at the time of the request:

  4a Select **Map Entitlement Values at Resource Request time**.

  4b Specify **Label for Value field**.

  4c (Optional) To **Allow this resource or entitlement to be assigned multiple times with different values**, select this option.

5 Click **Create Resource**.

The **Resource Name** and **Resource Description** fields are auto-populated based on the selected driver or entitlement.

6 (Conditional) Rename the **Resource Name** field to a valid name if it is containing any of these `< ; \ " + # = / | * ~` special characters or a whitespace.

7 (Conditional) Specify the **Subcontainer**, **Categories**, and **Owners** from the list.

NOTE: You cannot change the specified **Subcontainer** details later.

8 (Conditional) If you want to set the expiration for the resource:

8a Enable **Expiration Required**.

8b Set the number of **Days**/**Months**/**Years** for which the access to the selected resource(s) should expire.

8c Click **Apply**.

Create a Resource Without Entitlement

1 Select +.

2 Select the **Without Entitlement** option.

3 Specify the values for all the fields marked with an asterisk (*).

You can specify **Name**, **ID**, and **Description** for a resource in different languages. See, "Change Language" on page 82.

IMPORTANT:

- Do not use these `< ; \ " + # = / | * ' ! @ $ %~` special characters in the **ID** field.

- Do not use these < ; \ " + # = / | * ~ special characters in the **Name** field.
- Do not use these | ~ special characters in the **Description** field.

4 (Optional) Specify the **Subcontainer**, **Categories**, and **Owners** from the list.

NOTE: You cannot change the specified **Subcontainer** details later.

5 (Conditional) If you want to set the expiration for the resource:

5a Enable **Expiration Required**.

5b Set the number of **Days**/**Months**/**Years** for which the access to the selected resource(s) should expire.

6 Click **Create Resource**.

Edit Resources

Select the resources that you want to edit and click **Edit Resources**. You can edit resources in the following ways:

Editing Individual Resources

When you are editing an individual resource, you can perform the following actions:

- Modify the resource details, owners, and approvals for the selected resource.
- Assign a resource weightage to the selected resource.
- View the entitlements of the selected resource.
- Assign the selected resource to the required users.
- Check the request status for the selected resource.
- Update the resource form for the selected resource.

Editing Multiple Resources at once

When you are editing multiple resources at once, you can perform the following actions:

- Modify **Categories** and **Owners**, you can **Append** or **Overwrite** these values for the selected resources.
- Modify **Approval Details** for the selected resources.
- Change the expiration period for the selected resources.
- Modify **Resource Weightage** for the selected resources.

Assign Weightage to the Resources

You can assign weightage to the resources with entitlement. The Role and Resource Services Driver (RRSD) uses this value to determine the order of assignment and revocation of the resource entitlement in the connected systems. This provides you the control to prioritize the assignment and revocation of entitlements.

When you create a resource with entitlement, there is no weightage associated with it. However, while editing you can assign the weightage to one or more resources at the same time.

NOTE: The **Resource Weightage** option will not be available in the Dashboard if:

- The Identity Vault schema for resource weightage attribute is not updated.
- User Application Driver package and Role and Resource Service Driver are not updated to the latest version.

---

1. Select the resource(s) from the list that you want to assign a weightage.
2. Click **Edit Resources**.
3. Under **Details, Owners, and Approvals** tab, select the required value from the **Resource Weightage** drop-down list.

   For example, if you have selected a resource with user account entitlement and want this resource to be assigned before the group entitlement, then you must assign a resource weightage value of 100 to the user account entitlement and to the group entitlement resource any value other than 100 (say 300). The user is first assigned to the user account entitlement and then to the group entitlement.
4. Click **Apply**.

Change the Approval or Revocation Process

You can modify the approval or revocation process for one or more resources at the same time.

1. Select the necessary resources from the list that you want to change.
2. (Optional) If you want the role approval to override the resource approval process, enable **Role Approval overrides Resource Approval**.

   For example, an office resource such as Printer is mapped to the Facilities Manager role, granting the Facilities Manager role also grants an access to the Printer.
3. Select one of the following options to change the approval process:

   Serial

   Specify the reviewers and reorder the selected reviewers to the desired hierarchy.

   Quorum

   Specify the reviewers and set the required percentage to grant access. You can also use the slide bar to set percentage. The system grants an access if the approvals match or exceed the specified percentage criteria.

Custom

Select the customized workflow that you want to use from the list. The list displays the workflows that are defined using Designer. For more information about workflow, see Start Workflow in the *OpenText™ Identity Manager CE 24.4 (v4.10) - Using Designer to Create Policies*.

4 Select the **Revoke Approval Process** from the list.

5 (Conditional) If you want to set expiration for the selected resource(s):

5a Enable **Expiration Required**.

5b (Conditional) If you are editing the multiple roles, select **Change** from the **Expiration** list to change the resource expiration settings.

5c Set the number of **Days**/**Months**/**Years** for which the access to the selected resource(s) should expire.

6 Click **Apply**.

Assign Resource to the Users

1 Select the resource from the list that you want to assign.

2 In **Resource Assignments**, click **+**.

3 Specify the **Initial Request Description** that describes the purpose of this assignment.

4 Select the **Recipients** from the list.

5 Click **Assign Resource**.

Resource Form

A resource form is used to gather necessary data to properly assign a resource. Create and define the fields for the resource:

1 Click **+** to add a field.

2 Change properties of the field.

3 Specify the values for all the fields marked with an asterisk(*).

NOTE: To modify the languages for the **Display Label**, see "Change Language" on page 82

4 Click **Apply**.

5 Click **Save**.

NOTE: When any user requests for this resource, added fields appear on the request form.

Add Workflow to Resource

You can add a workflow to the resource by using the **Add Workflow** option on the Resources page. The option is enabled by default and displayed when you select a resource check box.

To add a workflow, select the check box for the desired resource and click **Add Workflow.** For more information, see Adding a Workflow in the *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to the Identity Applications*.

XI Separation of Duties (SoD)

Separation of Duties (SoD) helps in resolving the conflicts that might arise when an individual is assigned or requested for two contrasting roles. For example, in the bank environment, there can be conflicts if roles such as cashier and manager are assigned to a single person. If you define SoD for these conflicting roles, you can avoid the conflicts at the time of role assignments.

- Chapter 21, “Manage SoD,” on page 95

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

21 Manage SoD

As an administrator, you can create, modify, and delete SoD.

To update the content in **Separation of Duties**, select ↻.

- "Create SoD" on page 95
- "Edit SoD" on page 95
- "Delete SoD" on page 95

Create SoD

1. Specify the values for all the fields marked with an asterisk (*), including the two conflicting roles for which you want to create a SoD constraint.

   You can specify **Name**, **ID**, and **Description** for the SoD in different languages. See, "Change Language" on page 82.

2. (Conditional) If you want an approval process for the SoD, perform the following:

   2a Enable **Approval Required** for the SoD.

   This will initiate the approval process when the conflict arises between the specified roles during assignments.

   2b (Optional) Enable **Use Default Approvers**. If the default SoD approver is not defined, you may receive an error. For more information, see "Separation of Duties Settings" on page 112.

   2c (Conditional) If you want to use different approvers other than the default approvers, select the **Approvers** from the list and reorder the sequence to define the hierarchy.

   2d Click **Create SoD**.

Edit SoD

To edit the SoD, click the SoD and edit the necessary fields and click **Apply**.

Delete SoD

Select the check box next to the SoD that you wish to delete, then click 🗑 and confirm.

XII Controlled Permission Reconciliation Services

Controlled Permission Reconciliation Services (CPRS) helps you to keep the OpenText Identity Manager Resource Catalog synchronized with the permissions of a connected application. You must have Resource Administrator role to reconcile all the permissions into the OpenText Identity Manager Resource Catalog or migrate the permissions into the Identity Vault based on the individual permissions.

- Chapter 22, “View and Manage Permission Reconciliation,” on page 99

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

22 View and Manage Permission Reconciliation

You can migrate the permissions of the managed users from the connected application to resource catalog.

To view system resources, go to **Administration > Resources**. For more information, see "View and Manage Resources" on page 87.

To configure the default behavior of Permission Reconciliation service, go to **Configuration > Permission Reconciliation**. For more information, see Chapter 26, "Enable and Configure Permission Reconciliation Service," on page 117.

Controlled permission reconciliation allows you to perform the following tasks:

- "Monitor Permission Assignment Updates" on page 99
- "Manage Permission Reconciliation" on page 100
- "Compute the Selected Driver or Entitlement Assignments" on page 100
- "Publish Assignments for the Selected Driver or Entitlement" on page 101
- "View the Process Status for the Selected Entitlement Assignments" on page 101

Monitor Permission Assignment Updates

Following options allows you to migrate permissions from the connected applications to the resource catalog:

Manage Permission Reconciliation

Click to manage permissions from the connected applications. This page displays all the configured resource details which are migrated from connected applications. For more information, see "Manage Permission Reconciliation" on page 100.

Compute selected driver/entitlement assignments

Click to compute the changes in permission assignments between Resource Catalog and connected applications on the selected driver or entitlement. The difference or changes in permission assignments between Resource catalog and connected applications is called as *Delta*. For more information, see "Compute the Selected Driver or Entitlement Assignments" on page 100.

Publish All

Click to initiate the migration from connected application to Resource Catalog. This migrates the permissions based on the settings defined in **Permission Reconciliation Settings** page. For more information, see "Publish Assignments for the Selected Driver or Entitlement" on page 101.

View the process status for the selected entitlement

Click ⓘ to view the process status of all the new permissions that are added to the entitlement on the connected application. For more information, see "View the Process Status for the Selected Entitlement Assignments" on page 101.

IMPORTANT: To publish, you must select the required driver or entitlement from **Driver or Entitlement** list.

Manage Permission Reconciliation

1. Click ⚙.

   Displays all configurations made for permission reconciliation.

2. Click ✎.
3. Select the **Entitlement** that you wish manage.
4. (Conditional) To list the resources that allow users to choose entitlement values at the time of request, select **List Resources With Dynamic Value**.

   NOTE: When MDAD driver is selected, you will need to select the **Logical system**. This option comes up only for MDAD.

   ---

5. Click **Save**.

   This configuration is saved for the selected entitlement.

Compute the Selected Driver or Entitlement Assignments

1. In **Driver or Entitlement**, select the driver or entitlement that you want to initiate delta computation.
2. (Conditional) If you select an entitlement, you can select the **CPRS Assignments** that requires computation. You can search for CPRS assignments by name or permission or you can use following filters to refine the search results:

   All Assignments

   Shows all the assignments associated with the selected entitlement.

   New Assignments

   Shows the new assignments that are made for the selected entitlement.

   Revoked Assignments

   Shows all the assignments that are revoked for the selected entitlement.

3. Click ⟳ to compute the selected driver or entitlement assignments.

Publish Assignments for the Selected Driver or Entitlement

1. In **Driver or Entitlement**, select the driver or entitlement that you want to initiate migration.
2. (Conditional) If you select an entitlement, you can select the **CPRS Assignments** that requires migration. You can search for CPRS assignments by name or permission or you can use following filters to refine the search results:

   All Assignments

   Shows all the assignments associated with the selected entitlement.

   New Assignments

   Shows the new assignments that are made for the selected entitlement.

   Revoked Assignments

   Shows all the assignments that are revoked for the selected entitlement.
3. (Conditional) To migrate only the selected assignments, click in **CPRS Assignments**.
4. Click to migrate all permissions for the selected driver or entitlement assignments.

View the Process Status for the Selected Entitlement Assignments

If you have initiated the process such as Compute or Publish for the entitlements, you can view the process status for those entitlements. To view the process status, perform the following steps:

1. In **Driver or Entitlement**, select the entitlement for which you want to see the process status.
2. (Conditional) Select the required **CPRS Assignments** to see their process status. You can search for the CPRS assignments by name or permission or you can use the following filters to refine the search results:

   All Assignments

   Displays all the assignments associated with the selected entitlement.

   New Assignments

   Displays the new assignments that are made for the selected entitlement.

   Revoked Assignments

   Displays all the assignments that are revoked for the selected entitlement.
3. Click to view the process status of the selected entitlement assignments.

   The **PROCESS STATUS** page lists the following columns:

   Process Type

   Specifies the type of processes that are initiated for the entitlement such as Compute or Publish.

   Start Time

   Specifies the start time of the process.

   Completion Time

   Specifies the completion time of the process.

Status

Specifies the status of the process. For example, Submitted, Completed, or In Progress.

4 (Conditional) Click to refresh the **PROCESS STATUS** information.

XIII Monitoring Workflows

Once the Workflow Engine initiates the workflows, you can track their progress on the Workflow Monitoring page. Here, you can check the current status of the workflow, reassign activities within the workflow, terminate a workflow process, and even view the comments logged during their execution.

To monitor and manage workflows, see Monitor and Manage Workflows.

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

23 Monitor and Manage Workflows

You must have one of the following identity applications roles to monitor workflows:

- Security Administrator
- Provisioning Administrator

Search for Workflows

You can use any of the following search criteria to find a workflow process:

Simple Search

Enter the name of the recipient or requester in the search bar.

Filtered Search

Click and use one of the following options:

- Name of the requester who initiated the workflow process.
- Name of the recipient.
- Status of the workflow process.
- Status of the approval activity.
- Requested date. To filter by request date, enter a date and time, then choose whether you want to filter before or after the specified date.

Sort Workflows

Workflow processes, by default, are sorted by **Request Date**, with the most recently requested process at the top of the list.

You can also sort the list alphabetically by the requester or recipient name. To sort, click next to that column. You can then shuffle the list in ascending or descending order as desired.

Click to get an up-to-date workflow process list from the workflow runtime database.

Customize Columns

1. Click .
2. Select the check box next to the column that you want to display.

   TIP: To choose all columns, select the check box provided near the search field.

3. Click the close sign (x) on the **Column Customization** window.

Next time when you navigate to the page, columns that are configured to display will be shown.

View Workflow Status

At any given time, a workflow process will display one of the following statuses in the **Status** column:

Running

Indicates that a workflow process is in progress. One or more approval request activities are waiting for an action from the approver.

Completed

Indicates that a workflow process is complete. You can view the approval status in the **Approval Status** column. For more information on different states of approval, see View Approval Status.

Stopped

Applies to a non-clustered Workflow Engine environment.

Indicates that an instance of the workflow engine is currently down and not reachable.

Terminated

Indicates that a workflow process was terminated before completion.

View Approval Status

The **Approval Status** column displays the current approval status of a workflow process.

At any given time, a workflow process will display one of the following statuses:

Processing

Indicates that one or more workflow activities are awaiting approval from the approver. For example, two approval activities are defined in a workflow process, one is approved, and the other is pending approval. Because the workflow process is still in progress in this case, so the approval status is displayed as `Processing`.

Approved

Indicates that all approval activities in the workflow process are complete.

Denied

Indicates that the approver rejected one or more approval activities in the workflow process.

Retracted

Indicates that the requester retracted the permission access request. In this case, the workflow process is terminated before its completion.

Error

Indicates that one or more approval activities in the workflow process are not working properly. In this case, the workflow process is terminated before its completion. The errors can occur due to many reasons, some of them are listed below:

- An error occurred when calling the token end point

- An error occurred while initializing the scripting engine or the scripting context
- When forwarding a task, the Activity ID or Addressee details are missing or empty

Advanced Operations Available On This Page

Dashboard provides the following operations for managing workflow processes:

- Terminate a Workflow Process
- Reassign a Workflow Process
- View Comments to Know More About Workflows

Terminate a Workflow Process

1 Select the check box next to the name of the workflow process you want to terminate. When a workflow process is terminated or completed, the check box is automatically disabled.

TIP: You can select more than one check box to terminate multiple workflow processes.

---

2 Click ⊘.

3 Specify a reason for terminating the workflow processes.

4 Click **Terminate**.

Reassign a Workflow Process

1 Identify a workflow process you want to reassign, then click .

2 To reassign a workflow activity, select the check box next to it.

NOTE:

- Only one workflow process can be reassigned at a time. If a workflow process has more than one activity, you can either select all activities or just the ones you want to reassign.
- Check the status of any activity in the Status column before re-assigning it. For more information on different status types and their description, see View Approval Status.

---

3 In the **Reassign To** drop-down menu, select the addressee to whom you want to reassign the task.

4 Specify a reason for the reassignment in the **Comment** text box.

5 Click **Reassign**.

View Comments to Know More About Workflows

While a workflow process is running, the workflow engine logs key events as comments. You can read these comments by selecting from the **Actions** tab.

To view both system and user comments, select the **View System Comments** check box. By default, the application only displays user comments.

XIV Configuration

This page allows you to configure the default operations of identity applications components. The settings and configurations made on this page affect while performing any operations on the components that are listed on this page.

You can configure the default settings of the following components:

- Chapter 24, “View and Configure Roles and Resources Settings,” on page 111
- Chapter 25, “View and Configure Delegation and Proxy Settings,” on page 115
- Chapter 26, “Enable and Configure Permission Reconciliation Service,” on page 117
- Chapter 27, “View and Configure Log Events,” on page 119
- Chapter 28, “View and Manage Cache Events,” on page 121
- Chapter 29, “Assign Administrators in Identity Applications,” on page 125
- Chapter 30, “View and Configure the Workflow Engine and Cluster Settings,” on page 129
- Chapter 31, “View User Application Driver Status,” on page 133
- Chapter 32, “View and Configure the Default Provisioning Display Settings,” on page 135
- Chapter 33, “Configure Identity Governance Settings,” on page 137

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

24 View and Configure Roles and Resources Settings

This page defines the basic configurations of the Roles and Resources subsystem. You can modify some settings from the following list, whereas few settings provide an information that are set during installation and cannot be modified:

- "Role Settings" on page 111
- "Resource Settings" on page 112
- "Entitlement Query Settings" on page 112
- "Separation of Duties Settings" on page 112

Role Settings

These settings control the behavior of the role management components of identity applications. The **Role Container**, **Role Request Container**, and **Default Role Approval Definition** show the LDAP settings that are saved in the Identity Vault during installation.

Role Container

The container where all the roles are stored.

Role Request Container

The container where all the role provisioning requests are stored.

Default Role Approval Definition

This determines the default workflow used for role assignment or revocation process.

Role Assignment Grace Period

Specifies the grace period in minutes which determines the time difference between removing the role assignment and dissociating entitlements from the role.

Enable Role Approval

Enable the respective options in this setting to trigger an approval process before a role is assigned to groups, containers, or mapped to another role. The approval process will be triggered only if the approval is configured for that role. When this setting is disabled, the role will be assigned to the recipients directly, without seeking approval. The approver(s) will not receive an email notification, although the email approval setting is set as enable.

By default, the **Enable Role Approval** is disabled for **Role to Role**, whereas it is enabled for **Role to Container** and **Role to Group** options.

Role Level Display Names

You can change the display names of Role Levels for all supported languages. To change the language, see "Change Language" on page 82.

Click **Apply** to save your changes.

Resource Settings

These settings control the behavior of the resource management components of identity applications. You can only view the resource settings that are stored in Identity Vault.

Resource Container

The container where all the resources are stored.

Resource Request Container

The container where all the resource provisioning requests are stored.

Default Resource Approval Definition

The container where all the workflows related to resource approval process is stored. When you select Custom approval process for any resource, it populates the workflow options from this container.

Entitlement Query Settings

The identity applications periodically make queries to entitlements from connected systems that are displayed in the **Administration > Resources** list.

Default Query Timeout

Specifies the interval in minutes that system should wait for the query result.

Default Refresh Rate

Specifies the interval in minutes to refresh entitlement queries in the system.

Refresh Status

Indicates whether the entitlement values have been refreshed.

You can refresh **All Drivers** at a time or select specific driver or entitlements that you want to refresh. To refresh the entitlement values manually, click ↻.

Click **Apply** to save your changes.

Separation of Duties Settings

You can control the behavior of the separation of duties used in identity applications.

SoD Container

The container where all the SoD constraints are stored.

SoD Approval Definition

To allow permissions for users despite SoD constraints require an approval. This determines the workflow that is used for custom approvals. You can set the approval definition for the custom approval process.

This list displays the SoD approval definitions created using Designer. For more information, see *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications*.

Default Approval Type

This determines the default approval type for SoD constraints when the approval process is enabled for those SoD constraints.

Default SoD Approvers

This determines the default users, groups, roles, or containers who review SoD constraints and approve those requests as required.

Click **Apply** to save your changes.

25 View and Configure Delegation and Proxy Settings

View and Configure Delegation Settings

Delegation allows you to modify the default delegation settings, you must have one of the following roles:

- Provisioning Administrator
- Provisioning Manager

IMPORTANT: An assigned proxy can always see all your requests. This option does not apply to the proxy.

---

1. (Optional) Enable **Allow All Requests**.

   This provides the **All** option in **Request Type Selection** while creating delegation.
2. Specify the retention time (minutes) for the delegation assignments in the system after they expire.
3. Specify the retention time (minutes) for the availability settings in the system after they expire.
4. Select the **Delegation notification template** from the list.

   This list displays the delegation templates created using Designer. For more information, see *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications*.
5. Select the **Availability notification template** from the list.

   This list displays the availability templates created using Designer. For more information, see *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications*.
6. Click **Apply**.

View and Configure Proxy Settings

Proxy allows you to modify the retention time and set the notification template for proxy assignments.

Retention time for Proxy assignments

Specify the retention time (minutes) for the proxy assignments in the system after they expire.

Proxy notification template

Select the proxy template from the list. This list displays the proxy templates that are created using Designer. For more information, see *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications*.

Click **Apply** to save your changes.

View and Configure Synchronization and Cleanup Service

Synchronization and Cleanup Service allows you to define the interval for these services.

Synchronization Service Activation Interval

Specify the interval that synchronizes the delegation, proxy, and available settings.

Cleanup Service Activation Interval

This option allows you to clean up the expired assignments which have passed the retention time. You can set the cleanup service using one of the following methods:

- **Minutes:** This option removes the expired assignments that occur for every specified interval.
- **Date:** This option removes the expired assignments that occur within the every specified date.

Click **Apply** to save your changes.

NOTE: These changes will take effect next time you start the Identity Applications.

---

26 Enable and Configure Permission Reconciliation Service

Enabling Permission Reconciliation Service helps you to create custom entitlements for connected system roles or resources in order to synchronize the connected application's permission assignment changes to the OpenText Identity Manager resource catalog.

You must have Resource Administrator role to configure **Permission Reconciliation** settings.

To view system resources, go to **Administration > Resources**. For more information, see "View and Manage Resources" on page 87.

To add or modify the permission reconciliation settings of connected applications, go to **Administration > Permission Reconciliation**. For more information, see Part XII, "Controlled Permission Reconciliation Services," on page 97.

By default, the **Permission Reconciliation** option is enabled.

Following options control the information synchronization and its retention period between connected applications and OpenText Identity Manager resource catalog:

Polling time for status checker

Specifies the time interval in minutes to check the permission reconciliation status. This polls the status of requests that are under process for the specified period and updates the system.

By default, this interval is set to 60 minutes.

Retention time for computed permission assignments

Specifies the period in days to retain permission assignments that are reconciled.

By default, this period is set to 7 days.

Click **Submit** to apply the configured settings.

27 View and Configure Log Events

Logging allows you to debug the identity applications configuration. The logging service provides facilities for writing, viewing, filtering, and listening of log messages.

By default, OpenText Identity Manager saves the logging configuration in `idmuserapp_logging.xml` file that is located in the following location:

`/opt/netiq/idm/apps/tomcat/conf/`

Change Auditing Service Settings

Auditing Configuration allows you to enable or disable CEF format.

Enable CEF format

This option allows you to log the events in CEF format. You should also specify the following auditing server details to use CEF format:

Fields	Description
Destination host	Specifies the destination hostname or IP address of the auditing server.
Destination port	Specifies the destination port number of the auditing server.
Network protocol	Specifies the protocol that should be used to establish communication with the auditing server. To establish a secure communication with the auditing server, select TCP protocol and enable Use TLS option. Provide the Keystore file name and the Keystore password.
Intermediate event store directory	Specifies the temporary directory where the events can be are stored. This directory serves as a backup for an auditing server.

Add an OpenText Identity Manager Package

Each feature in identity applications uses one or more packages. Each package handles a specific area of a feature and has its own independent log level that obtains event messages from different parts of the application.

The package names are based on log4j conventions. The event messages include these package names indicating the context of the message output. The logs include tags and values that allow the administrator to identify and correlate which package log entries pertaining to a given transaction and user.

To add a package:

1. In Logging Configuration, click +.

2 Search for the package name that you want to add.

3 Select the package from the list.

4 (Conditional) Select the **Log level** for the package. See, "Change the Log Levels for OpenText Identity Manager Packages" on page 120

5 Click **Add**.

Change the Log Levels for OpenText Identity Manager Packages

The logs contain information about processing and interactions among identity applications components that occur while fulfilling users and administrative requests and during general system processing. By enabling the correct log levels for various packages, an administrator can monitor how identity applications process users and administrative requests.

You can change the log level of the packages individually by searching a package name. If you want to change the log level for all the packages:

1 Select **Change log level for the listed packages**.

2 Select the log level from the list.

Table 27-1 *Types of Log Levels*

Level	Description
Fatal	The least detail. Writes fatal errors to the log.
Error	Writes errors that can cause system processing to not proceed.
Warn	Logs potential failures, but the impact on execution is minimal. Warnings indicate that you should be aware that this event is happening and might want to make a configuration change to avoid it.
Info	Logs informational messages. No execution or data impact occurred.
Debug	Includes debugging information.
Trace	The most detail. Writes tracing information (plus all of the above) to the log.

NOTE: By default, the log level is set to **Info** for all the packages.

3 (Conditional) To retain these changes after restarting the application server, select **Persist the logging changes**.

4 Click **Apply**.

NOTE: The portal functionality and export or import of portal content within the User Application are discontinued from this release. If you have the packages corresponding to these features, manually remove the packages from the `idmuserapp_logging.xml` file.

28 View and Manage Cache Events

Caching allows you to manage various caches maintained by Identity Applications. These caches store the reusable data temporarily on the application server to optimize the system performance.

This page displays the cache settings (latest to your application restart). You can manage the cache collection mechanism by changing their configuration settings. You can also flush the cache contents, if necessary.

There are two levels of settings available to control the cache collection on your application server:

- **Global Settings:** Global settings are stored in a central location (the Identity Vault) so that multiple application servers can use the same setting values. For example, If you have a cluster of application servers, the cluster configuration values use the global settings.
- **Local Settings:** Local settings are stored separately on each application server so that an individual server can override the value of one or more global settings. For example, you might want to specify a local setting to remove an application server from the cluster specified in the global settings, or to reassign a server to a different cluster.

The global settings are the default values for every application server that uses a particular instance of User Application driver. Altering the global settings values affects every server unless it specifies local settings to override the global settings.

Flushing Caches

1. In **Flush Cache**, select the type of cache from the list that you want to flush.
2. Click **Flush Cache**.

View and Manage Cache Settings

Following cache settings apply to both clustered and non-clustered application servers. For more information, see How these cache settings work.

NOTE: The changes to the cache configuration will take effect after application restart.

Basic Cache Settings

Settings	What to do
Lock Acquisition Timeout	Specify the time interval (in milliseconds) that the cache waits for a lock to be acquired on an object. You might want to increase this setting if the Identity Applications imposes a lot of lock timeout exceptions in the application log. The default value is 15000 ms.
Wake Up Interval	Specify the time interval (in seconds) that the cache eviction policy waits before invoking the following activities: ◆ Processes the evicted node events. ◆ Cleanup the size limit and expired nodes.
Eviction Policy Class	Specify the classname for the cache eviction policy that you want to use. The default is the LRU eviction policy that JBoss Cache provides: `org.jboss.cache.eviction.LRUPolicy` If appropriate, you can change this to another eviction policy that JBoss Cache supports.

TIP: In Local Settings, select Enable Local for the required settings to override the global settings and specify the values.

Non Customizable Cache Settings

Settings	What to do
Max Nodes	Specify the maximum number of nodes allowed in the cache. If you don't want restrict the number of nodes, specify `0`.
Time To Live Seconds	Specify the time to idle (in seconds) before the node is swept away. If you don't want restrict the Time To Live Seconds, specify `0`.

TIP: In Local Settings, select Enable Local for the required settings to override the global settings and specify the values.

Click Save to save your configuration values.

Customizable Cache Settings

This allows you to customize certain cache holders in identity applications. To modify the cache holders:

1. Click the Cache Holder ID that you want to modify.
2. (Conditional) Change the required values such as Max Nodes, Time To Live Seconds, and Max Age.

NOTE: The system clears the events in the cache according to the value specified for **Max Age**.

3 (Conditional) In **Local Settings**, select **Enable Local** for the required settings to override the global settings and specify the values.

4 Click **Save**.

View and Manage Cluster Cache Configuration

Specify the following settings in Cluster Configuration that helps in caching across the cluster:

Setting	What to do
Permission Index Cluster Enabled	Enable this option if you want to update the permission index changes to the other nodes in the cluster for the specified **Permission Index Group ID**.
Permission Index Group Id	Specify the Permission Index Group ID of the JGroups cluster in which you want to participate. There is no need to change the default Group ID that is provided for the User Application's cluster unless you want to use a different cluster.
Permission Index Cluster Properties	Specify the JGroups protocol stack for the cluster specified by Permission Index Group ID. This setting is to adjust the cluster properties.
Cluster Enabled	Enable this option if you want to overwrite the cache changes to the other nodes in the cluster for the specified **Group ID**.
Group ID	Specify the Group ID of the JGroups cluster in which you want to participate. There's no need to change the default Group ID that's provided for the User Application's cluster unless you want to use a different cluster. The Group ID must be unique and must not match any of the known JBoss cluster names such as `DefaultPartition` and `Tomcat-Cluster`. **TIP:** To see the Group ID in logging messages, make sure that the level of the caching log (`com.sssw.fw.cachemgr`) is set to Info or higher.
Cluster Properties	Specify the JGroups protocol stack for the cluster specified by Group ID. This setting is to adjust the cluster properties.

TIP: In **Local Settings**, select **Enable Local** for the required settings to override the global settings and specify the values.

29 Assign Administrators in Identity Applications

An administrator assignment specifies a domain type (Provisioning, Role, Resource, and Security), as well as a set of permissions for the assignment.

To assign administrative roles, you must either be a Security Administrator or have a Domain Administrator-type of role, such as Provisioning Administrator.

NOTE: The delegated administrators of a domain have no access to this page.

The permissions for an administrator assignment define the actions that administrators can take on a particular scope of object instances within the domain type selected. For example, if you select the Role domain as the domain type for an assignment, the permissions determine what actions the administrators can take on the set of role instances selected as the scope for the assignment. These permissions might specify, for the selected scope of roles, that administrators can perform actions such as assigning roles to users, viewing role assignments, and deleting on role assignments.

Listing the Administrator Assignments

Administrator Assignments displays the existing administrator assignments in the system.

- "Find an Administrator Assignment" on page 125
- "Customize Columns" on page 126

Find an Administrator Assignment

You can search for administrator assignments by specifying the username. You can also filter the assignments in one of the following categories:

All

Displays all administrator assignments in the system.

User

Displays the administrator assignment made to the users in the system.

Group

Displays the administrator assignments made to the groups in the system.

Container

Displays the administrator assignments made to the containers in the system.

Role

Displays the administrator assignments made to the roles in the system.

Customize Columns

You can customize columns and reorder the sequence of columns.

1 Click ⚙ to customize the columns.

   On the page, you can only see the columns that are listed in the **Selected Columns** list.

2 (Conditional) Drag and drop the required columns from **Available Columns** to **Selected Columns**.

   By default, **Domain** and **Assignee** columns are displayed.

3 Click **Apply**.

NOTE: If you want to revert your changes and keep the default columns, click **Restore Defaults**.

Create a New Administrator Assignment

You can create an administrator assignment for a user, group, container, or role type. Perform the following steps to create a new administrator assignment:

1 Click +.

2 Specify the **Initial Request Description** that describes the purpose of this assignment.

3 Select the **Domain Type** from the list.

Domain	Description
Provisioning	This domain defines the rights to launch and retract process requests, manage addressee tasks, and configure delegate, proxy, and availability settings.
Role	This domain defines the rights to manage roles and SoDs, assign, revoke, and report on roles, as well as rights to configure role settings.
Resource	This domain defines the rights to manage resources, assign, revoke, and report on resources, as well as rights to configure resource settings and bind entitlements.
Security	This domain defines the rights to manage Identity Applications security, such as assign and revoke domain administrators and managers. This also provides the right to configure teams.

4 Select the **Assignment Type** for which you want to create an assignment.

   This displays the list of users, groups, container, or roles based on the selected assignment type.

5 Select the required user, group, container or a role on from the provided list to create an assignment.

6 (Conditional) Specify the **Effective Date** for this assignment. If you do not specify any date, creates an assignment immediately.

7 (Conditional) Specify the **Expiration Date** for this assignment. If you do not specify any date, the expiration date is set to never.

8 (Conditional) To create a domain administrator assignment for the selected domain, enable **All Permissions**.

NOTE: This option cannot be edited after creating the assignment. For a delegated administrator, you can assign permissions individually. See, "Assign Permissions to a Delegated Administrator" on page 127.

If this option is disabled, a delegated administrator is created for the selected domain.

9 Click **Create**.

Assign Permissions to a Delegated Administrator

A delegated administrator has the ability to perform selected operations for a subset of authorized objects within the domain for all users. For more information about different types of users, see Types of User Categories in Identity Applications in the *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to the Identity Applications*.

1 Select the administrator assignment for which you want to assign permissions.

2 In Permissions, click +.

3 Click **Add Permissions**.

Displays the permissions based on the domain type of the selected assignment.

For example: If the selected assignment belongs to **Roles** domain, you can add role permissions, SoD permissions, or role configuration permissions.

TIP: Click ⓘ to see the permissions that belong to the specified domain.

The assigned permissions are listed under **Permissions**.

To delete the assigned permissions,

1 Select the permissions that you want to delete.

2 Click 🗑.

Delete an Administrator Assignment

1 In **Administrator Assignments**, select the check box of the administrator assignment that you want to delete.

You can select multiple check boxes to delete multiple assignments.

2 Click 🗑.

30 View and Configure the Workflow Engine and Cluster Settings

This page helps in configuring the Workflow Engine and configuring cluster settings. These settings apply to all engines in the cluster. When any of these settings are changed, other engines in the cluster will detect these changes in the database and use the latest values. The engines check for changes to these settings at the same rate as specified by the **Pending Process Interval**.

Configure the Workflow Engine Settings

The following are the engine settings that you might require to configure for your workflow engine settings:

Engine Setting	Description
Enable Email Notification	Enables or disables email notifications for the entire workflow engine. Defaults to enabled.
Web Service Activity Timeout (minute)	Specifies the default Web Service activity timeout in minutes. The default is 50 minutes.
User Activity Timeout (hour, 0 for no timeout)	Specifies the default user activity timeout. The default is 0 days, which indicates no timeout.
Completed Process Timeout (day)	Specifies the number of days that a completed process state is kept in the workflow database system. The default is 120 days.
Completed Process Cleanup Interval (hour)	Specifies how often the engine checks for and removes completed processes that have been in the workflow database system for longer than the completed process timeout. The default is 12 hours.
Pending Process Interval (second)	User activities that are executed on an engine which the process is not bound to are put into a pending state. This interval specifies how often to check for pending activities in order to continue their execution. The default is 30 seconds.
Retry Queue Interval (minute)	Activities that fail because of suspected database connectivity issues are put on a retry queue. This interval specifies how often the engine attempts to retry these activities. The default is 15 minutes.
Thread Keep Alive Time (second)	If the pool is larger than the minimum size, excess threads that have been idle for more than the keep-alive time will be destroyed. The default is 5 minutes.

Engine Setting	Description
Maximum Engine Shutdown Timeout (minute)	The engine attempts to shutdown gracefully. When shutting down it stops queuing new activities for execution and attempts to complete any activities already queued. This timeout specifies the maximum time that the engine waits for all queued activities and threads executing activities to complete. If this time is exceeded, the engine halts processing of queued activities and attempts to stop all threads executing activities. The default is `1` minute.
Maximum Thread Pool Size	The maximum number of threads that the engine uses to execute activities. The default is `20`.
Minimum Thread Pool Size	The minimum number of threads that the engine uses to execute activities. When a thread is requested and fewer than the minimum are in the pool, a new thread will be created even if there are idle threads in the pool. The default is `10`.
Initial Thread Pool Size	Number of pre-started threads in the pool when it is created. The default is `5`.
Process Cache Load Factor	The load factor specifies how full the cache is allowed to get before increasing its capacity. If the number of entries in the cache exceeds the product of the load factor multiplied by the current capacity, then the capacity is increased. The default is `0.75`.
Process Cache Initial Capacity	The process cache is backed by a hash map. The capacity is the number of buckets in the hash map. The initial capacity is the number of buckets at the time the cache is created. The default is `700`.
Process Cache Maximum Capacity	Before adding a process to the cache, if the number of processes in the cache equals or exceeds the Process Cache Maximum Capacity, the cache attempts to remove the oldest inactive process from the cache. The maximum capacity is a soft limit, so the number of processes in the cache might exceed the Process Cache Maximum Capacity if there are no inactive processes (only active processes) in the cache. The default is `500`.

Configure Workflow Cluster Settings

Following are the settings that you might require to configure for your workflow cluster settings:

Cluster Setting	Description
Heartbeat Interval	Specifies the interval at which the workflow engine's heartbeat is updated. When the workflow engine starts up, it detects if its engine ID is already being used by another node in the cluster and refuses to start if the ID is in use. The User Application database maintains a list of engine IDs and engine states. If an engine crashes and is restarted, its last state in the database indicates that it is still running. The workflow engine therefore uses a heartbeat timer, which writes heartbeats at the specified interval, to determine if an engine with its ID is still running in the cluster. If it's already running, it refuses to start. The minimum value for the heartbeat interval is 60 seconds.
Heartbeat Factor	Specifies the factor that is multiplied with the heartbeat interval to arrive at the heartbeat timeout. The timeout is the maximum elapsed time permitted between heartbeats before an engine will be considered timed out. The minimum value for the heartbeat factor is 2.

View the Workflow Engines State

The workflow engine checks the cluster database to see if the status of the engine is **SHUTDOWN** or **TIMEDOUT**. If the status is **STARTING** or **RUNNING**, the workflow engine logs a warning, then waits for a heartbeat timeout to occur. **Workflow Engines State** displays the state of the workflow engines in the cluster:

SHUTDOWN

Indicates that the engine is shutdown gracefully.

TIMEDOUT

Indicates that accessing the engine is timed-out. This state depends on the specified Heartbeat Interval. See, "Configure Workflow Cluster Settings" on page 130.

STARTING

Indicates that the engine is starting.

RUNNING

Indicates that the engine is active.

31 View User Application Driver Status

Driver Status page displays the following details of User Application Driver:

Driver Name

Displays the name of the driver in LDAP format. For example:

```
cn=User Application Driver,cn=driverset1,o=system
```

Driver Version

Displays the driver version used in OpenText Identity Manager.

Application Revision

Displays the revised version of Identity Applications.

Patch Level

Displays the patch applied for the driver.

Build Revision

Displays the updated build version.

Status

Displays the driver state.

32 View and Configure the Default Provisioning Display Settings

The **Provisioning Display Settings** page controls the behavior of general search results of Identity Applications objects such as **Users**, **Permissions**, **Tasks**, **Roles**, **Resources**, **Separation of Duties**, and more. You can also modify the appearance of **Tasks** and **Request History** page.

View and Manage General Display Settings

These settings apply for the search results showing on the accessed Identity Applications pages.

Default number of results displayed per page

Specifies the number of results should be displayed on the page.

Options for number of results displayed per page

Specifies the options to modify the number of results that are showing on the page.

Choose the default option as sort by in new request page

Specifies how the permissions are sorted on the New Request page.

View and Manage the Appearance of Tasks Page

Field	Description
Select Column to set default sort	By default, the task results in the **Tasks** page are sorted by **Assigned To**. You can select a different column from the list to sort the task results. Also, you can sort the results by ascending or descending order. Use **Sort by Descending Order** to sort the results in descending order. Disabling this option displays the results in ascending order.
Allow user to customize columns	By default, this option is enabled. Disabling this option restricts the user from customizing columns in the **Tasks** page. ◆ **Available columns:** Displays the columns which are disabled for user customization. ◆ **User default columns:** Displays the columns that are already showing on the **Tasks** page. ◆ **Available columns for User customization:** Displays the columns that can be customized by users.

Field	Description
Allow user to customize task detail open	By default, this option is enabled. This option allows you to change the preferences of opening the approval form in the Tasks page. Go to Tasks page and click ⚙ to change the preferences. Disabling this option will restrict the system users from changing the preferences of opening the approval form in the Tasks page. However, you can change this preferences in the Settings > Customization page.

Click Save to apply your changes.

View and Manage the Appearance of Request History Page

Field	Description
Select Column to set default sort	By default, the request statuses in the Request History page are sorted by Request Date. You can select a different column from the list to sort the results. Also, you can sort the results by ascending or descending order. Use Sort by Descending Order to sort the results in descending order. Disabling this option displays the results in ascending order.
Allow user to customize columns	By default, this option is enabled. Disabling this option restricts the user from customizing columns in the Request History page. ◆ **Available columns:** Displays the columns which are disabled for user customization. ◆ **User default columns:** Displays the columns that are already showing on the Request History page. ◆ **Available columns for User customization:** Displays the columns that can be customized by users.

Click Save to apply your changes.

33 Configure Identity Governance Settings

This page allows you to configure the Identity Governance settings:

Application URL

Displays the Identity Governance URL.

Administrator Username

Displays the username of the administrator.

Administrator Password

Specifies the administrator password.

Show IG Approvals in tasks page

Enable this option to display the **Identity Governance Approvals** in the **Tasks** page.

Show IG Catalog in request page

Enable this option to display the **Identity Governance Catalog** in the **Access > Request** page.

NOTE: Identity Governance must collect all the OpenText Identity Manager roles and resources. Else, only the Identity Governance permissions will be displayed in the **Request** page.

Click **Apply** to save the changes.

XV Client Customization

If you have administrator privileges, this application enables you to perform the following activities:

- Chapter 34, “Customize the User Interface,” on page 141

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

34 Customize the User Interface

If you have an administrative role, you can establish the brand, accessibility, and visibility settings for each client that connects to the identity applications.

Select *Your ID* > **Settings**, then select the **client** that you want to manage.

- "Manage Clients" on page 141
- "Control User Access" on page 141
- "Customize the Views" on page 143
- "Customize the Branding" on page 146
- "Client Helpdesk Settings" on page 147
- "Manage Dashboard Widgets" on page 147

Manage Clients

To manage client names and attributes, select the client, then **General**.

You can modify the name and LDAP attribute match for each client that connects to `idmdash`. You can also create a new client and delete any client except the default client.

LDAP Filter to match represents the user root container that stores the account(s) for the User Application Administrator role. This setting enables the administrator to log in simply by username (instead of requiring the fully distinguished name each time). The User Application Administrator account does not need special directory rights because this role controls application-level access.

Control User Access

Access settings allow you to specify which user accounts are **trustees** for the different Identity Applications pages within the client. When a trustee logs in, the application displays the page that has been provisioned. Otherwise, the page remains hidden to the logged in user. You can add users, groups, roles, and containers as trustees.

- "Considerations for Configuring User Access" on page 141
- "Configuring User Access" on page 142

To control user access, select the client, then **Access**.

Considerations for Configuring User Access

When configuring user access, you should consider the following conditions:

- Make sure that the users specified in **Trustees** are having sufficient Identity Vault rights to perform tasks within the Identity Applications. However, the trustees can access the page but operations on the page will fail if they do not have the proper Identity Vault rights.

- Each **Navigation Item** has a set of default trustees suitable for the services that can be accessed through that page. However, if you remove all trustees for a navigation item, every user will be able to access that page.
- If a user does not have access to the default navigation (or to the default menu item within a navigation area), the application redirects the user to the **Dashboard** page. The application might also display an error message, such as when a user attempts to login to page without proper authorization. The user can log in but will be directed to the **Dashboard** page.
- When a user is in **proxy** mode, the application provides access according to the permissions for the account being proxied, as opposed to the permissions for the logged in user. The proxy can perform tasks on behalf of the other user but does not assume any of the role-type permissions. For example, a user cannot perform Domain Administrator functions on behalf of a Domain Administrator unless that user also has that role.

Configuring User Access

Before configuring user access, review "Considerations for Configuring User Access" on page 141.

1. Expand the required **Page** item that you want to provision access to the users, groups, roles, or containers.

   Navigation Items are listed based on the look and accessibility of the page in Identity Applications user interface.

2. Specify one or more trustees for the selected **Page** item.

   For example, roles such as Helpdesk or IT Operators should be trustees for **Groups**. Expand **People > Groups** item and assign trustees to this page item.

   NOTE: **Password Sync Status** is listed under **People** item. You should expand **People** item to modify trustees for **Password Sync Status**.

   In some cases, you might specify a user as a trustee but the application does not display that user's name in the trustee list. This occurs because that user is a member of a group or a role that is already listed as a trustee. The application does not list the user twice.

3. Select **OK**.
4. (Conditional) To set a default landing page for the OpenText Identity Manager Dashboard, enable the **Area default** option for that navigation item. For example, if you select the **Area default** radio button for **Application**, users will be directed to the Applications page when they login to the Dashboard.

   NOTE:

   - If you want to restore the default, the Dashboard will become the default landing page again.
   - When a user logs out of the OpenText Identity Manager Dashboard and then logs back in, they are taken to the same page from where they logged out.

   ---

5. Click **Save**.

Customize the Views

Enables you to configure the items displayed on the **Users** page for the selected client. You can also specify general settings for notifications and request forms.

- "General Settings" on page 143
- "User Settings" on page 144
- "Entity Settings" on page 145

To customize the views, select the client, then **Customization**.

General Settings

The **General** settings specify how the client responds upon user login and when the user initiates forms.

Notification Expiry

Specifies the number of days before a task or role expires that the application begins displaying a notification when the user logs in.

Enable Task Bulk Approval

Allows the client users to approve or deny multiple requests at a time.

Disable Implicit Claim of Task

Specifies whether it is mandatory for the user to claim a task before approving or denying it. By default, this flag is set as false; user can approve or deny the task without claiming it. If you set this flag as true, user must claim the task explicitly. In this case, the approval and deny options are not displayed until the task is claimed by a user. The functioning of **Disable Implicit Claim of Task** option also applies to bulk approval of tasks.

Set Availability while creating a Delegation Assignment

Specifies whether the application displays options for providing the availability details when the user creates a delegation. When selected, the application displays the availability options at the same time when the delegation is created. If you want to create delegation and specify availability details in separate actions, do not select this option.

Show Add Workflow in Roles Page

Enabling this setting displays the **Add Workflow** action on the **Roles** Page. By default, it is enabled.

Show Add Workflow in Resources Page

Enabling this setting displays the **Add Workflow** action on the **Resources** Page. By default, it is enabled.

Feedback Message Span

Specifies the period for a information message to appear on the page.

Identity Governance URL

Specifies the Identity Governance URL.

Managers Hierarchy

Specifies the manager's hierarchy. This helps the helpdesk users to reassign the helpdesk tickets to the managers of the specified level. You can set the hierarchy up to 3.

Enable Eager Search Results in Roles and Resources Page

Enable this option to display the roles in the Roles page and the resources in the Resources page. By default, this option is enabled. Disabling this option will not display the roles and resources when the Roles and the Resources pages are loaded.

Organization Chart separator for multi-valued attributes

Specifies the character or symbol that the application will use to separate values when displaying a multi-valued attribute for an entity (user or custom) in the **Organization Chart** page. By default, comma is used.

Organization Chart hierarchy depth

Specifies the maximum depth of the organization chart that the application can display for a user relationship in the **Organization Chart** page. An organization chart hierarchy depth of 3, for example will display the hierarchy of a user up to level 3 from the root user for a given relationship.

Notification Interval

Specifies the time interval at which the application calls the `notifyService` API to retrieve the information on any new task, role, or resource assigned to the logged-in user, then notify the user on the Dashboard. The default value of this setting is 120000 milliseconds (2 minutes).

User Settings

The **User** settings enable you to configure the attributes displayed on the **Users** page and organization chart for the selected client.

Card View

Represents the attributes that you want the application to display by default when the user selects **Card View** in the **Users** page. These attributes will also appear on a user's card on the Organization Chart page.

Other Attributes

Represents additional attributes that provide details about a selected user.

Editable Attributes

Represents the attributes that can be modified for a user's details. For most attributes, you can also enter text to serve as default values or examples to aid in new user creation, as desired.

User Default Photo

Represents the image that you want the application to display by default when you enable the image toggle button in the **Card View** on **Users** page.

User Search Lookup Attribute

Represents the attributes that users can define when searching for a user entity. It applies to the fields that use the DN Lookup widget in Identity Applications Dashboard.

User Search Default Attribute

Represents the attributes that users can define when searching for a user or filtering search results on the **Users** page.

User General Settings

Represents the default container for storing users and how the application responds when displaying search results.

- **Base Container**

  Specifies the container in the Identity Vault that stores a newly created user.

  When creating a user, you can see this value but cannot modify it. This limitation ensures that all users are stored in the same container for that client.

- **User List Container**

  Specifies the container in the Identity Vault that you want the application to use for listing users in the **Users** page.

- **User Profile Entity**

  Specifies the entity that the application will display in the **My Profile** page. By default, the user entity is displayed.

- **Show All Permissions**

  Enable this setting to list all permissions assigned to the user on the **Permissions** page. This include permissions directly assigned to the user and those assigned indirectly through groups or containers. By default, this settings is disabled, allowing the user to see the list of direct assigned permissions only.

- **User Search Limit**

  Specifies the maximum number of users that the application can list as a result of a user search.

- **Default Organization Chart Relationship**

  Specifies the relationship that the application will display by default in the **Organization Chart** page. By default, it is set as Manager-Employee.

  In addition to the default relationships provided with Identity Applications installation package, the administrator can also create custom relationship in the Directory Abstraction Layer using the Designer. For more information, see OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications.

View Permissions Type

Enable the permission types such as **Roles**, **Resources**, and **PRD**. This allows your client users to view or request the permission types that are selected.

By default, all the permission types are enabled.

Entity Settings

You can configure the entities that are added to Identity Applications through Designer.

1. (Conditional) To configure an entity, click **+** next to Customization Settings.
2. (Conditional) If you want to modify the settings for a configured entity, select the required entity from the **Navigation Items** list.

3 Specify the following details:

View Attributes

Drag and drop the required attributes into **Selected Attributes** from **Available Attributes**.

These attributes are displayed when you select this entity from the **Entities** menu.

Editable Attributes

Specify the attributes that can be modified for an entity.

You can specify one or more editable attributes.

Search Attribute

Specify the attributes to search records for an entity.

You can specify one or more search attributes.

Base Container

Specify the container where you want to store the objects created for this entity.

For example,

If you select **data > group** container to the **group** entity, the groups created using this entity will be stored under **group** container.

Default Organization Chart Relationship

Specify the relationship that will be displayed in the organization chart page for this entity.

Organization Chart View

Drag and drop the required attributes into **Primary Attributes** and **Secondary Attributes** from **Attributes** field.

These attributes are displayed when you want to view the organization chart for this entity under the **Entities** menu.

Display Attributes for Organization Chart Search

Specify the display attributes for organization chart search results. A maximum of two attributes are allowed for selection.

Organization Chart Photo

Specify the attribute whose value will be used to display the image for this entity in the organization chart under the **Entities** menu. If an attribute has multiple values, the first value is selected for display by default.

4 Click **Save**.

Customize the Branding

For each client, you can customize the following look and feel attributes:

- Change the logo, title, and colors in the page header.
- Specify the URL that the application displays when a user clicks the page title or footer.
- Add links and contact information to the footer or disable the page footer.
- Localize the content in the header and footer.
- Specify a customized cascading style sheet (CSS).

To use a CSS, you can modify the sample under **Advance Settings**.

1. Click **Download Sample CSS**, to download the sample `custom.css` file.
2. Modify the `custom.css` file values and click **Upload CSS**.

To customize the branding, select the client, then **Branding**. For more information, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

Client Helpdesk Settings

For each client, you can setup a **Helpdesk** to assist their users.

1. Specify **Helpdesk Name**.
2. Specify the **Email Address** of the helpdesk.
3. Specify the **Contact Number** of the helpdesk.
4. Click **Add** to add more contact numbers.
5. Enable **Show in Footer** to display the helpdesk information in the footer of user's page.
6. Enable **Show in Request History** to display the helpdesk information in the Request History page.
7. Enable **Show in Menu** to display the helpdesk information in the Dashboard menu.
8. Provide **Access Rights** to the selected users for the following Helpdesk resources:

   Organization Chart Access

   Selected users can view the organization chart of respective client.

   Group Access

   Selected users can view groups of respective client.

   Reassign Access

   Selected users can reassign the user's tasks to the approver's managers.

   NOTE: You can configure **Managers Hierarchy** in **Customization**, this helps the helpdesk users to reassign the user's tasks to the managers of the specified level, if necessary.

   Teams Access

   Selected users are allowed to view teams and team members configured for respective client.

   History Access

   Selected users can view request history of any user of respective client.

   User Catalog Access

   Selected users can view details of any user of respective client.

Manage Dashboard Widgets

In **Dashboard Widgets**, you can provision widgets for a User, Group, Container, or a Role.

Widgets

Lists all widgets available in the system.

Trustees

Allows you to select Users, Group, Container, and Roles that you wish to provision this widget on their Dashboards.

Order

Specifies the order in which the widget should display on the dashboard. You can drag the widgets up and down to rearrange the order. By default, the widgets are displayed in the order mentioned in this page. Users can personalize the order after adding widgets to their dashboards.

XVI Entities

You can manage one or more entities in your organization using Identity Applications. You can add entities to Identity Applications using Designer. For more information, see Adding Entities in the *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to Designing the Identity Applications*.

OpenText Identity Manager Dashboard lists all the configured entities under the **Entities** menu. To configure entity settings in OpenText Identity Manager Dashboard, see Entity Settings in the"Customize the Views" on page 143.

To see trustees who can access entities, go to **Your ID > Settings** > **Access** and search for **Entities**.

- Chapter 35, "Managing Entities," on page 151

For more information about this software product, see the OpenText Identity Manager documentation (https://www.netiq.com/documentation/identity-manager-4.10/).

35 Managing Entities

The **Entities** menu is displayed only if:

- An entity is added and deployed to identity applications from Designer, and
- The user is assigned as trustees for that entity

In the **Entities** menu, click the entity for which you wish to create and manage objects associated with it.

For example, **Entities > <entity_name>**

- "Creating an Object" on page 151
- "Editing an Object" on page 151
- "Deleting an Object" on page 151
- "Exporting an Object to a CSV file" on page 151
- "Viewing Organization Chart of an Object" on page 152

Creating an Object

1. Click +.
2. Specify the details for the fields marked with an asterisk (*).
3. Click **Create**.

Editing an Object

1. Select the object you want to edit.
2. Click **Edit**.
3. Edit the required fields.
4. Click **Save**.

Deleting an Object

1. Select the object you want to delete.

   You can select one or more objects at a time.
2. Click 🗑.

Exporting an Object to a CSV file

1. Select the object for which you require the results to be exported to a CSV file.

You can select one or more objects at a time.

2 Click .

3 Click **Save**.

Viewing Organization Chart of an Object

1 Select the object to view the organization chart.

You can view organization chart of only one object at a time.

2 Click .

The organization chart of the object is displayed based on the default relationship set for that entity.

3 (Optional) If the **Default Organization Chart Relationship** for the entity is not defined in the **Settings** page, then a prompt to select the required relationship is displayed. Select the organization chart relationship from the drop-down list and click **View**.

Part I Welcome to OpenText Identity Manager 3

1 Applications Page 5

Customize the Applications Page . . . 5

2 Configure the Applications Page 7

Create and Edit Items and Permissions . . . 7
Add, Modify, or Delete a Category . . . 7
Add a Category . . . 7
Modify a Category . . . 8
Delete a Category . . . 8

Part II Dashboard 9

3 Customize Your Dashboard 11

Manage the Global Dashboard . . . 11
Manage Widgets and Layouts . . . 11
Add a Widget . . . 12
Add General Widgets . . . 12
Add OpenText Identity Manager Widgets . . . 14
Widget Options . . . 14
Configure a Widget . . . 15
Change the Dashboard Layout . . . 16

Part III Tasks 17

4 View and Manage Tasks 19

Viewing your Tasks . . . 19
Approve and Deny Requests . . . 20
One Request at a Time . . . 20
Multiple Requests at the Same Time . . . 20
Managing Requests for Approval or Denial . . . 20
Manage Helpdesk Tasks . . . 21

5 Review the History of Executed Tasks 23

Viewing your Task History . . . 23
Review the Details of a Workflow . . . 24

6 Act as or Assign a Proxy 25

Act as a Proxy . . . 25
Manage Proxy Assignments . . . 25

7 Manage Approvals by Email 27

Configuring Email-based Approvals . . . 27

Part IV Permissions 35

8 Review Your Permissions 37

Review the Details of a Permission . . . 37
Find a Permission of Self . . . 38
Find a Permission of Others . . . 39
Remove a Permission . . . 39
Customize Columns. . . . 40

9 Request Permissions 41

Request Permission(s) . . . 41
Find a Permission to Request . . . 43
Manage Featured Items . . . 43
Add a Permission . . . 43
Delete a Permission . . . 44
Edit a Permission . . . 44

10 Review a History of Requests 45

Review the Details of a Request . . . 45
Find a Request of Self . . . 45
Find a Request of Others . . . 46
Raise a Helpdesk Ticket . . . 46
Cancel a Request . . . 46
Customize the View . . . 46

Part V Users and their Organization Chart 49

11 View and Manage Users 51

Find a User . . . 51
Create a User Profile . . . 51
Modify a User's Profile . . . 52
View a User's Organization Chart . . . 52
Enabling Login for Disabled User Accounts. . . . 52

12 View and Manage the Organization Chart 53

Working With the Organization Chart . . . 53
Reset the Root in the Organization Chart View . . . 53
Switch to the Organization Chart View . . . 54
Choose a Relationship to View . . . 54
Navigate to the Next Level in Relationship Hierarchy . . . 54
Send Email to Users from the Organization Chart . . . 55
View Detailed Information of a User . . . 56

Part VI Groups 57

13 Manage Groups 59

Create a Group . . . 59
Edit a Group . . . 59
Delete a Group . . . 59

Part VII Teams 61

14 View Teams 63

Create a New Team . . . 63
Modify an Existing Team . . . 63

15 Add a Team 65

Create a New Team . . . 65
Add Permissions to the Team . . . 65
Add Resources and Roles . . . 66
Add Provisioning Request Definitions . . . 67
Enable Requesters to Make Proxy Assignments . . . 67
Use Case Example . . . 68

16 Modify a Team 69

Part VIII Delegation 71

17 View and Manage Delegations 73

List Delegations . . . 73
Create a Delegation . . . 73
Modify Delegations . . . 74

Part IX Availability 75

18 Specifying Your Availability 77

View Availability Status . . . 77
Change the Availability Status . . . 77
Create an Availability Setting . . . 78
Edit an Availability Setting . . . 78

Part X Roles and Resource Administration 79

19 View and Manage Roles 81

List Roles . . . 81
Find a Role . . . 81
Customize Columns . . . 81

Create a Role 82
Change Language 82
Edit Roles 82
Change the Approval or Revocation Process 83
Map Resources to the Role 83
Assign Role to the Users 84
Map Role to Role 84
Add Workflow to Roles 85

20 View and Manage Resources 87

List Resources 87
Find a Resource 87
Customize Columns 87
Create a Resource With Entitlement 88
Create a Resource Without Entitlement 88
Edit Resources 89
Assign Weightage to the Resources 90
Change the Approval or Revocation Process 90
Assign Resource to the Users 91
Resource Form 91
Add Workflow to Resource 92

Part XI Separation of Duties (SoD) 93

21 Manage SoD 95

Create SoD 95
Edit SoD 95
Delete SoD 95

Part XII Controlled Permission Reconciliation Services 97

22 View and Manage Permission Reconciliation 99

Monitor Permission Assignment Updates 99
Manage Permission Reconciliation 100
Compute the Selected Driver or Entitlement Assignments 100
Publish Assignments for the Selected Driver or Entitlement 101
View the Process Status for the Selected Entitlement Assignments 101

Part XIII Monitoring Workflows 103

23 Monitor and Manage Workflows 105

Search for Workflows 105
Sort Workflows 105
Customize Columns 105
View Workflow Status 106
View Approval Status 106

Advanced Operations Available On This Page 107
Terminate a Workflow Process 107
Reassign a Workflow Process 107
View Comments to Know More About Workflows 107

Part XIV Configuration 109

24 View and Configure Roles and Resources Settings 111

Role Settings 111
Resource Settings 112
Entitlement Query Settings 112
Separation of Duties Settings 112

25 View and Configure Delegation and Proxy Settings 115

View and Configure Delegation Settings 115
View and Configure Proxy Settings 115
View and Configure Synchronization and Cleanup Service 116

26 Enable and Configure Permission Reconciliation Service 117

27 View and Configure Log Events 119

Change Auditing Service Settings 119
Add an OpenText Identity Manager Package 119
Change the Log Levels for OpenText Identity Manager Packages 120

28 View and Manage Cache Events 121

Flushing Caches 121
View and Manage Cache Settings 121
View and Manage Cluster Cache Configuration 123

29 Assign Administrators in Identity Applications 125

Listing the Administrator Assignments 125
Find an Administrator Assignment 125
Customize Columns 126
Create a New Administrator Assignment 126
Assign Permissions to a Delegated Administrator 127
Delete an Administrator Assignment 127

30 View and Configure the Workflow Engine and Cluster Settings 129

Configure the Workflow Engine Settings 129
Configure Workflow Cluster Settings 130
View the Workflow Engines State 131

31 View User Application Driver Status **133**

32 View and Configure the Default Provisioning Display Settings **135**

View and Manage General Display Settings 135
View and Manage the Appearance of Tasks Page 135
View and Manage the Appearance of Request History Page 136

33 Configure Identity Governance Settings **137**

Part XV Client Customization **139**

34 Customize the User Interface **141**

Manage Clients 141
Control User Access 141
Considerations for Configuring User Access 141
Configuring User Access 142
Customize the Views 143
General Settings 143
User Settings 144
Entity Settings 145
Customize the Branding 146
Client Helpdesk Settings 147
Manage Dashboard Widgets 147

Part XVI Entities **149**

35 Managing Entities **151**

Creating an Object 151
Editing an Object 151
Deleting an Object 151
Exporting an Object to a CSV file 151
Viewing Organization Chart of an Object 152