NetIQ® Identity Manager

User's Guide to the Identity Applications

May 2024

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.

For additional information, such as certification-related notices and trademarks, see http://www.microfocus.com/about/legal/ (http://www.microfocus.com/about/legal/).

Contents

About this Book and the Library 7

Part I Welcome to Identity Manager 9

1 Getting Started 11

Understanding Roles and Resources . . . 11
Understanding the Identity Applications . . . 11
Understanding Identity Manager Dashboard . . . 11
Exploring the Dashboard . . . 12
Understanding Applications Page . . . 13
Understanding Tasks . . . 14
Typical Ways to Use the Identity Applications . . . 14
How Identity Self-Service Works . . . 14
How Roles and Resources Work . . . 14
How Process Requests Work . . . 16
How Helpdesk Works? . . . 16

2 Accessing the Identity Applications 19

Considerations for Accessing the Identity Applications . . . 19
Logging in the First Time . . . 20
Responding to a Preferred Locale Check . . . 21
Troubleshooting Login Issues . . . 22
If You Forget Your Password . . . 22
If You Have Trouble Logging In . . . 22
If You're Prompted for Additional Information . . . 22
Logging Out . . . 22

Part II Customizing Your Dashboard 23

3 Managing Widgets and Layouts 25

Managing the Global Dashboard . . . 26
Changing the Dashboard Layout . . . 26
Adding a Widget . . . 27
Add General Widgets . . . 28
Add Identity Manager Widgets . . . 29
Add Identity Governance Widgets . . . 30
Widget Options . . . 30
Configuring a Widget . . . 31

Part III Managing Your Permissions and Identity Profile 33

4 Managing Your Permission Requests 35

Viewing Your Permissions . . . 35
Requesting Permissions . . . 37
Viewing Requests . . . 37
Tracking a Request . . . 38
Canceling a Request . . . 38
Raising a Helpdesk Ticket . . . 38
Revoking Permissions . . . 39
Deep Linking to a Request . . . 40

5 Managing Applications 41

Creating Featured Items . . . 41
Adding an Application . . . 41
Adding a Permission . . . 42
Add, Modify, or Delete a Category . . . 42
Add a Category . . . 42
Modify a Category . . . 42
Delete a Category . . . 43

6 Managing Your Tasks 45

Viewing your Tasks . . . 45
Managing Requests for Approval or Denial . . . 46
Managing Helpdesk Tasks . . . 47

7 Acting on Behalf of Someone Else 49

Viewing Your Proxy Assignments . . . 49
Acting as a Proxy . . . 49
Managing Proxy Assignments . . . 49

8 Managing Delegations 51

9 Managing Your Availability 53

10 Managing Your Profile 55

Updating Your Profile . . . 55

11 Managing the Organization Chart 57

Viewing an Organization Chart . . . 57
Understanding the Organization Chart . . . 58
Working with the Organization Chart . . . 59
Reset the Root in the Organization Chart View . . . 60
Switch the Organization Chart view . . . 60
Choose a Relationship to View . . . 61
Navigate to the Next Level in Relationship Hierarchy . . . 62

Send Email to Users from the Organization Chart 63
View Detailed Information of a User 63

12 Managing Your Password 65

Using Self-Service Password Management in Identity Manager 65
Understanding Password Challenge Response 66
Changing Your Password 66
Password Policy Status 67
Using the Legacy Password Management 67
Password Challenge Response 68
Password Hint Change 69
Change Password 69
Password Policy Status 70
Password Sync Status 70

Part IV Managing Users, Groups, and Teams 71

13 Managing Users 73

Creating a User 73
Editing User Information 73
Listing Users 74
Finding Users 75
Sorting Users 76

14 Managing Teams 77

View Teams 77
Create a Team 78
Modify a Team 78

15 Managing Groups 79

Creating a Group 79

About this Book and the Library

This guide describes how end-users and some administrators can use the NetIQ Identity Manager identity applications, particularly the Dashboard and User Application.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Other Information in the Library

For more information about the library for Identity Manager, see the Identity Manager documentation Website (https://www.netiq.com/documentation/identity-manager-49/).

Welcome to Identity Manager

NetIQ Identity Manager is a system software product that your organization uses to securely manage the access needs of its user community. If you're a member of that user community, you benefit from Identity Manager in a number of ways. For example, Identity Manager enables your organization to:

- Give users access to the information (such as group org charts, department white pages, or employee lookup), as well as roles and resources (such as equipment or accounts on internal systems) that they need, right from day one
- Synchronize multiple passwords into a single login for all your systems
- Modify or revoke access rights instantly when necessary (such as when someone transfers to a different group or leaves the organization)
- Support compliance with government regulations

Read this part first to learn about the Identity Manager identity applications and how to begin using them. This guide is designed to assist the following types of online activity in your organization:

- Manage your online identity associated with organizational resources.
- View or modify your access to organizational roles and resources.
- Approve requests for access to resources and roles.
- Manage the permissions associated with software applications and other resources that your organization provides to members of your organization.

1 Getting Started

This section tells you how to begin using the identity applications. Topics include:

- "Understanding Roles and Resources" on page 11
- "Understanding the Identity Applications" on page 11
- "Understanding Identity Manager Dashboard" on page 11
- "Exploring the Dashboard" on page 12
- "Understanding Tasks" on page 14
- "Typical Ways to Use the Identity Applications" on page 14

Understanding Roles and Resources

In the identity applications, a **permission** represents the access provided to a user or group of users for a role or resource. A **role** defines a set of permissions related to one or more target systems or applications. For example, a user administrator role might be authorized to reset a user's password, while a system administrator role might have the ability to assign a user to a specific server. A **resource** is any digital entity such as a user account, computer, or database that a business user needs to be able to access.

Understanding the Identity Applications

The Identity Manager identity applications are an interconnected set of browser-based Web applications. They enable your organization to manage the user accounts and permissions associated with the wide variety of roles and resources available to users. You can configure the identity applications to provide self-service support for your users, such as requesting roles or changing their passwords. You can also set up workflows to improve the efficiency in managing and assigning roles and resources.

Understanding Identity Manager Dashboard

NetIQ Identity Manager Dashboard (the Dashboard) serves as the primary entry portal to the identity applications. The Dashboard can have one or many widgets that helps you with the quick information about particular activity. From your Dashboard, you can perform the following activities:

- Manage your profile settings and password.
- View your organization chart details.
- Review and complete your tasks, such as approving user requests for access.
- Request permissions for roles, resources, or processes.
- Review the status and history of the requests for permissions.
- Find other users in your organization.

- Personalize your dashboard, you can add widgets and reposition them based on your interests.
- Set any user as your proxy from the system.
- Delegate your tasks to other users from the system.

You can perform the following tasks with the appropriate **Permissions**:

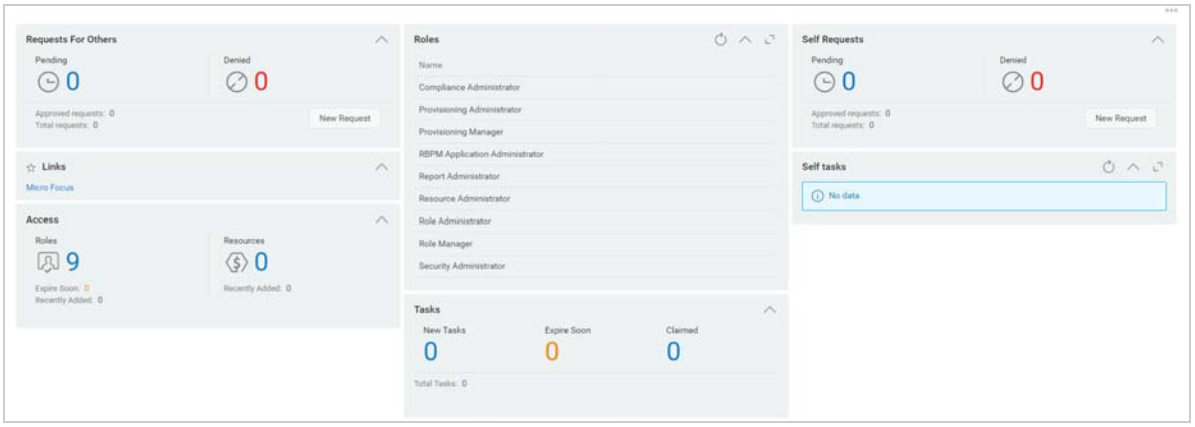
- Create and modify user profiles.
- View the organization chart details of other users.
- Create and modify teams that represent a set of users and groups that can perform provisioning requests and approval tasks associated with the teams.
- Request permissions or revoke permissions on behalf of other users in the organization.

Exploring the Dashboard

The Dashboard provides quick information about your tasks, permissions, and requests in the form of widgets. You can navigate to specific pages or applications with a single click. Additionally, you can add, remove, reposition, and configure widgets on your Dashboard. For more information about personalizing your Dashboard, see Chapter 3, “Managing Widgets and Layouts,” on page 25.

Following is an example that describes the default widget options on the Dashboard.

Figure 1-1 *Example Personal Dashboard*



Identity Manager Dashboard allows you to manage different activities on Identity Manager. Following are the pages that help you to manage your tasks and activities:

Application

Lists all the applications that are provisioned for you. This provides default links to several areas to streamline the basic tasks that you need to perform in Identity Manager. For more information, see “Understanding Applications Page” on page 13.

Tasks

Shows all your tasks that are pending for an action. With an appropriate role, you can view the tasks of others. For example, Team Manager.

Access

Allows you to view permissions or request permissions. To view the status of requested permissions, go to **Request History**. This page displays all your requests and their status.

People

Allows you to view other users or groups in the system and other user's **Organization Chart**. This helps them to visualize how those users and groups are related.

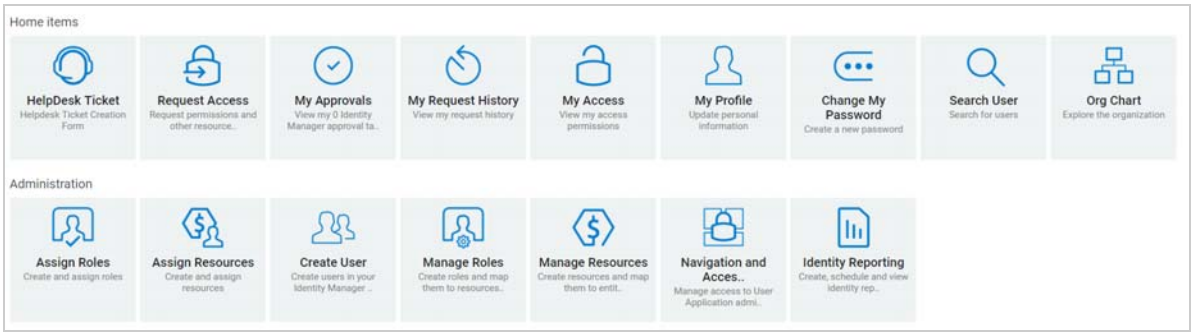
Administration

Allows you to view and manage roles, resources, permission reconciliation, and their configurations. This option appears only for administrators. For more information about Administration tasks, see Identity Applications Administration in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Understanding Applications Page

The second significant view in the Dashboard is the **Applications** page (Figure 1-2), which provides default links to several areas to streamline the basic tasks that end users and administrators need to perform in Identity Manager.

Figure 1-2 *Example of the Applications page on the Dashboard*



By default, **Helpdesk Ticket** appears on your **Applications** page. This option allows you to raise a ticket to your helpdesk.

Your identity administrator customizes the **Applications** page to include tiles that link to commonly requested resources or applications that users regularly access. You can configure the user access for these tiles with an appropriate administrative role. Navigate to **Your ID > Settings > Access** to add trustees for the required navigation items. For more information about provisioning access, see Managing User Access in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Some of the tiles on this page might appear only for users with an administrative role in the identity applications. For example, a person who can create or modify roles should see a tile similar to **Create User** and **Manage Roles**.

For more information about using the Dashboard, click ⓘ on the Dashboard.

Understanding Tasks

The **Tasks** page allows you to approve or deny actions for the tasks listed.

The Identity Manager dashboard allows you to manage the Identity Manager and Identity Governance tasks from the Tasks page. You can now view and approve both Identity Manager and Identity Governance tasks from the same user interface.

Typical Ways to Use the Identity Applications

Here are some examples of how people typically use the identity applications within an organization.

- "How Identity Self-Service Works" on page 14
- "How Roles and Resources Work" on page 14
- "How Process Requests Work" on page 16
- "How Helpdesk Works?" on page 16

How Identity Self-Service Works

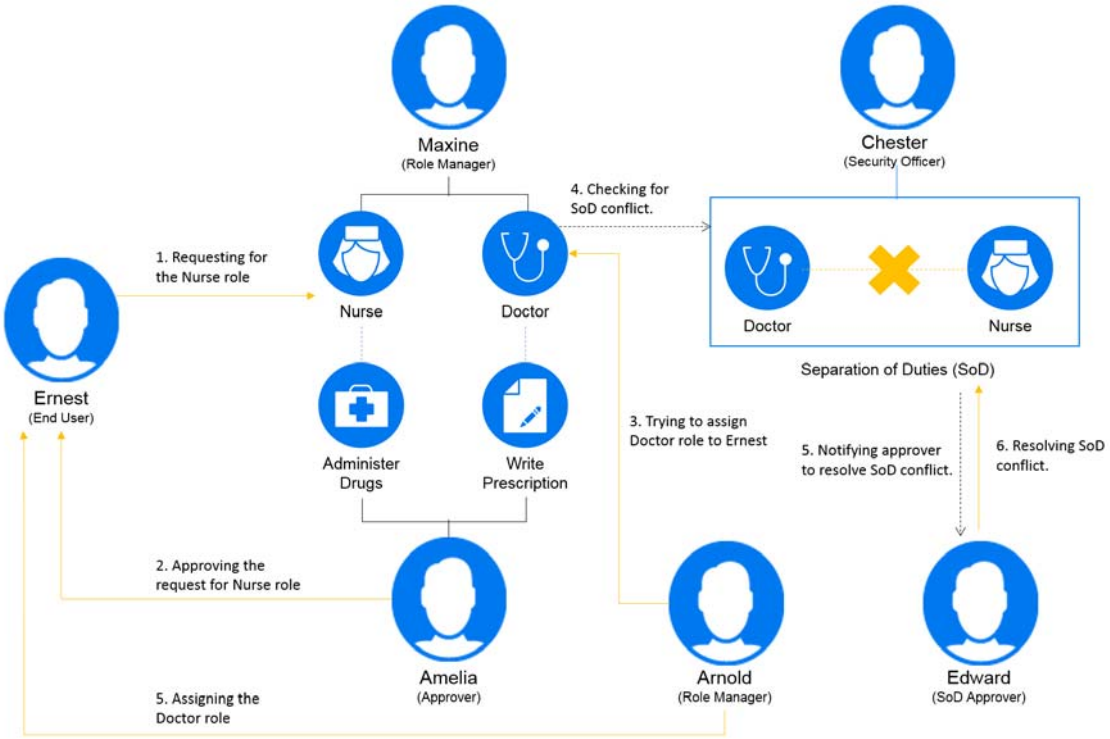
- Ella (an end user) recovers her forgotten password through the identity self-service features when logging in.

  By default, Identity Manager uses Self Service Password Reset (SSPR) to allow users to modify their passwords. However, the identity applications can use other methods for managing forgotten passwords.
- Erik (an end user) performs a search for all employees who speak German at his location.
- Eduardo (an end user) browses the organization chart, finds Ella, and clicks the e-mail icon to send a message to her.

How Roles and Resources Work

Following is an example that explains the flow of roles and resources request in the system:

Figure 1-3 *Example Scenario of Role Assignment*



- Maxine (a Role Manager) creates the Nurse and Doctor business roles and the Administer Drugs and Write Prescriptions IT roles. Maxine creates several resources that are needed for these roles, and associates the resources with the roles.
- Maxine (a Role Manager) defines a relationship between the Nurse and Administer Drugs roles, specifying that the Nurse role contains the Administer Drugs role. Max also defines a relationship between the Write Prescriptions and Doctor roles, specifying that the Doctor role contains the Write Prescriptions role.
- Chester (a Security Officer) defines a separation of duties constraint that specifies that a potential conflict exists between the Doctor and Nurse roles. This means that ordinarily the same user should be not assigned to both roles at the same time. In some circumstances, an individual who requests a role assignment may want to override this constraint. To define a separation of duties exception, the individual who requests the assignment must provide a justification.
- Ernest (an end user) browses a list of roles available to him, and requests assignment to the Nurse role.
- Amelia (an approver) receives notification of an approval request via e-mail (which contains an URL). She clicks the link, is presented with an approval form, and approves it.
- Arnold (a Role Manager) requests that Ernest be assigned to the Doctor role. He is notified that a potential conflict exists between the Doctor role and Nurse role, to which Ernest has already been assigned. He provides a justification for making an exception to the separation of duties constraint.

- Edward (a separation of duties approver) receives notification of a separation of duties conflict via e-mail. He approves Arnold's request to override the separation of duties constraint.
- Amelia (an approver) receives notification of an approval request for the Doctor role via e-mail. She approves the Arnold's request to assign Ernest to the Doctor role.
- Bill (a Role Auditor) looks at the SoD Violations and Exceptions Report and sees that Ernest has been assigned to both the Doctor and Nurse roles. In addition, he sees that Ernest has been assigned the resources associated with these roles.

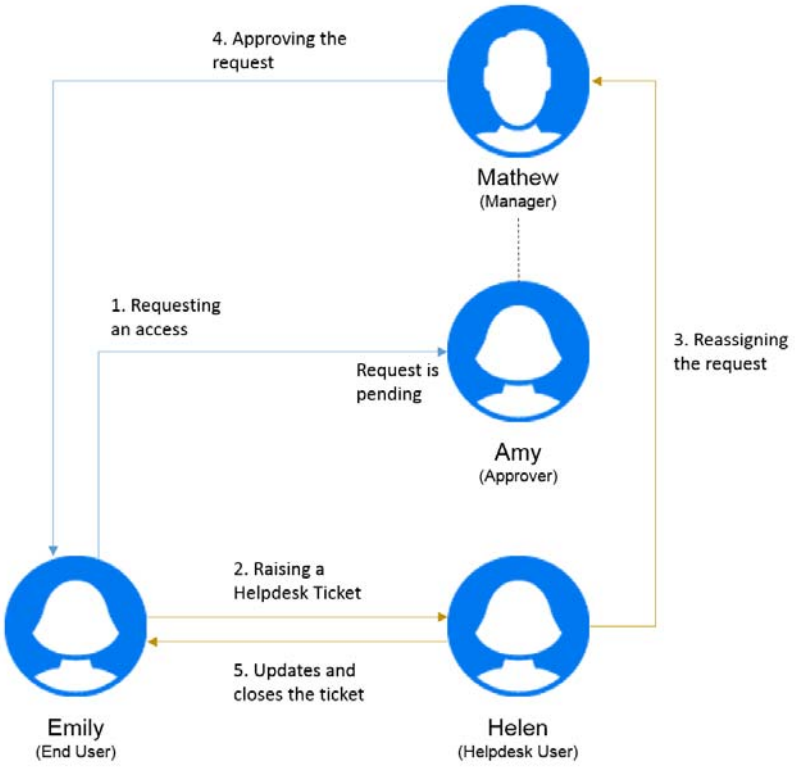
How Process Requests Work

- Ernie (an end user) browses a list of resources available to him, and requests access to the Siebel* system.
- Amy (an approver) receives notification of an approval request via e-mail (which contains an URL). She clicks the link, is presented with an approval form, and approves it.
- Ernie checks on the status of his previous request for Siebel access (which has now gone to a second person for approval). He sees that it is still in progress.
- Amy is going on vacation, so she indicates that she is temporarily unavailable. No new approval tasks are assigned to her while she is unavailable.
- Amy opens her approval task list, sees that there are too many for her to respond to in a timely manner, and reassigns several to co-workers.
- Pat (an administrative assistant, acting as a proxy user for Amy) opens Amy's task list and performs an approval task for her.
- Max (a manager) views the task lists of people in his department. He knows that Amy is on vacation, so he reassigns tasks to others in his department.
- Max initiates a request for a database account for someone in his department who reports directly to him.
- Max assigns Dan to be an authorized delegate for Amy.
- Dan (now a delegated approver) receives Amy's tasks when she is unavailable.
- Max engages an unpaid intern, who should not be entered into the HR system. The system administrator creates the user record for this intern and requests that he be given access to Notes, Active Directory*, and Oracle*.

How Helpdesk Works?

Following is an example that explains the flow of helpdesk ticket in the system:

Figure 1-4 *Example for Helpdesk*



- Emily (an end user) has requested for an office printer access. This request was pending for a long time. Therefore, she raised a helpdesk ticket.
- Helen (a helpdesk user) receives a notification of the helpdesk ticket in her list of tasks.
- Helen analyzes the issue and finds out that request is assigned to Amy (an approver).
- This request is pending in the system because Amy is out of office.
- Helen has a permission to reassign task requests. She reassigns this request to Mathew (Amy's manager).
- Mathew reviews the request and approves it. Emily can access the office printer.
- Helen updates and closes the helpdesk ticket.

2 Accessing the Identity Applications

You access the identity applications, such as the Dashboard, in a Web browser. Identity Manager supports the most popular browser versions. See your system administrator for a list of supported browsers or for help installing one. Your organization should provide you with the URL and credentials required to access the applications.

- "Considerations for Accessing the Identity Applications" on page 19
- "Logging in the First Time" on page 20
- "Responding to a Preferred Locale Check" on page 21
- "Troubleshooting Login Issues" on page 22
- "Logging Out" on page 22

Considerations for Accessing the Identity Applications

Before accessing the Dashboard or any of the other identity applications, review the following considerations:

- You must enable cookies and enable JavaScript* in your Web browser.
- When using Internet Explorer, you should set at least **Medium** privacy level. You should also select the **Every time I visit the webpage** option under **Tools** > **Internet Options** > **General**, **Browsing History** > **Settings** > **Check for newer versions of stored pages**. If you do not have this option selected, some of the buttons may not be displayed properly.
- If you have previously accessed the Identity Manager User Application, you may be able to use the same user name and password to access the Dashboard.
- You cannot access the identity applications using an account that includes any of the following characters in the name:

  `\ /, * ? . $ # +`

- If you cannot log in, you can click **Forgot password**. For more information, see "If You Forget Your Password" on page 22.
- If you see a different first page when accessing the Identity Manager user interface, it's typically because the application has been customized for your organization. As you work, you might find that other features of the identity applications have also been customized.

  If this is the case, you should check with your system administrator to learn how your customized identity applications differ from the default configuration described in this guide.

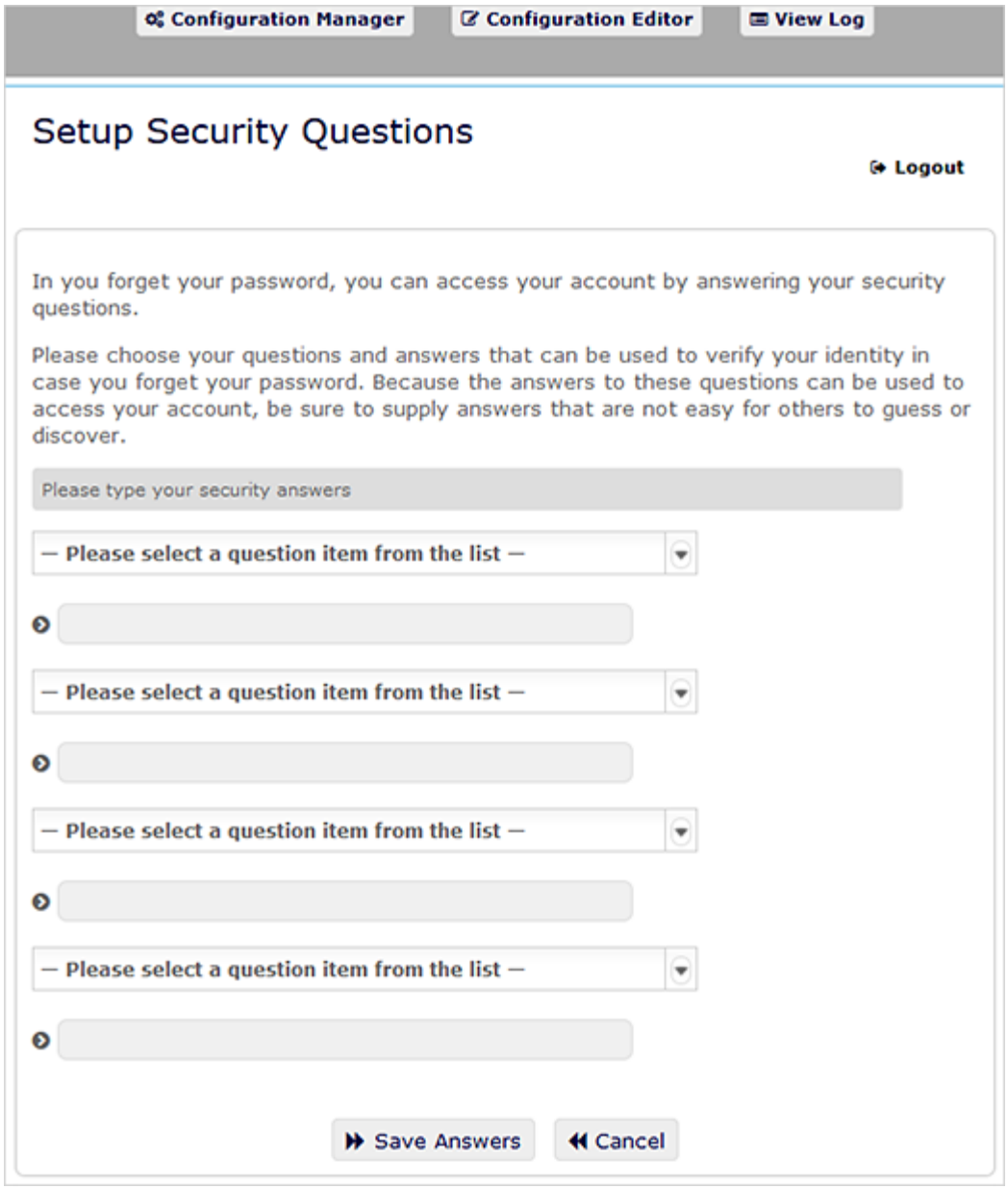
Logging in the First Time

You must be an authorized user to log in to the identity applications, such as the Dashboard. If you need help getting a username and password to supply for the login, see your system administrator.

The first time that you log in to the identity applications, Identity Manager requires you to establish security parameters for your account to help with resetting your password in future. If you forget your password and try to reset it next time you log in, Identity Manager prompts these configured questions and asks you to specify the correct answer. When the answer matches with the response that you save in this page, you can reset the password.

To set up the security questions during your first log in:

1. Enter your username and password, then click **Login**.
2. The login page automatically redirects you to the **Challenge-Response** page.
3. Specify the questions and answers for the Security Questions.



4 Click **Save Answers**, and you are redirected to the Dashboard.

Responding to a Preferred Locale Check

If you receive a prompt to select your own preferred locale when you log in, your administrator configured the identity applications to perform a language check on users' browsers. This might be necessary to ensure that the content that you see appears in a supported language.

When prompted to add a locale, open the **Available Locales** list, select a locale, and click **Add**. For more information, see Adding the New Language to the Identity Applications.

Troubleshooting Login Issues

This section provides solutions to the following types of common login problems:

- "If You Forget Your Password" on page 22
- "If You Have Trouble Logging In" on page 22
- "If You're Prompted for Additional Information" on page 22

If You Forget Your Password

If you can't remember the password, you might be able to use the **Forgot Password** link for assistance. When you are prompted to log in, this link appears on the page by default. You can use this link if your system administrator has set up an appropriate password policy for you.

1. When you're prompted to log in, click the **Forgot Password** link.
2. Type your username and click **Submit**.

   If Identity Manager responds that it can't find a password policy for you, see your system administrator for assistance.
3. Answer the challenge questions that display. Identity Manager prompts you to answer the configured questions. When the answer matches with the response that you had saved earlier, you can reset the password. Click **Submit**. For example:

   Answer the challenge questions to get assistance with your password. Depending on how the system administrator has set up your password policy, you could:

   - Receive an e-mail containing your password about it
   - Be prompted to reset your password

If You Have Trouble Logging In

If you are unable to log in, make sure that you're using the right username and typing the password correctly (spelling, uppercase or lowercase letters, etc.). If you still have trouble, consult your system administrator. It is helpful if you can provide details about the problem you are having (such as error messages).

If You're Prompted for Additional Information

You might be prompted for other kinds of information as soon as you log in. It all depends on how the system administrator has set up your password policy (if any). For example:

- If this is your first login, you are prompted to define your challenge questions and responses
- If your password has expired, you are prompted to reset it

Logging Out

When you are finished working on the Dashboard and other identity applications, you should log out. On the Dashboard, click your username in the upper right corner, then select **Sign out**.

11 Customizing 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*.

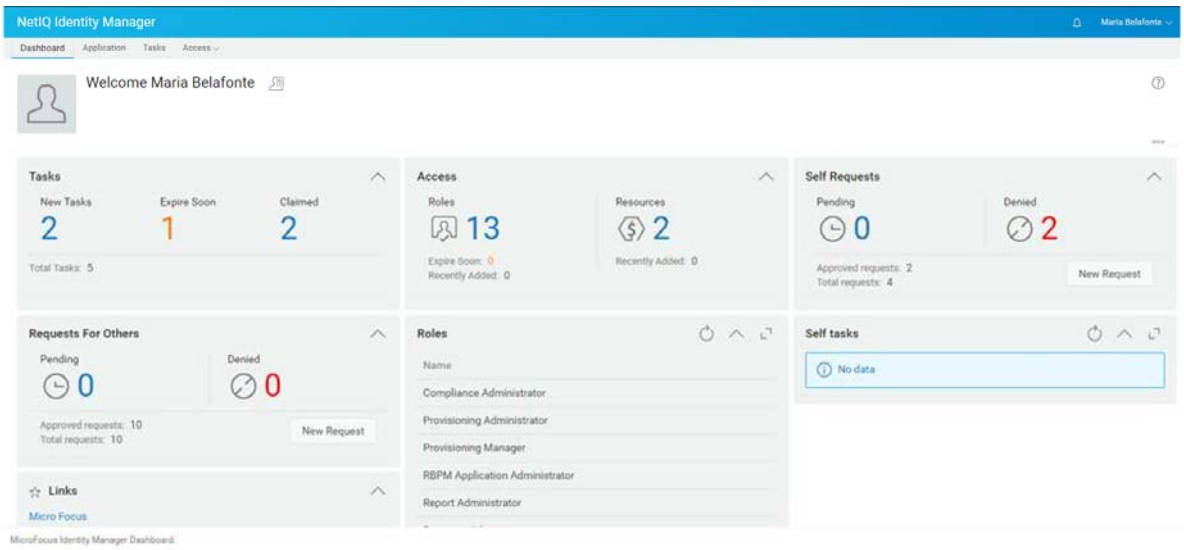
3 Managing Widgets and Layouts

Widgets are Dashboard objects that are designed to provide specific details to a user for a 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 Role from **Your ID** > **Settings** > **Dashboard Widgets**.

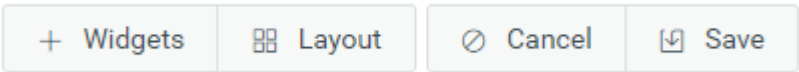
To personalize your Dashboard, go to your **Dashboard** and click ∘∘∘.

Figure 3-1 *Personalize Dashboard*



Use the following are options to personalize your Dashboard:

Figure 3-2 *Personalization Options*



Widgets

Allows you to add Widgets on your Dashboard. See "Adding a Widget" on page 27.

Layout

Allows you to change the Dashboard layout. See "Changing the Dashboard Layout" on page 26.

Cancel

Cancels all the changes made to your Dashboard.

Save

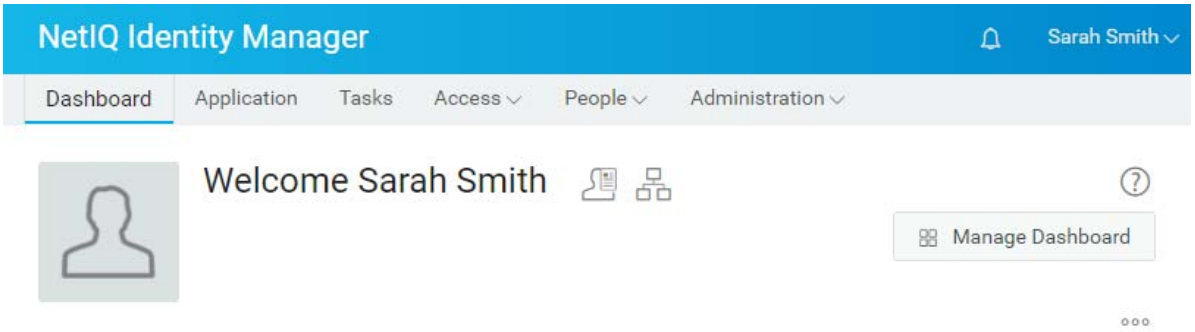
Saves your changes and applies to your Dashboard.

Managing 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 provisioned by an administrator. The **Manage Dashboard** option allows you to add, modify or remove widgets from the global dashboard.

NOTE: You should be added as a trustee to use the **Manage Dashboard** option.

Figure 3-3 *Example of Global Dashboard*



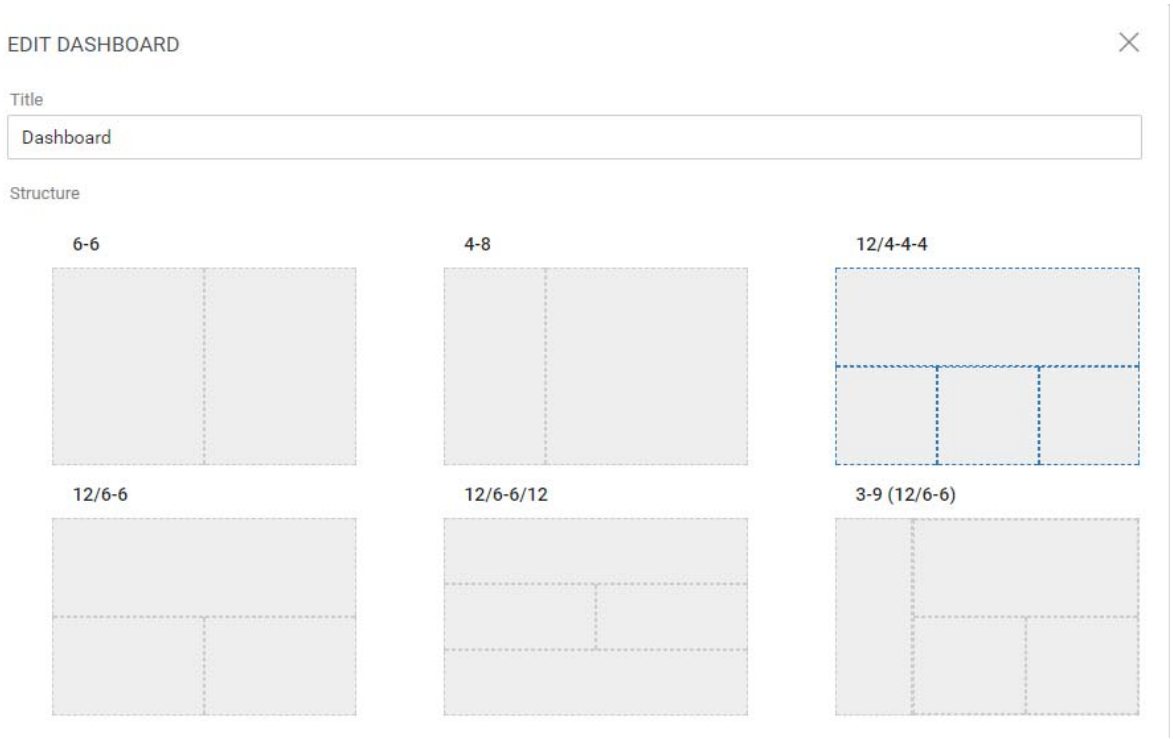
The administrator can add any user, group, container or role as a trustee to manage the global dashboard. To modify trustees to manage dashboard, go to **YourID** > **Settings** > **Access** and click **Global Dashboard** from the list. For more information about modifying configuration access, see Managing Dashboard Widgets in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Changing the Dashboard Layout

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

1. In **Dashboard** and click ∘∘∘.
2. Select **Layout**.
3. Choose the layout that you wish to see on your dashboard.

Figure 3-4 *Change Layouts*



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

Adding a Widget

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

Figure 3-5 *Add Widgets*

Add General Widgets

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

1. Select any of the following widget types from the list:
   - **Line Chart:** Displays the requested information for the selected element in the form of the line chart.
   - **Links:** Allows you to bookmark frequently used links that help you to access them quickly.
   - **Pie Chart:** Displays the requested information for the selected element in the form of the 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"
                }
```

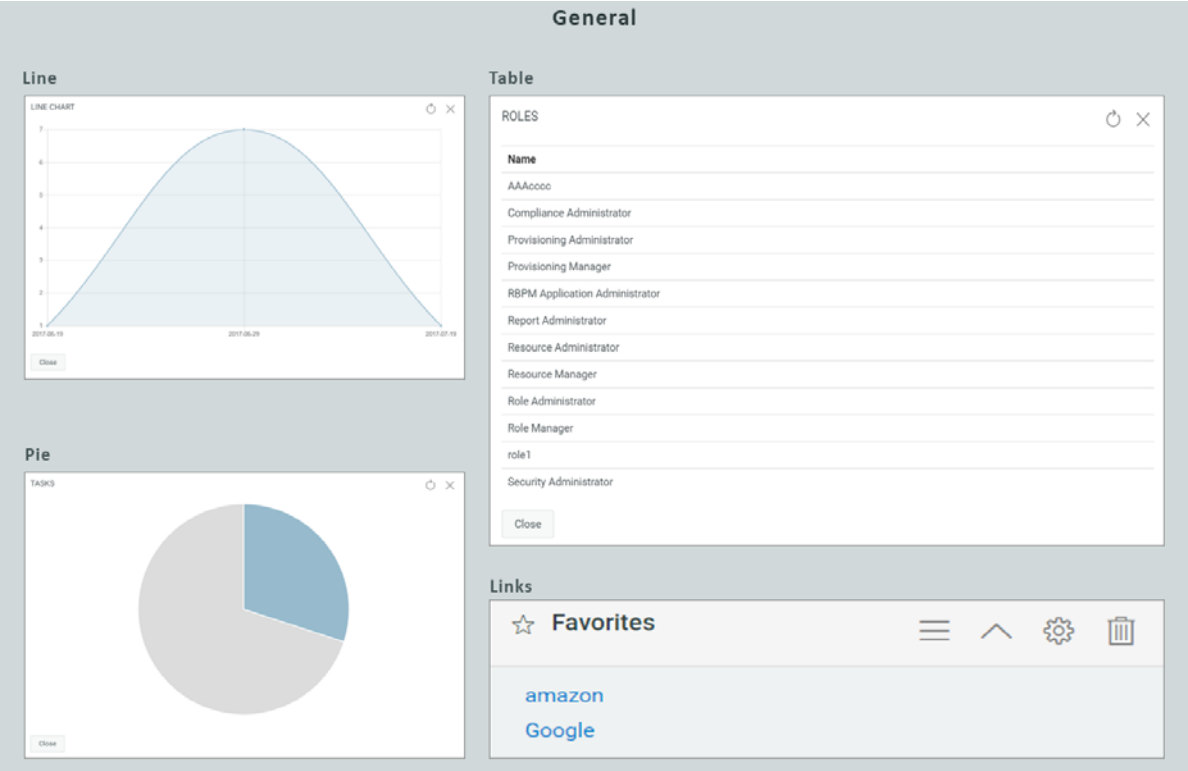
In this sample, `assignments` is the Root element and `name` is the selected column to display that will be displayed on the widget. You can also bookmark any URL that you wish to access from your Dashboard

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 the sample chart and link widgets that can be added to your Dashboard:

Figure 3-6 *Example for General Widgets*



Add Identity Manager Widgets

The **IDM** category allows you to add standard 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 the count of pending and denied requests of other users and allow you to create a request for these users.
- **Self Requests:** Displays the count of pending and denied requests count and also allow you to create a new request.
- **Tasks:** Displays the count of new, pending tasks, or the tasks that are about to expire.

To configure these widgets, see "Configuring a Widget" on page 31.

IMPORTANT: To apply your changes, click Save.

Add Identity Governance Widgets

To use Identity Governance widgets, you must install and configure Identity Governance with Identity Manager Dashboard.

IG category allows you to add standard Identity Governance widgets to your Dashboard. For example:

Fulfillment Tasks

Displays the count of access requests, business roles, and permission assignment errors in the system.

Review Tasks

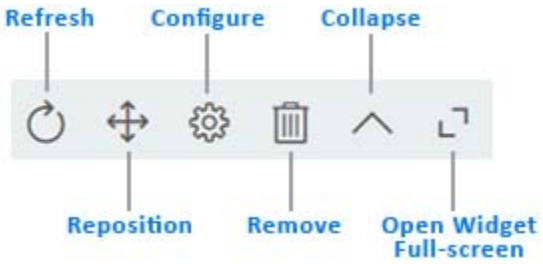
Displays the count of pending and completed reviews in the system.

SoD Violations

Displays the count of not reviewed, approved, or resolving SoD violations in the system.

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 "Configuring a Widget" on page 31.

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 the widgets that belong to **General** category.

- To apply your changes, click **Save**.

Configuring a Widget

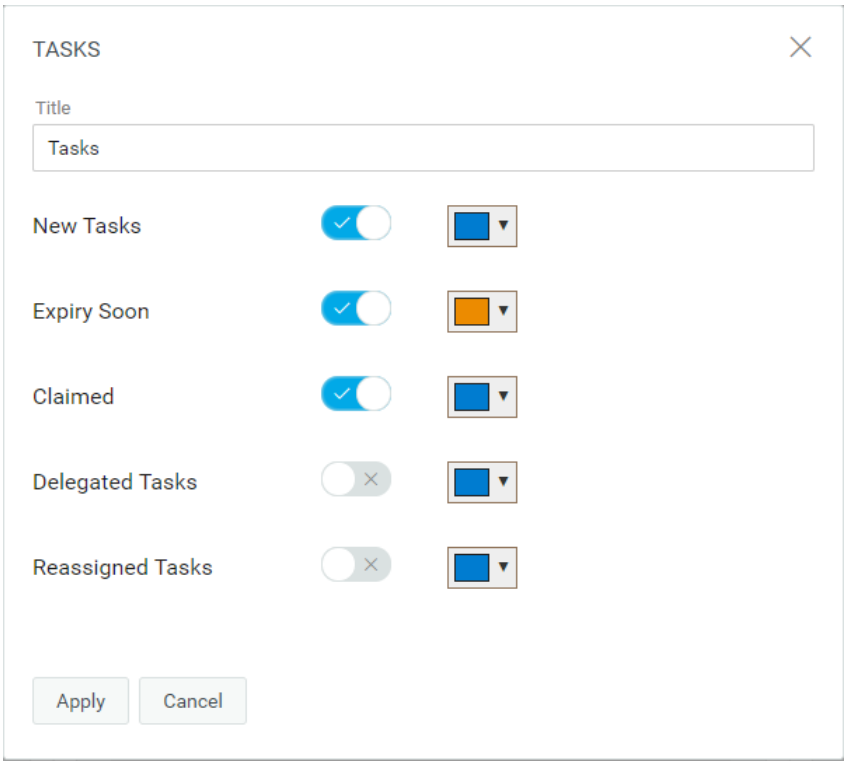
You can configure each widget that is added to your Dashboard. For example, you can enable or disable the fields of a widget or change the display color of the fields.

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

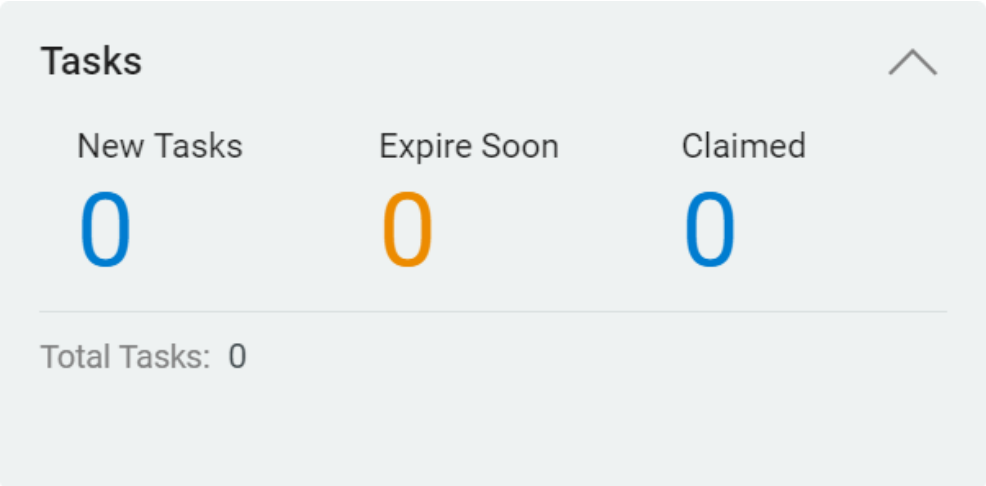
   For example, you can change the title of a widget, or change the color of a label for a widget field. You can also enable or disable a widget field in the properties page.
3. Click **Apply** to view the changes on the dashboard.

For example, you can modify the task widget as shown below:

Figure 3-7 *Example for Widget Configuration*



Click **Apply** to view the changes on the Dashboard.



To configure General widgets, modify the options that are displayed while adding widgets. See "Add General Widgets" on page 28.

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

III Managing Your Permissions and Identity Profile

Identity Manager Dashboard helps you request access to the resources and roles that you need to complete your daily tasks. You can also act on any tasks assigned to you in the Identity Manager environment, such as approving requests for access. Owners of resources and roles can manage the process.

When you request a permission, Identity Manager initiates a process to efficiently review your request so you can have the role or resource that you need. Your manager receives a notification either in email or on the Dashboard to review your request. In some cases, your request might also be approved by other individuals in your organization.

Some users can also make requests on behalf of others or act as a proxy for another user.

- Chapter 4, “Managing Your Permission Requests,” on page 35
- Chapter 5, “Managing Applications,” on page 41
- Chapter 6, “Managing Your Tasks,” on page 45
- Chapter 7, “Acting on Behalf of Someone Else,” on page 49
- Chapter 8, “Managing Delegations,” on page 51
- Chapter 9, “Managing Your Availability,” on page 53
- Chapter 10, “Managing Your Profile,” on page 55
- Chapter 11, “Managing the Organization Chart,” on page 57
- Chapter 12, “Managing Your Password,” on page 65

4 Managing Your Permission Requests

This section provides guidance for the following activities:

- "Viewing Your Permissions" on page 35
- "Requesting Permissions" on page 37
- "Viewing Requests" on page 37
- "Revoking Permissions" on page 39
- "Deep Linking to a Request" on page 40

You can also review ⓘ for information about the Dashboard for these activities.

Viewing Your Permissions

Permissions represent the accounts, roles, or resources that are available to you. Permissions may be assigned automatically to you by your organization or you can request for specific permissions. You can also inherit some permissions indirectly through role relationships or if you are a member of a group or a container.

To view the roles and resources to which you have access, on the Dashboard select:

Access > Permissions

You can then select a specific permission for further details on that role or resource. The permission might also list any reasons provided for the permission assignment. To find a particular permission in a large list, type the name, CN, or description of the permission in the Search box. You can also filter the list.

NOTE:

- By default, you can see the lists of permissions that are assigned or approved to you directly. However, it may vary depending on how the administrator has configured the settings for the page. For more information, see User Settings in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.
- To see the child permissions mapped with the assigned or approved permissions, click ⊜.

Viewing the Permission Details

Select the permission for which you want to view more details. The following table lists the fields displayed for individual permission:

Table 4-1 Permission fields and its description

Fields	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.
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.

If you are an identity applications Administrator, you can see the permissions of other team members in the **Others** tab. Go to the **Others** tab and search by user name or permission details.

- Searching by User will list all the assigned permissions of that user. You can then select a specific permission to review the details such as the date assigned, who assigned the permission, and if any reason has been provided for the permission assignment. For more information, see the Table 4-1 on page 36.
- Searching by Permission will list all users, individual as well those present in a group or container, who are assigned to that permission.

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.

For more information, click ⓘ on the Dashboard.

Requesting Permissions

To request roles and resources, click **Access** > **Requests**

Before requesting permissions, review the following considerations:

- You might be able to request access on behalf of another user. For example, if you are a team manager, you usually can act on behalf of team members. The process is the same, except you must specify that the request is for **Others** instead of **Self**.
- Do not use punctuation when specifying a permission that you want to request. If the name of the permission you want to request includes punctuation, omit the punctuation when searching.
- Different permissions require different information, depending on how the administrator has configured the permission form. If the permission requires detailed information, the Dashboard redirects you to a separate window when you select the permission.
- You can request multiple permissions at the same time.

  However, if the permission form for one of the requests requires special types of information, you might not be able to include that permission in a multi-permission request. To request multiple permissions at once, the request forms for the various requests cannot require detailed information.
- You can specify the expiry date while requesting for a resource or a role.

To request Identity Governance Permissions:

Applies only on two conditions namely, when you have enabled the **Show IG Catalog in request page** *option in the* **Configuration** > **Identity Governance** *page and when you request permission for* **Self***.*

- **IDM Catalogs:** Lists all the available 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.

For more information, click ⓘ on the Dashboard.

Viewing Requests

To view the status of a request in progress and completed requests, in the Dashboard select:

Access > **Request History**

A team manager or supervisor can see the request history of other team members in the **Others** tab.

You can also raise a Helpdesk ticket for your pending requests.

- "Tracking a Request" on page 38
- "Canceling a Request" on page 38
- "Raising a Helpdesk Ticket" on page 38

For more information, click ⓘ on the Dashboard.

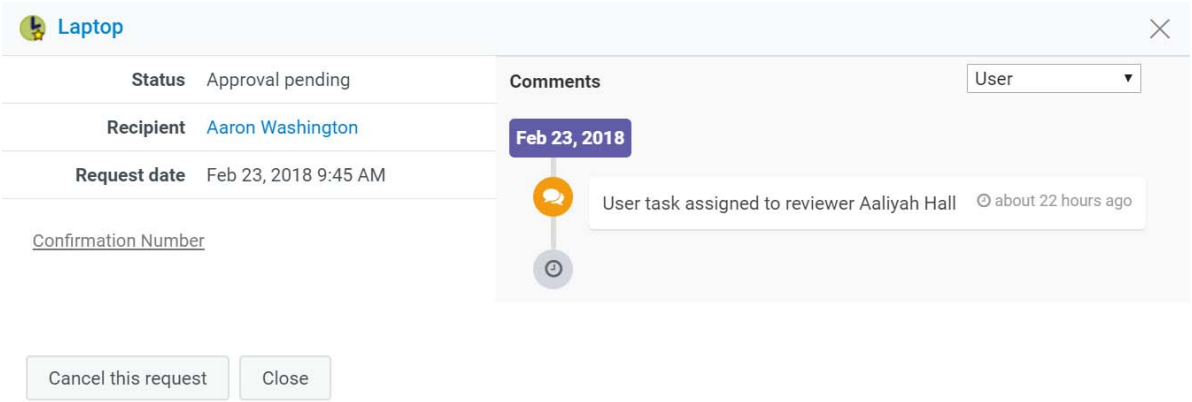
Tracking a Request

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.

NOTE: If you request for applications or technical roles from the **IG Applications** or **IG Technical Roles** tabs, such requests cannot be tracked through the **Request History** page. To track the IG requests, you can add the IG history URL from the **Applications** page of the Dashboard.

To track a pending request, select the request, then change the upper-right menu to **User and System**. The Dashboard shows the current state of the request in the approval process.

Figure 4-1 *Tracking a Request*



Canceling a Request

You can cancel a *pending* request from **Request History**. Select the request in the list, then select **Cancel this request** on the subsequent window.

Raising a Helpdesk Ticket

You can contact the Helpdesk if you are seeking help for any unattended requests for a long time.

You can raise a Helpdesk ticket in the following places:

- **Access** > **Request**, click **Helpdesk Ticket**.
- **Applications**, click **Helpdesk Ticket**.
- **Access** > **Request History**, click on the request that you want to raise a helpdesk ticket.

  For more information, click ⓘ on the Dashboard.

Helpdesk members receive a notification about the helpdesk ticket. You will get the notification on your ticket, after the ticket is resolved or closed.

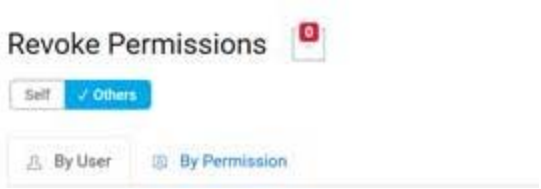
Revoking Permissions

If you no longer need access to a role or a resource, you can revoke the permission to that role or resource. To revoke a permission, navigate to **Access** > **Permissions** and select the required permission and specify a reason for revoking the permission.

You can also revoke a permission on behalf of other users. For example, if your team member has moved from Department 1 to Department 2, and the team member does not need access to a particular resource any longer, Identity Manager provides the facility to revoke the permission for that user. To revoke a permission, select **Others** and remove the permission. You can revoke multiple permissions at one time.You can add these permission to a queue for reviewing them before deciding to revoke them.

Only the administrator and a team manager can revoke permissions for other users. An administrator can revoke permissions for any user in the organization while a team manager can revoke permissions only for his team members.

You can revoke permissions for other users through the following ways:

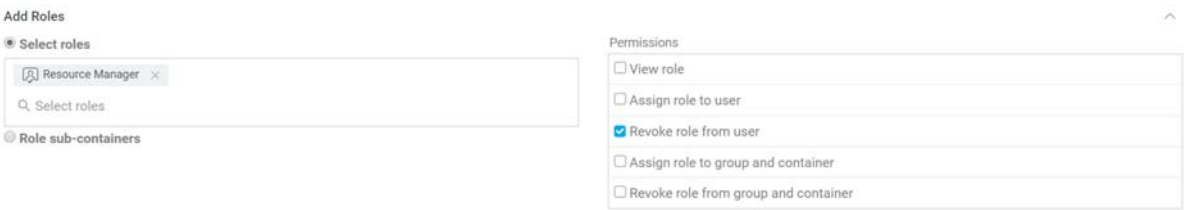


- **Search by user:** Allows you to search for a user and revoke permissions for that user. You can directly revoke a permission for the user or add the permission to a queue. A queue is a persistent work area where you can temporarily store permissions that you can review and revoke if required. You can then search for other permissions that you want to revoke for that user and add them to the queue. This allows you to revoke all permissions at one time.
- **Search by permissions:** Allows you to search for a specific permission. If you select a permission, it will list all the users who have that permission. You can directly revoke the permission for the selected user or add this permission to a queue and revoke that permission for multiple users at one time.

Team Manager: If you are a team manager, you can revoke permissions of your team members in the **Others** tab. Ensure you have required permissions to revoke others permissions.

Administrator: If you are an administrator, you can add revoke permissions for a team manager. For example, if you want to add revoke a role from a user permission for a team manager. Go to **People > Teams**, edit the team permissions to enable revoke permissions for a team manager.

Figure 4-2 *Example to Add Revoke Permission for a Team Manager*



This option allows the team manager to revoke the selected role from the team members.

NOTE: If you revoke a permission, your permissions list might not immediately reflect the change. This may be because the permission is associated with a revoke process which can take time. Refresh the list to view the changes.

For more information, click ⓘ on the Dashboard.

Deep Linking to a Request

Identity applications lets you to deep link to a specific process request (also known as a provisioning request). This feature gives a manager the ability to send a specific process request URL to an employee, so this employee can request the process quickly without having to go through the Identity Manager Dashboard. When you deep link to a process request, the request form is displayed in the body of the page, along with the header for the Identity Applications.

When a permission is requested, the request appears in the **Access** > **Request History** page of the requester and also appears on the **Tasks** page of the reviewer.

The URL used for deep linking to a process request uses the following format:

- For legacy forms,

  ```
  https://<server:port>/IDMProv/
  requestForm.do?uid=<PRD_ID>&aqua=true&idmdash=true&recipient=<recipien
  t>&jsa=<operation_type>
  ```

  Here's an example that shows what the URL one might use to deep link to a provisioning request definition:

  ```
  https://testserver:8543/IDMProv/requestForm.do?uid=cn=request mobile
  approval app,cn=requestdefs,cn=appconfig,cn=user application
  driver,cn=driverset1,o=system&aqua=true&idmdash=true&recipient=&jsa=%7
  B%22submit%22%3A%22submitThenOpener%283000%29%22%2C%22cancel%22%3A%22w
  indow.close%28%29%22%7D
  ```

- For the new JSON forms,

  ```
  https://<server:form_renderer_port>/forms/#/form/
  details?id=<formID>&recipient=<recipient>&pid=<workflowID>&sid=IDM&uri
  =<forms_uri>&formContainer=RequestForms&locale=<language>
  ```

  Here's an example that shows what the URL one might use to deep link to a provisioning request definition:

  ```
  https://testserver:18600/forms/#/form/details?id=cn%3DHelp-
  desk%20Request%20Form,cn%3DWorkflowForms,cn%3Dappconfig,cn%3DUser%20Ap
  plication%20Driver,cn%3Ddriverset1,o%3Dsystem&recipient=&pid=cn%3Dhelp
  deskticket,cn%3Drequestdefs,cn%3Dappconfig,cn%3Duser%20application%20d
  river,cn%3Ddriverset1,o%3Dsystem&sid=IDM&uri=%2Frest%2Faccess%2Fforms&
  formContainer=RequestForms&locale=en
  ```

5 Managing Applications

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 **Editing done** to return to **Applications**.

Creating Featured Items

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

1. (Conditional) To create a new item, click **+** on **Applications** or **Permissions** tab.
2. Complete the form for an application or a permission. See "Adding an Application" on page 41 or "Adding a Permission" on page 42.

   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.

Adding an Application

To add an application, specify the following details:

(Conditional) Add to Category

Specifies the category for this application.

Name

Specifies the name of the application.

Description

Specifies the nature of the application.

(Optional) Image

Specifies a logo or image for an application.

Link

Specifies a link for this application. See "Deep Linking to a Request" on page 40.

(Optional) API URL

Specifies the URL of the REST endpoint with JSON data that provides extra details, such as the value of parameters and a badge. Refer documentation for more details.

Adding a Permission

To add a permission, specify the following details:

Permissions

Specifies the permission. This can be a role, resource, or PRD.

(Conditional) Add to Category

Specifies the category for this application.

(Optional) Image

Specifies a logo or image for an application.

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**.

   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.

6 Managing Your Tasks

If you are responsible for approving or denying requested permissions in Identity Manager, you can use the Dashboard to manage your tasks as you might have previously done in the User Application. You can approve or deny requests one at a time, or you can approve or deny multiple simple requests that do not require detailed information in bulk.

To review pending requests, click **Tasks**.

Alternatively, you might receive an email notification with a link that allows you to approve or reject a request in a response email.

Before acting on user requests, review the following considerations:

- You can multi-select tasks for a batch approval/denial.
- For a more complex request that requires detailed information, the Dashboard does not display a check box. You must approve or deny those requests by selecting each request and completing the forms.
- 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.
- In general, you must provide a comment explaining why you want to approve or deny the selected tasks.

Viewing your Tasks

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

If you are serving as a proxy or delegate for others tasks, you can complete tasks that are assigned to someone else. For more information about proxy assignments and delegation assignments, see Acting as 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 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.

At times, you might need 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.

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**.

Release Request

If you do not want to act on the request that you have claimed, you can release that request.

Reassign Request

A task that is assigned to you can be reassigned to other user in the organization. The following considerations apply to reassigning tasks:

- If you are unable to complete the task, you can reassign it to your manager. Select the request under the **Self** tab and then select **Reassign**. The task is automatically reassigned to your manager.
- 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 the **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.

- If you have not acted on the task in the specified time frame, the following actions can occur:
  - An administrator can reassign the task to another user. An administrator has a permission to reassign a task to any user in the organization.
  - Team Manager can reassign the task to another member in the team. Ensure that team manager is enabled with Manage Addressee Task permission at the time of team creation.

    This applies only when **Members** option is used to add members to the team at the time of team creation. For more information, see "Create a Team" on page 78

    NOTE: If you use **All Users** or **Relationship** option to create a team, the team manager cannot reassign the tasks to another member in the team.

  - The Helpdesk user can reassign the task to your manager up to the hierarchy level defined in the **Settings** page. Administrator configures the manager hierarchy.

If a task is reassigned to you and you are unable to take it, you can return the task to the user who assigned the task to you.

Return Request

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

NOTE: Only a reassigned request can be returned.

For more information, click ⓘ on the Dashboard.

Managing Helpdesk Tasks

Helpdesk tasks are generated for every helpdesk ticket raised in the system. According to example in "How Helpdesk Works?" on page 16, Emily's ticket creates a helpdesk task in Helen's **Tasks** page. Helen can take appropriate actions for this helpdesk task.

If you are a helpdesk user, select the Helpdesk Ticket that requires your action. Perform any of the following actions on the selected helpdesk ticket:

Update

Updates the helpdesk ticket with an appropriate comment.

Complete

Completes the helpdesk ticket enclosed with your resolution comment.

Cancel

Closes the helpdesk ticket with an appropriate comment.

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.

For more information, click ⓘ on the Dashboard.

7 Acting on Behalf of Someone Else

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.

- "Viewing Your Proxy Assignments" on page 49
- "Acting as a Proxy" on page 49
- "Managing Proxy Assignments" on page 49

For more information, click ⓘ on the Dashboard.

Viewing Your Proxy Assignments

To view your proxy assignments, in the Dashboard select:

Access > **Proxy Assignments**

Acting 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.

Your ID > **Proxy As**

For example, Sarah Smith manages Customer Relations. The identity applications includes a Customer Relations team with Sarah Smith as the Team Manager. She can act on behalf of Maria Belafonte who is a member of her team. In the Dashboard, she selects **ssmith** > **Proxy As**, then specifies **mbelafonte**.

Managing 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. The team manager can create assignments for team members only.

8 Managing Delegations

In some organizations, delegating tasks to another user is allowed. If you are a delegate for other's tasks or your tasks are delegated to other users in the organization, you can see the delegation information in **Administration** > **Delegation**.

You can see the delegated tasks in the **Tasks** page. The tasks with icon indicates that task is delegated.

IMPORTANT: Creating delegation assignment also requires you to specify your availability details. You can either provide your availability details while creating the delegation assignment or create delegation and then specify availability details in a separate action. This depends on whether the administrator has enabled the required settings, in which case you see the **Unavailable From** option in the **Create Delegate Assignment** page. However, if you are unable to see the **Unavailable From** option, you must specify your availability details from the **Availability Settings** page after creating the delegation assignment. This ensures that the delegation functions as expected. For more information, click on the Dashboard.

---

9 Managing Your Availability

You can specify which resource 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.

To view your availability, in the Dashboard select

People > Availability

Before using the **Unavailable From** action, you need to have at least one delegate assignment to work on. You need to have your team manager (or the Provisioning Application Administrator) create delegate assignments for you.

The global settings pertaining to availability-based delegation are specified by **Set Availability while creating a Delegation Assignment** in **Settings > Customization > Navigation Items > General**. 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.

For more information, click ⓘ on the Dashboard.

10 Managing Your Profile

The identity applications give you a convenient way to display and work with your identity information. They also enable your organization to be more responsive by giving you access to the information about other users that you need whenever you need it. For example, you might want to:

- Manage your own user account directly
- Look up other users and groups in the organization on demand
- Visualize how those users and groups are related
- List applications with which you are associated

Your system administrator is responsible for setting up the contents of the identity applications for you and the others in your organization. What you can see and do is typically determined by your job requirements and your level of authority.

Updating Your Profile

To view or update your identity profile, in the Dashboard select:

[your ID] > **My Profile**

Or,

Click on your dashboard.

This page lists your reporting manager, roles, resources, and group. You should have administrator access to edit your information or to view your organization chart.

Your profile includes settings such as your name, email address, and phone number. This page displays the user attributes that are enabled with **Search** and **Read** accesses, these access properties can be configured in Directory Abstraction Layer (DAL). For more information, see Attribute Properties in the *NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications*. Your organization determines which settings you can modify. For example, you might be able to change your phone number but not your last name.

11 Managing the Organization Chart

The Identity Manager Dashboard gives you a convenient way to search for an entity in your organization and view its organization chart (an entity can be a user, group, or custom entity defined by your administrator). An organization chart shows the hierarchy of relationships, such as Manager-Employee, Group's membership, or User groups among entities in your organization.

By default, the **Organization Chart** page in the Dashboard shows the placement of a user entity within the organization and its relationship hierarchy with other user entities based on the organization chart relationship set by the administrator. For more information about default settings for organization chart page, see Customizing the Views. For more information about how to view organization chart of entities other than user entity, see Viewing the Organization Chart of an Object in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

The organization chart is often referred as "org chart". You may find both these terminologies used in the Dashboard.

Viewing an Organization Chart

By default, Security Administrator and Provisioning Administrator can view the organization chart for all the entities in the system.

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

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

  To find the organization chart of other users in the system, type the name of other users in the search bar provided in the **Organization Chart** page.

- Go to **People** > **Users** and select any user from the list and click that is beside the user name. For more information, see Chapter 13, "Managing Users," on page 73.

NOTE: You should have **Org Chart** access to view the **Organization Chart**. Contact your administrator to provide this access. For more information, see User Settings in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Understanding the Organization Chart

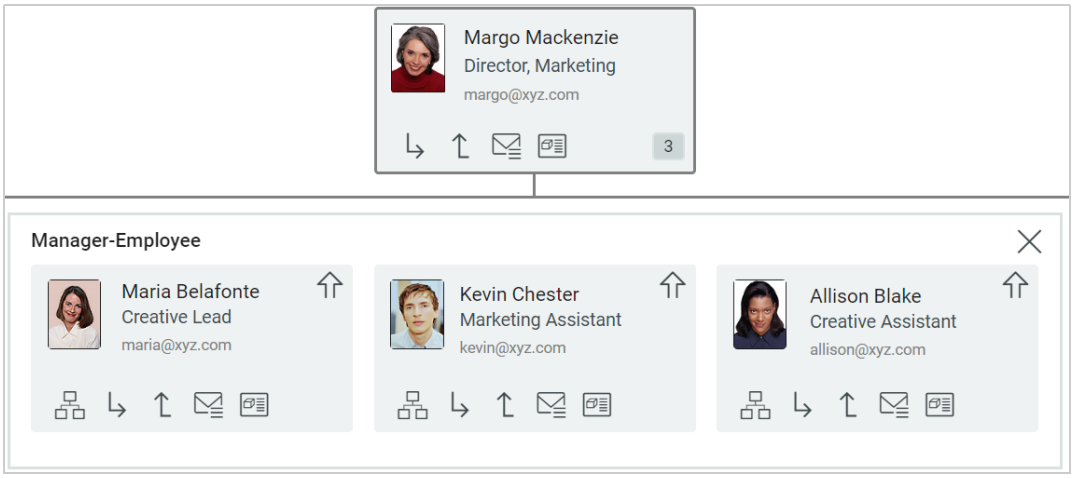
Organization chart displays the entity information in a card format. These cards are arranged in a hierarchical order based on the default organization chart relationship configured by your administrator. A root or selected entity that is displayed on the top is the starting point or orientation point in the organization chart and the child entity directly under the root entity is displayed at the bottom based on the default relationship.

Each card displays information based on the primary and secondary attributes defined by your administrator. For more information about how these attributes can be customized, see Customizing the Organization Chart View in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*. For a user entity specifically, the card is set to display the full name of the user in addition to the primary and secondary attributes defined by the administrator. As a result, when the administrator configures the first name and last name as primary attributes, the full name of the user may appear twice in the **Card View** on the **Users** page and in the organization chart.

NOTE: In the organization chart view, if the primary and secondary attributes of an entity are not defined by the administrator, then the Identity Applications display the CN attribute of that entity in the **Organization Chart** page.

Figure 11-1 shows an example of organization chart for the user *Margo Mackenzie* where the default organization chart relationship is set to Manager-Employee.

Figure 11-1 *Example of the organization chart on the Dashboard*



In this example, *Margo Mackenzie* is the manager, and *Maria Belafonte*, *Kevin Chester*, and *Allison Blake* are employees who report to her. Each card is displaying the user's full name on top, which in Margo's case is *Margo Mackenzie*, followed by the role in the organization and email address that are set as primary and secondary attributes by the administrator. The count at the bottom-right corner of *Margo Mackenzie*'s card signifies the number of employees who report to her.

Working with the Organization Chart

Based on the search input entered in the **Organization Chart** page, the Dashboard displays the organization chart of the entity. You can perform other tasks on the page such as view other relationships of the entity, change the root entity and view its organization chart, or view the organization chart of an entity at next level in the relationship hierarchy.

To understand more about the tasks that you can perform in the **Organization Chart** page, let us consider the following example of a marketing team in the XYZ company:

Margo Mackenzie is the Director in marketing team where *Allison Blake*, *Kevin Chester*, and *Maria Belafonte* are employees who report to her. *Margo Mackenzie* reports to *Timothy Swan,* the Vice President of the Marketing team.

Go to **People** > **Organization Chart** in the Dashboard and search for *Timothy Swan* to view his organization chart. Similarly, perform a search for *Margo Mackenzie*. Figure 11-2 and Figure 11-3 shows you their individual organization chart based on the Manager-Employee relationship.

Figure 11-2 *Organization chart of Timothy Swan in the role of Manager.*

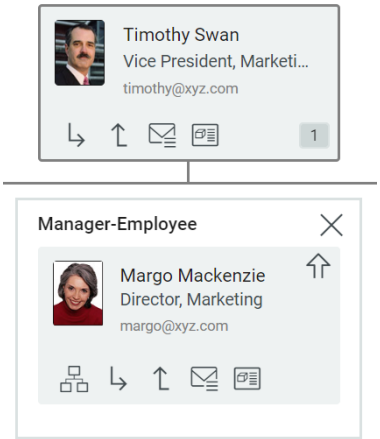
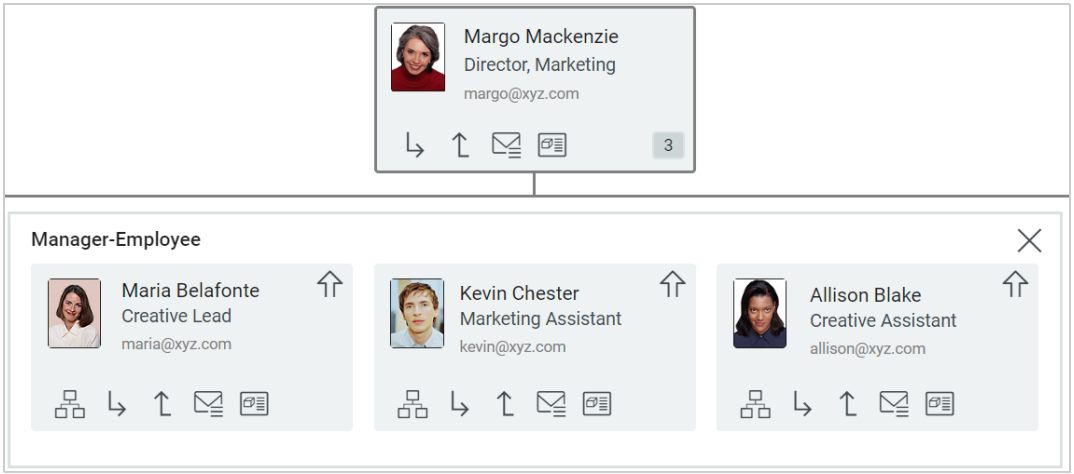


Figure 11-3 *Organization chart of Margo Mackenzie in the role of Manager.*



Let us look at the tasks that you can perform in the **Organization Chart** page based on the above example:

- "Reset the Root in the Organization Chart View" on page 60
- "Switch the Organization Chart view" on page 60
- "Choose a Relationship to View" on page 61
- "Navigate to the Next Level in Relationship Hierarchy" on page 62
- "Send Email to Users from the Organization Chart" on page 63
- "View Detailed Information of a User" on page 63

NOTE: The above tasks are applicable to both user and custom entities.

Reset the Root in the Organization Chart View

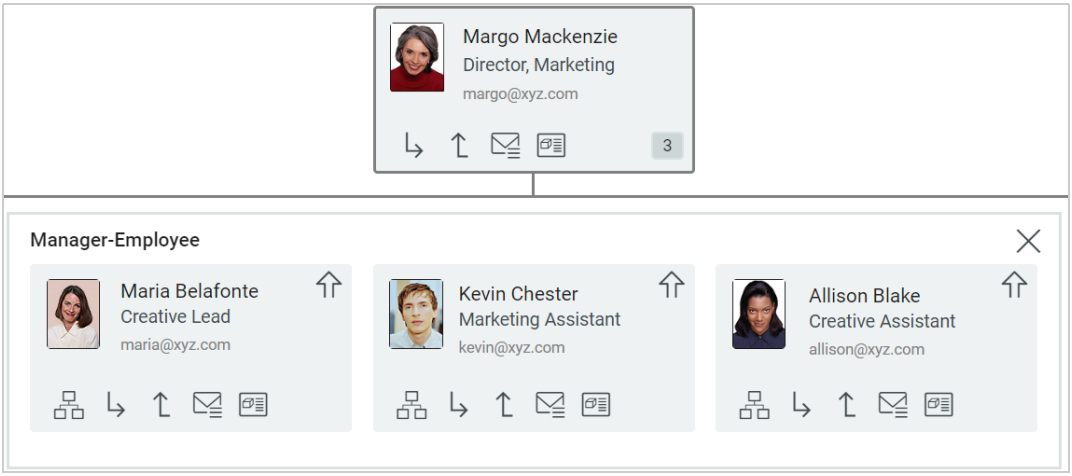
To reset the root user in your organization chart view,

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

   Suppose you are viewing the organization chart where *Timothy Swan* is in the role of Manager and you want *Margo Mackenzie* as the new root.

2. Go to *Margo Mackenzie's* card and click icon. She becomes the new root and is now at the top in the Manager-Employee organization chart. The employees who reports to *Margo Mackenzie* namely *Maria Belafonte*, *Kevin Chester*, and *Allison Blake* are listed under her.

   Figure 11-4 *Margo Mackenzie as new root in the organization chart view*



Switch the Organization Chart view

To reset the root user and the default relationship in your organization chart view, perform the following actions:

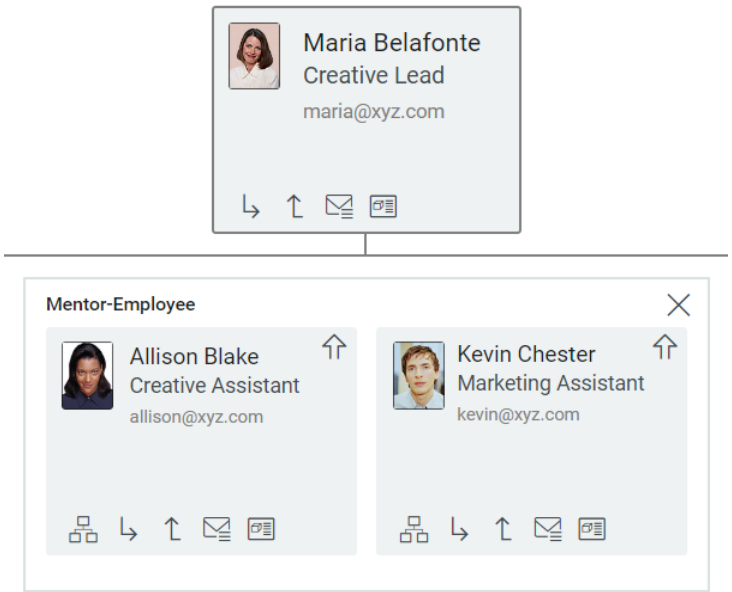
1. Identify the user whose organization chart you want to view.

Suppose you are viewing the organization chart where *Margo Mackenzie* is in the role of Manager. *Maria Belafonte*, the employee under *Margo Mackenzie* is also a mentor to *Kevin Chester* and *Allison Blake*. You want to view the Mentor-Employee relationship of *Maria Belafonte*.

2 Go to *Maria Belafonte's* card and click .

3 From the drop-down menu, select the relationship as **Mentor-Employee**. *Maria Belafonte* becomes the root of the Mentor-Employee organization chart and *Kevin Chester* and *Allison Blake* are listed as employee under her.

Figure 11-5 *Organization chart of Maria Belfonte in the role of Mentor*



Choose a Relationship to View

To view relationships of a user other than the default, perform the following actions:

1 Identify the user whose relationship you want to view.

Suppose you are viewing the organization chart where *Margo Mackenzie* is in the role of Manager. You want to view the user group relationship of *Maria Belafonte* who is a part of Marketing group.

2 Go to *Maria Belafonte's* card and click .

3 From the drop-down menu, select the relationship as **User groups**. *Maria Belafonte's* group membership chart is added inline in the existing organization chart view.

NOTE: The maximum level to which you can expand the organization chart of a user and view the relationships inline is defined by the administrator. By default, you can expand up to level 3, wherein level 1 is always assigned to the root user.

Navigate to the Next Level in Relationship Hierarchy

To understand this task, let us consider second example of *Edward Miller* who is the Director in sales team. *Allison Blake* and *Filla Martell* are the direct reports to *Edward Miller*. As you can see, *Allison Blake* is a common member of sales and marketing team and reports to two managers, namely *Edward Miller* and *Margo Mackenzie*.

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.

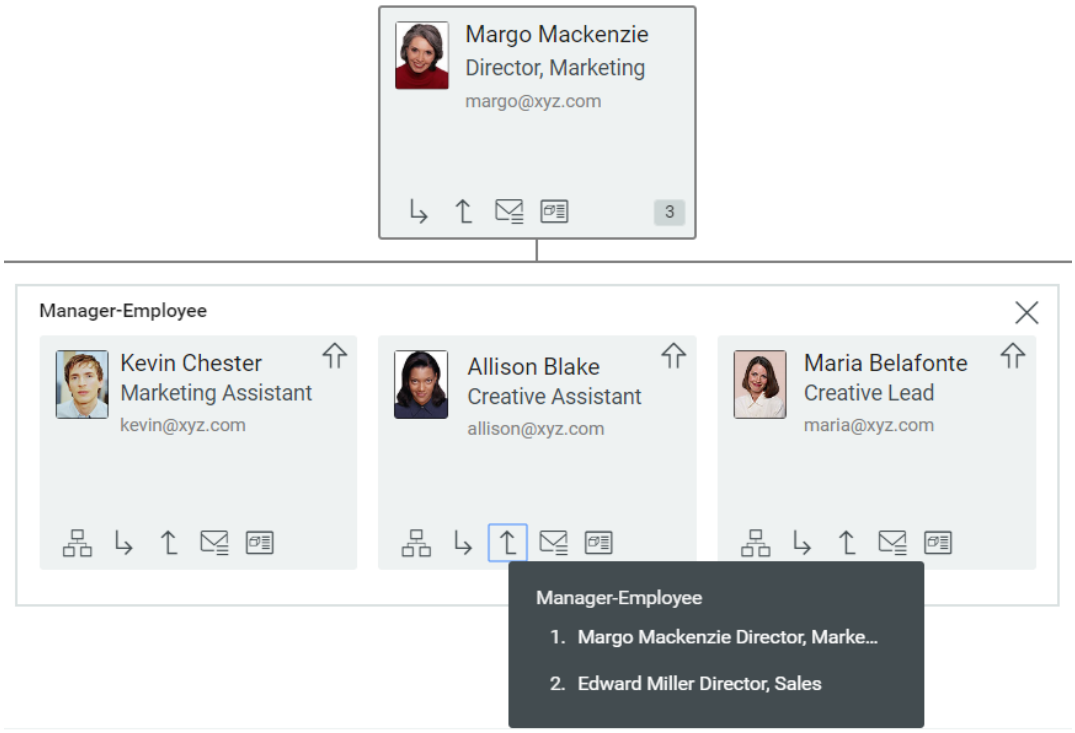
   Suppose you are viewing the organization chart where *Margo Mackenzie* is in the role of Manager and you want to view the organization chart of *Allison Blake*.

2. Go to *Allison Blake's* card, click and select the recursive Manager-Employee relationship from the list.

3. Click .

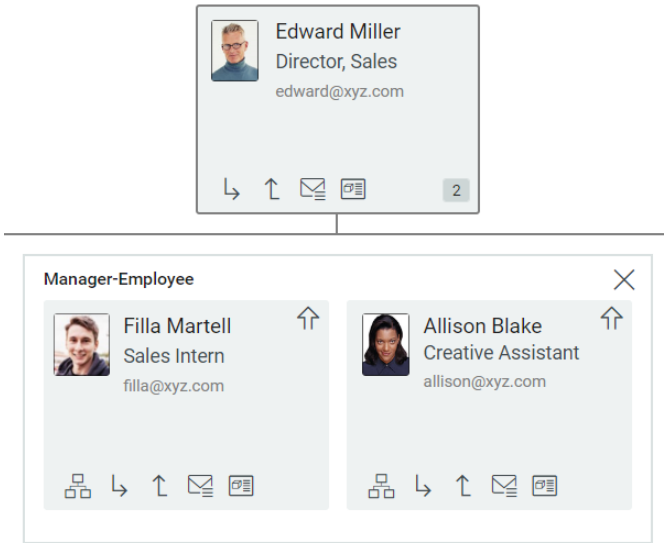
   In the Manager-Employee drop-down menu, the employee *Allison Blake* displays two managers namely *Margo Mackenzie* and *Edward Miller* whom she reports to.

   Figure 11-6 *Recursive Manager-Employee relationship of Allison Blake*



4. Select the manager, *Edward Miller*. The organization chart of the *Allison Blake* is displayed.

Figure 11-7 Organization chart of Allison Blake



Send Email to Users from the Organization Chart

Using option, you can:

- Send an email to the selected user.
- Share the profile link of an entity over email.
- (Optional, only applicable to the Manager-Employee relationship) Send an email to all team members under the selected user.

For more information, click on the Dashboard.

IMPORTANT:

- Before sending an email from the organization chart view, you must ensure that a default email client is configured in your system.
- To ensure that the **New Email** and **Email Team** options work, configure the Email attribute as a primary or secondary attribute on the Settings page. For more information, see User Settings in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

View Detailed Information of a User

1 Identify the user whose information you want to view.

   Suppose you are viewing the organization chart where *Margo Mackenzie* is in the role of Manager and you want to view additional details such as the roles and resources assigned to *Kevin Chester*.

2 Go to *Kevin Chester*'s card and click icon. The profile page displays a detailed information including the roles and resources assigned to him.

If you cannot see icon on a user's card, for example *Jack Miller's* card, who is the President of XYZ organization, it indicates that you do not have appropriate permissions to the user catalog and therefore cannot view his profile. Contact your administrator if you require the necessary access to view a profile.

For more information, click on the Dashboard.

12 Managing Your Password

Identity Manager includes Self Service Password Reset (SSPR) to help you manage the process for changing passwords and resetting forgotten passwords. During password reset, SSPR uses a challenge-response authentication method to authenticate the you.

- "Using Self-Service Password Management in Identity Manager" on page 65
- "Using the Legacy Password Management" on page 67

NOTE: This section describes the default features of the managing your password. You might encounter some differences because of your job role, your level of authority, and customizations made for your organization; consult your system administrator for details.

Using Self-Service Password Management in Identity Manager

SSPR automatically integrates with the single sign-on process for the identity applications and Identity Reporting. It is the default password management program for Identity Manager. When a user requests a password reset, SSPR requires the user to answer the challenge-response question. If the answers are correct, SSPR responds in one of the following ways:

- Allow users to create a new password
- Create a new password and send it to the user
- Create a new password, send it to the user, and mark the old password as expired.

You configure this response in the SSPR Configuration Editor. After upgrading to a new version of Identity Manager, you can configure SSPR to use the NMAS method that Identity Manager traditionally used for password management. However, SSPR does not recognize your existing password policies for managing forgotten passwords. You also can configure SSPR to use its proprietary protocol instead of NMAS. If you make this change, you cannot return to using NMAS without resetting your password policies.

You can use SSPR to do any of the functions listed in Table 12-2, "Password Management Functions," on page 68:

Table 12-1 Password Management Functions

This Password Management page	Enables you to
Password Challenge Response	Set or change either of the following: ◆ Your valid responses to administrator-defined challenge questions ◆ User-defined challenge questions and responses
Change Password	Change (reset) your password, according to the rules established by your system administrator
Password Policy Status	Review your password policy requirements.

Understanding Password Challenge Response

Challenge questions are used to verify your identity during login when you have forgotten your password. If the system administrator has set up a password policy that enables this feature for you, you can use the Password Challenge Response page to:

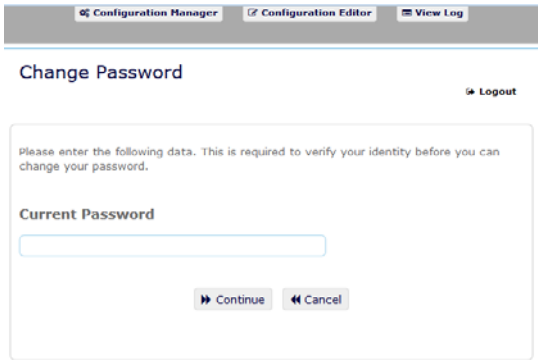
- Specify responses that are valid for you when answering administrator-defined questions
- Specify your own questions and the valid responses for them (if your password policy enables this)

During the login process, the login page automatically redirects you to the Challenge-Response page. You set up the responses for challenge questions on this page. For more information, see "If You Forget Your Password" on page 22. When you log in again and try to reset the forgotten password, SSPR prompts the configured questions and asks you to specify the correct answer. When the answer matches with the response that you had saved earlier, SSPR allows you to reset the password.

Changing Your Password

You can change your password (providing that the system administrator has enabled you to do so).

1. In the Dashboard, click **Applications > Change My Password**.
2. Type your current password. The Change Password page displays.



3. Type your new password in the **New Password** text box.

4 Type your new password again in the **Confirm Password** text box.

5 Click **Change Password**.

If your new password violates any of the password rules defined in the password policy by your administrator, you will see an error message on the Change Password page.

This page typically provides information about how to specify a password that meets the policy's requirements as defined by your administrator. Review the password rules, and try again.

6 Click **Continue**. The status of your request is displayed. On success, it takes you back to the OSP login page.

Password Policy Status

NOTE: This feature is only available for administrator users.

You are assigned a password policy by your administrator. The policy determines the security measures associated with your password. You cannot check your password policy requirements unless the User Application administrator has provided you with rights to do so. The User Application administrator can check the status of password policy on the Identity Manager Home page. This link does not exist by default. You need to customize the Home page to include it. For customizing the default Identity Manager Home items, see Chapter 5, "Managing Applications," on page 41.

On the landing page, click **Password Status and Policy** link. The **Password Policy Status and Policy** page displays. To change your Identity Manager password, go to Identity Manager Home and select Change My Password. The Identity Manager Home link redirects you to the Change Password area of SSPR.

Using the Legacy Password Management

This section tells you how to use the Password Management pages on the **Identity Self-Service** tab of the Identity Manager User Application. Topics include:

- "Password Challenge Response" on page 68
- "Password Hint Change" on page 69
- "Change Password" on page 69
- "Password Policy Status" on page 70
- "Password Sync Status" on page 70

NOTE: This section describes the default features of the Password Management pages. You might encounter some differences because of your job role, your level of authority, and customizations made for your organization; consult your system administrator for details.

For more general information about accessing and working with the **Identity Self-Service** tab, see Chapter 10, "Managing Your Profile," on page 55.

You can use the Password Management pages to do any of the functions listed in Table 12-2, "Password Management Functions," on page 68:

Table 12-2 Password Management Functions

This Password Management page	Enables you to
Password Challenge Response	Set or change either of the following: ◆ Your valid responses to administrator-defined challenge questions ◆ User-defined challenge questions and responses
Password Hint Change	Set or change your password hint
Change Password	Change (reset) your password, according to the rules established by your system administrator
Password Policy Status	Review your password policy requirements.
Password Sync Status	Display the status of synchronization of application passwords with the Identity Vault **NOTE:** Accessing applications prior to completion of synchronization causes application access issues.

Password Challenge Response

Challenge questions are used to verify your identity during login when you have forgotten your password. If the system administrator has set up a password policy that enables this feature for you, you can use the Password Challenge Response page to:

- Specify responses that are valid for you when answering administrator-defined questions
- Specify your own questions and the valid responses for them (if your password policy enables this)

To use the Password Challenge Response page:

1. On the **Identity Self-Service** tab, click **Password Challenge Response** in the menu (under **Password Management**).

   The Password Challenge Response page displays.

2. Type an appropriate response in each **Response** text box (they are all required), or use your previously stored response. When **Use Stored Response** is selected, the challenge answers, including the labels, are not shown. In addition, user-defined challenge questions are disabled.

   Make sure you specify responses that you can remember later.

3. Specify or change any user-defined questions that are required. You may not use the same question more than once.

4. Click **Submit**.

   After you save the challenge responses, the User Application displays a message indicating that the challenge responses were saved successfully and displays the challenge response screen again with "Use Stored Response?" selected.

Password Hint Change

A password hint is used during login to help you remember your password when you have forgotten it. Use the Password Hint Change page to set or change your password hint.

1. On the **Identity Self-Service** tab, click **Password Hint Change** in the menu (under **Password Management**).

   The Password Hint Definition page displays.

2. Type the new text for your hint.

   Your password cannot appear within the hint text.

3. Click **Submit**.

   The status of your request displays.

Change Password

You can use this page whenever you need to change your password (providing that the system administrator has enabled you to do so).

1. On the **Identity Self-Service** tab, click **Change Password** in the menu (under **Password Management**).

   The Change Password page displays. If the system administrator has set up a password policy for you, the Change Password page typically provides information about how to specify a password that meets the policy's requirements. For example:

   If no password policy applies, you'll see the basic Change Password page, which simply provides fields for changing your password.

   The User Application supports the following password syntax types:

   - Microsoft complexity policy

     This password syntax type is used for backward compatibility with Active Directory 2003.

   - Microsoft Server 2008 Password Policy

     This is a new password syntax type that has been added to eDirectory 8.8.7 to support Active Directory 2008.

     The following settings are supported with Microsoft Server 2008 Password Policy:

     - Use Microsoft Server 2008 Password Policy
     - Maximum number of complexity policy violations in password (0-5)

   - Novell syntax

     The following new settings are supported with the Novell syntax:

     - Minimum number of non-alphabetic characters (1-512)
     - Maximum number of non-alphabetic characters (1-512)

   For all three types password syntax types, the User Application supports the following features:

   - Number of characters different from current password and passwords from history (0-6)
   - Number of passwords in history to be considered for character exclusion (0-10)

   If your administrator has enabled the Microsoft Server 2008 Policy syntax, fill the following fields in the Change Password page:

2 Type your current password in the **Old password** text box.

3 Type your new password in the **New password** text box.

4 Type your new password again in the **Retype password** text box.

5 Click **Submit**.

If your new password violates any of the password rules defined by your administrator, you will see an error message on the Change Password page. If you are using Microsoft Server 2008 Policy, and your password is in violation, the user interface will show this message at the top of the page:

```
Password AD2008 complexity policy violation.
```

If your new password is in violation, review the password rules defined by your administrator, and try again.

6 You might be prompted to supply a password hint, if your administrator configured your security policy to do so. If so, see "Password Hint Change" on page 69.

7 The status of your request is displayed.

Password Policy Status

You are assigned a password policy by your administrator. The policy determines the security measures associated with your password. You can check your password policy requirements as follows:

1 On the **Identity Self-Service** tab, click **Password Policy Status** in the menu (under **Password Management**).

The **Password Policy Status** page displays.

Items labeled invalid are items that you cannot change.

Password Sync Status

Use the Password Sync Status page to determine if your password has been synchronized across applications. Access another application only after your password has synchronized. Accessing applications prior to completion of synchronization causes application access issues.

1 On the **Identity Self-Service** tab, click **Password Sync Status** in the menu (under **Password Management**).

The **Password Sync Status** page displays. Full-color icons indicate applications for which the password is synchronized. Dimmed icons indicate applications that are not yet synchronized.

NOTE: Only the administrator can see the **Select User** box.

IV Managing Users, Groups, and Teams

If you have the appropriate role in the identity applications, you can create and manage users, groups, and teams. You can create users and teams in dashboard and User Application. You create and manage groups in the User Application.

System administrators can create users and groups. The system administrator can give others (typically, selected people in administration or management positions) access to this functionality.

You might encounter some differences from functions documented in this section because of your job role, your level of authority, and customizations made for your organization. Consult your system administrator for details.

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. See Chapter 14, “Managing Teams,” on page 77.

13 Managing Users

This section tells you how to create users and groups in the Dashboard and User Application. Topics include:

- "Creating a User" on page 73
- "Editing User Information" on page 73
- "Listing Users" on page 74
- "Finding Users" on page 75
- "Sorting Users" on page 76

Creating a User

Create User page displays the user attributes that are enabled with **Search** and **Read** accesses, these access properties can be configured in Directory Abstraction Layer (DAL). For more information, see Attribute Properties in the *NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications*.

To create a user, in the Dashboard select:

People > **Users** > **+**

The identity administrator defines the values that you can specify for the user. Also, when creating a user, you can see the user **Container** but you cannot modify its value. This limitation ensures that all users are stored in the same container.

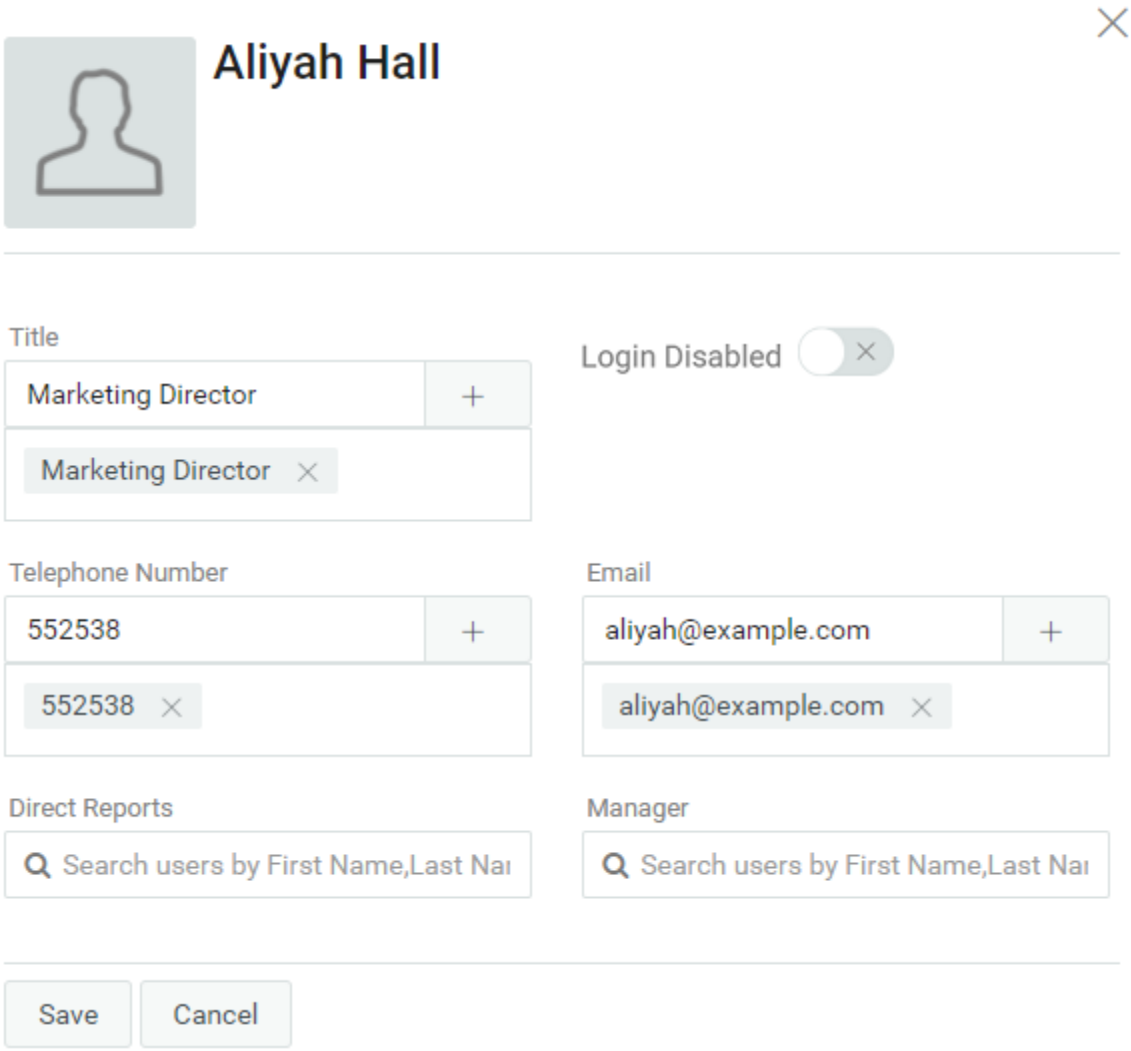
For more information, click ⓘ on the Dashboard.

Editing User Information

Select a user from a list view, click ✎ to modify the user information such as Title, Email, Telephone Number, Manager, and more. You are allowed to modify the user attributes that are set by your administrator. For more information about configuring user attributes, see Customizing the Views in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*. You can delete users in the **Manage Users** view.

The following is an example of editing a user information:

Figure 13-1 *Editing User Information*



NOTE: The **Login Disabled** toggle switch can be used to disable a user account. This switch is only visible if the administrator adds the `Login Disabled` attribute in the Card View and Editable Attributes in the **Settings** > **Customization** page. For more information, click ⓘ on the Dashboard.

Listing Users

Following are the different ways to list users in identity applications:

- **List view:** To view the users in the list format, click ☰. This displays user information on the right-hand side. To edit user information such as Telephone Number, Email, Manager, and more, click ✎. If you want to see the organization chart of a particular user, click ⊞.
- **Card view:** To view the users in the card format, click ▦. This displays users basic information on the cards. Administrator can configure what information to display on the user's card. For more information, see Customizing the Views in *NetIQ Identity Manager - Administrator's*

Guide to the Identity Applications. Click to edit the user information such as **Telephone Number**, **Email**, **Manager**, and other attributes. If you want to see the organization chart of a particular user, click .

- **Manage Users view:** To view the users in the tabular format, click . This displays the users in a tabular view. This view allows you to sort users according to the user attributes such as Telephone Number, Email, Department, and more. You can customize the columns to be shown in this view. For more information about customizing columns, click on the Dashboard.

  This view also allows you to delete users from the system. To delete users:

  1. Select a user that you want to delete.
  2. Click .

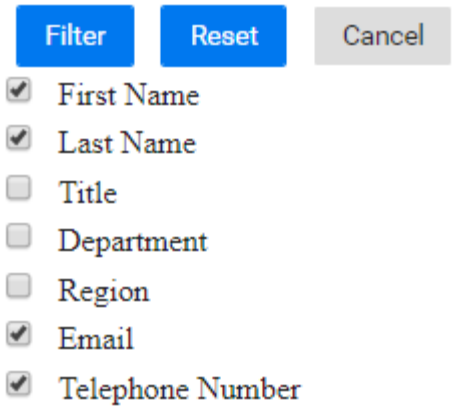
Finding Users

Following are the different ways to find users in identity applications:

- **Quick Search:** Specifies the user attribute and lists the users based on the selected filters. To modify the filter options:

  1. Click .
  2. Select the filter options to search users.

     Following is an example of the selected user attributes for a quick search:



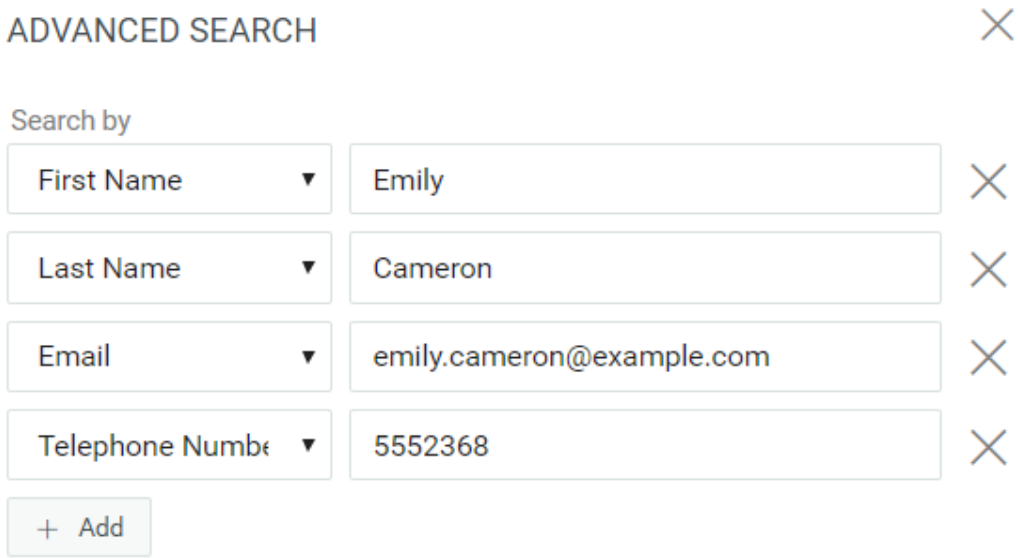
  3. Click **Filter**.

  For example, to search a user with name Smith where First Name and Last Name filters are selected. Quick search lists all the users who has Smith in their First Name and Last Name.

- **Advanced Search:** This option fetches the more refined list of users than quick search. You can search for a user with the defined user attributes. To use Advanced Search:

  1. Click .
  2. Specify the exact user information for each user attributes.

     Following is an example of the specified user attributes for an advanced search:



3. Click **Filter**.

For example, if you want to search for a user having **First Name** as Aliyah, **Last Name** as Hall, and **Title** as Director. You can specify these attributes in the Advanced Search to find a user who has the exact set of attributes.

You can also configure the search results on a page by setting the index at the bottom. Dashboard uses Virtual List View (VLV) control that runs at LDAP OID 2.16.840.1.113730.3.4. This works in combination with sort control.

Identity Manager Dashboard displays two different counts while showing the results:

- **Total Count:** This is the total count of users found in the system.
- **Search Count:** This is the count of users shown for the specific search.

Sorting Users

Manage Users view allows you to sort users according to their attributes. Administrator has to configure compound indexes for the user attributes to enable sorting. For more information about compound indexing, see Creating Compound Indexes in *NetIQ Identity Manager Install and Upgrade Guide for Windows*.

NOTE: If you are unable to sort users using any user attributes, contact your administrator to configure compound index for the required attribute to sort users.

---

14 Managing Teams

A team consists two types of users such as:

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 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.

To perform any of the following activities, go to **People > Teams**:

- "View Teams" on page 77
- "Create a Team" on page 78
- "Modify a Team" on page 78

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**.

For more information, click ⓘ on the Dashboard.

Create a Team

As an administrator, you can create 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.

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, click ⓘ on the Dashboard.

Modify a Team

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

- Changing Name and Description of the team.
- Modify Requesters for the team.
- Add or remove team members.
- Add or remove permissions for a team manager.

For more information, click ⓘ on the Dashboard.

15 Managing Groups

A group consists of users and other accounts that have a common characteristics. For example, the Finance group consisting of all employees in the Finance department.

Groups can be searched based on its description. However, Administrators who have access to the **Settings** page can customize the attributes for which a group entity can be searched. This means that when searching for a specific group while assigning a role to a group, making a group as the owner of a resource, or performing a simple search in the **Groups** page, the application will return the names of the group as a result that match the searched attribute. For more information, see Entity Settings in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Creating a Group

If you have an administrative role in the identity applications, you can create a group.

1. In the Identity Manager Dashboard, go to **People > Groups**.
2. Click **+**.
3. Specify values for the following required attributes:

Attribute	What to Specify
Name	The group name for this new group. **IMPORTANT:** Do not use the following special characters in the **Name** field: `< ; \ " + # / | * ~`
Description	A description of this new group. The description is used as a group search criteria in the Dashboard. **IMPORTANT:** Do not use the following special characters in the **Description** field: `| ~`
Container	An organizational unit in the identity vault under which you want the new group stored (such as an OU named groups). For example: `ou=groups,ou=MyUnit,o=MyOrg` To learn about using the buttons provided to specify a container, see "Creating a User" on page 73. **NOTE:** You won't be prompted for **Container** if the system administrator has established a default create container for this type of object.

4. Click **Create**.

   When the group is created successfully, the **Group Members** panel is displayed that allows you to add the users to the newly created group.
5. To add users to the group, click **+** icon that is beside the group members.

6 Select the required users in the modal window.

7 Click **Add**.