NetIQ® Identity Manager

User's Guide to the Identity Applications

March 2018

Legal Notice

Contents

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.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

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

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 on 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**:

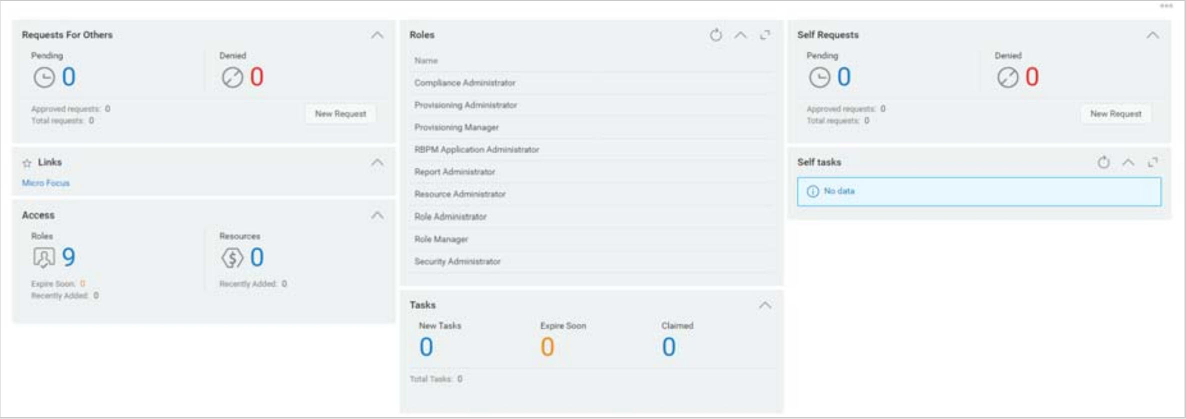
- Create and modify user profiles.
- View the organization chart details of other users.
- Create and modify teams that represent a set of users and groups that can perform provisioning requests and approval tasks associated with the teams.
- Request permissions or revoke permissions on behalf of other 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 27.

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

Figure 1-1 *Example Personal Dashboard*



Requests For Others

Pending 0

Denied 0

Approved requests: 0
Total requests: 0

Links

Micro Focus

Access

Roles 9

Expire Soon: 0
Recently Added: 0

Resources 0

Recently Added: 0

Roles

Name
Compliance Administrator
Provisioning Administrator
Provisioning Manager
RBPM Application Administrator
Report Administrator
Resource Administrator
Role Administrator
Role Manager
Security Administrator

Tasks

New Tasks 0

Expire Soon 0

Claimed 0

Total Tasks: 0

Self Requests

Pending 0

Denied 0

Approved requests: 0
Total requests: 0

Self tasks

No data

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 15.

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*.

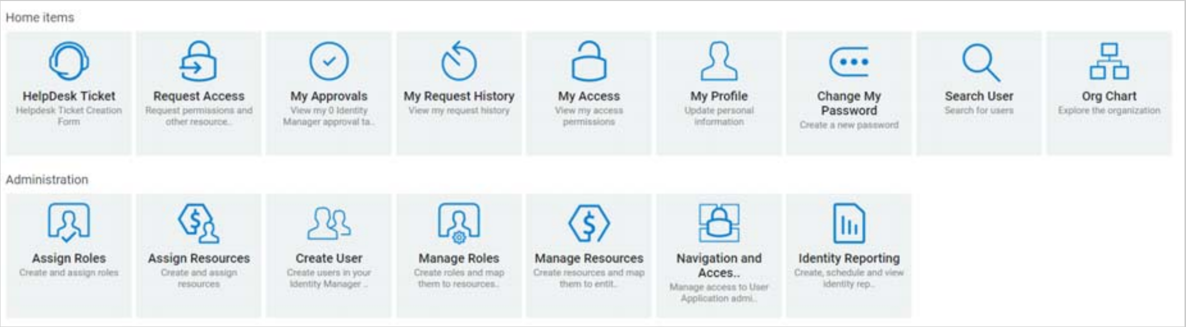
To know more on the capabilities of Identity Manager Dashboard, watch the following video:

🎬 http://www.youtube.com/watch?v=PrKa_gv5-0A

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*


Home items
HelpDesk Ticket
Helpdesk Ticket Creation Form
Request Access
Request permissions and other resource..
My Approvals
View my 0 Identity Manager approval ta..
My Request History
View my request history
My Access
View my access permissions
My Profile
Update personal information
Change My Password
Create a new password
Search User
Search for users
Org Chart
Explore the organization
Administration
Assign Roles
Create and assign roles
Assign Resources
Create and assign resources
Create User
Create users in your Identity Manager ..
Manage Roles
Create roles and map them to resources..
Manage Resources
Create resources and map them to entit..
Navigation and Acces..
Manage access to User Application admi..
Identity Reporting
Create, schedule and view identity rep..

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 on 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

Tasks page allows you to approve or deny actions for the tasks listed. By default, it lists all the **Self** tasks. You can view others tasks with an appropriate role. If you want to list the tasks of others, 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.

For more information about managing tasks, see Chapter 6, “Managing Your Tasks,” on page 43.

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 16
- “How Roles and Resources Work” on page 16
- “How Process Requests Work” on page 18
- “How Helpdesk Works?” on page 18

How Identity Self-Service Works

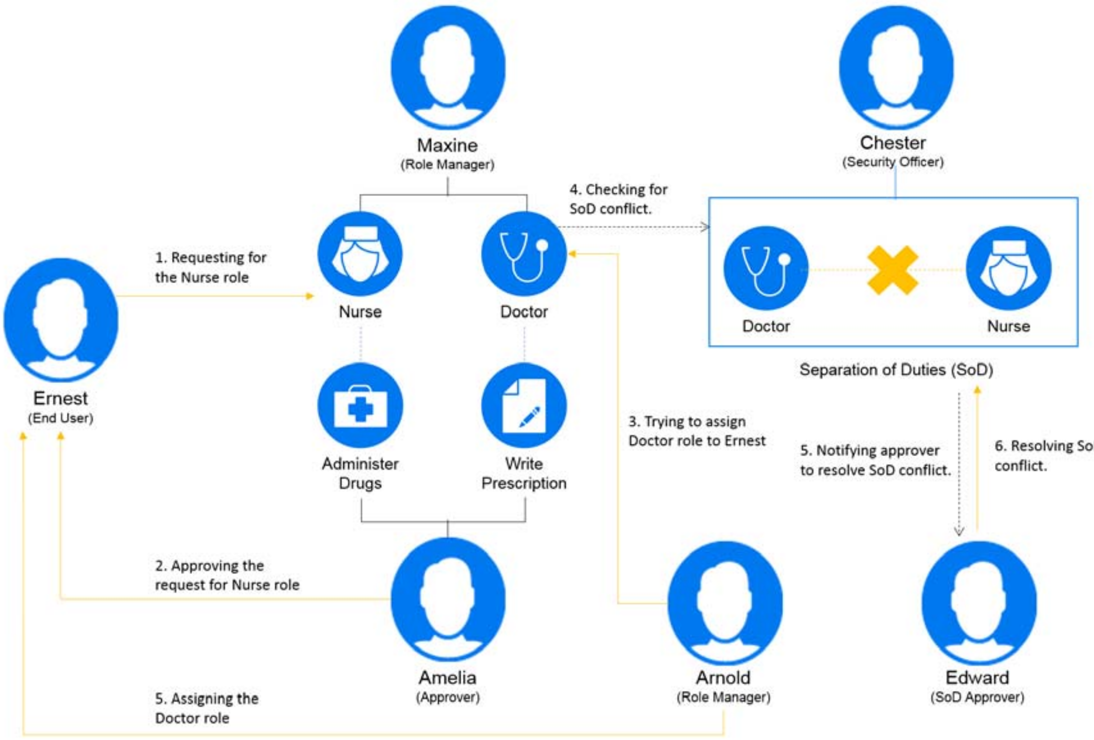
- Ella (an end user) recovers her forgotten password through the identity self-service features when logging in.

  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
(Role Manager)
Chester
(Security Officer)
4. Checking for SoD conflict.
1. Requesting for the Nurse role
Nurse
Doctor
Doctor
Nurse
Ernest
(End User)
Separation of Duties (SoD)
Administer Drugs
Write Prescription
3. Trying to assign Doctor role to Ernest
5. Notifying approver to resolve SoD conflict.
6. Resolving SoD conflict.
2. Approving the request for Nurse role
Amelia
(Approver)
Arnold
(Role Manager)
Edward
(SoD Approver)
5. Assigning the Doctor role

- 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.

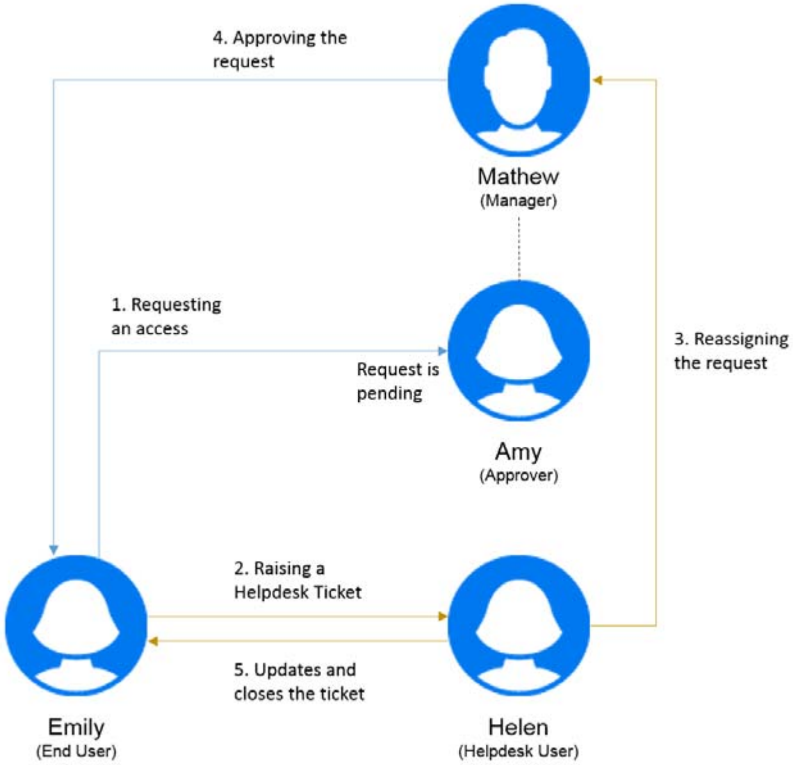
How Process Requests Work

- 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

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 24.
- 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.

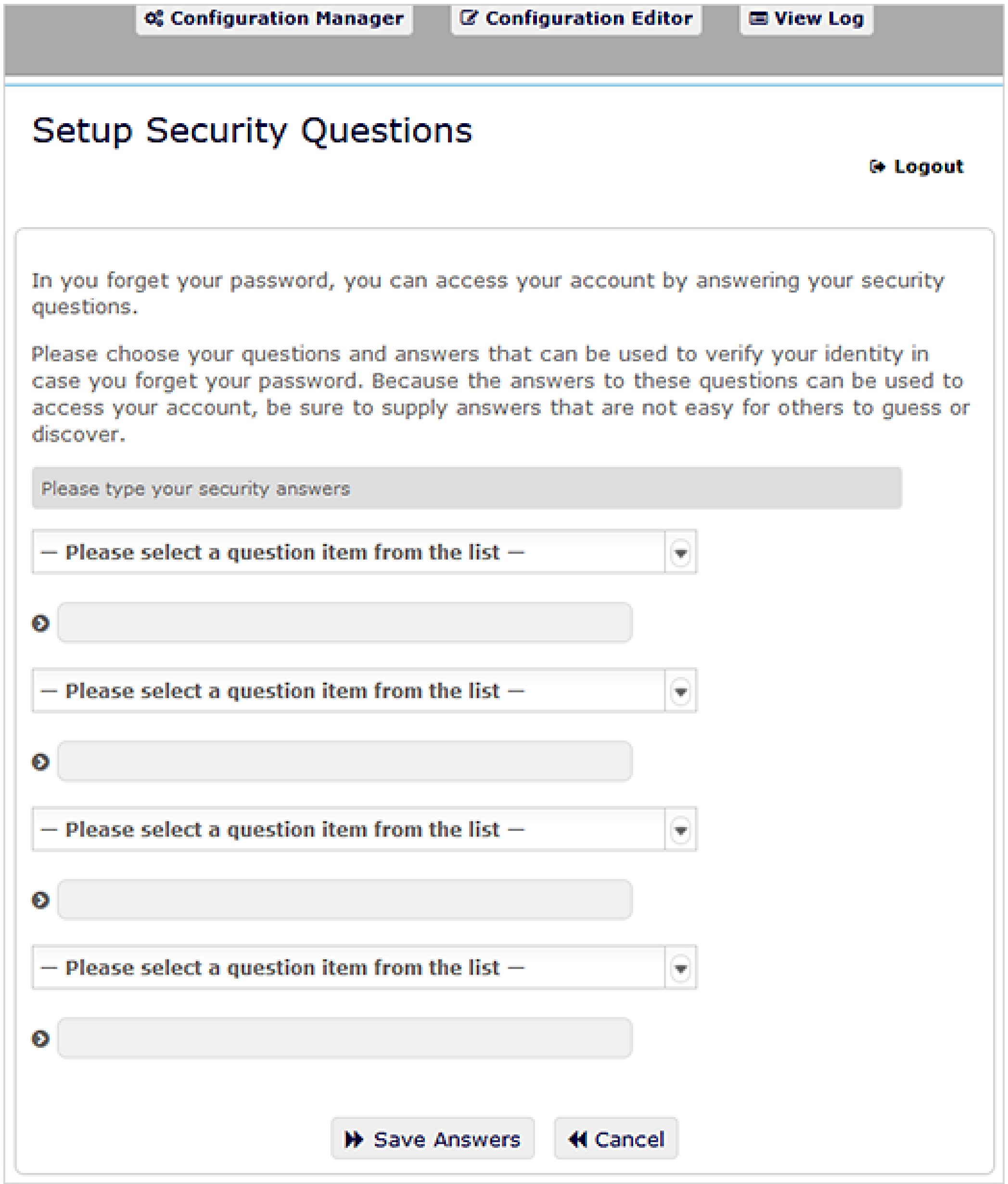
Logging in the First Time

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.


Configuration Manager
Configuration Editor
View Log
Logout
Please type your security answers
— Please select a question item from the list —
— Please select a question item from the list —
— Please select a question item from the list —
— Please select a question item from the list —
Save Answers
Cancel

Setup Security Questions

In you forget your password, you can access your account by answering your security questions.

Please choose your questions and answers that can be used to verify your identity in case you forget your password. Because the answers to these questions can be used to access your account, be sure to supply answers that are not easy for others to guess or discover.

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 tha tyou 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 24
- "If You Have Trouble Logging In" on page 24
- "If You're Prompted for Additional Information" on page 24

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**.

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*.

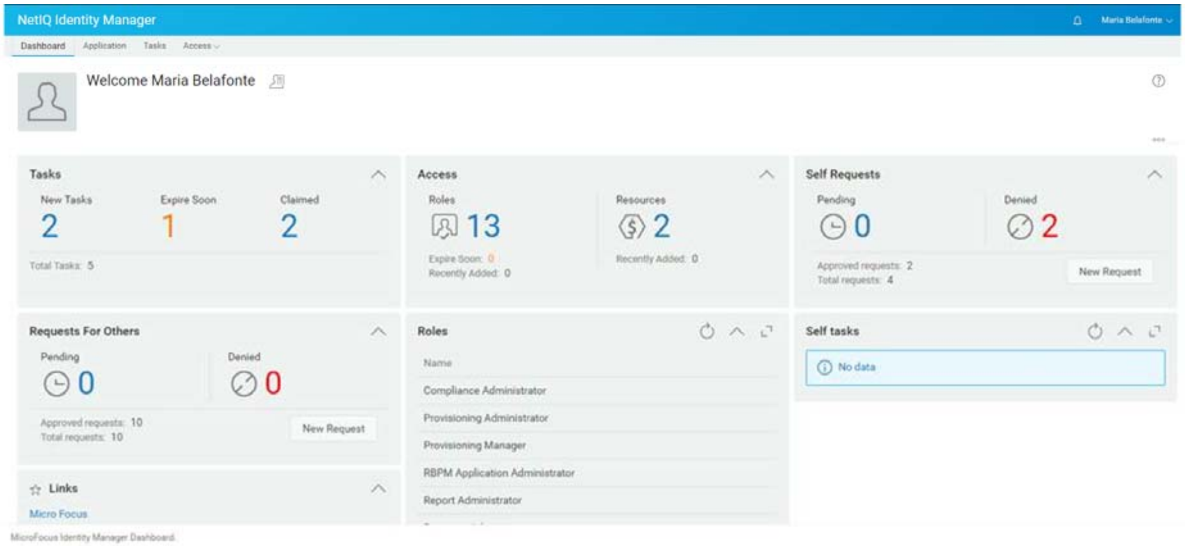
3 Managing Widgets and Layouts

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**.

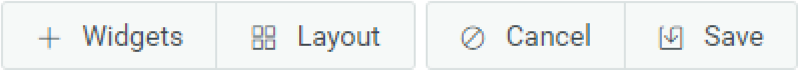
To personalize your Dashboard, go to your **Dashboard** and click ∘∘∘.

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 29.

Layout

Allows you to change the Dashboard layout. See "Changing the Dashboard Layout" on page 28.

Cancel

Cancels all the changes made to your Dashboard.

Save

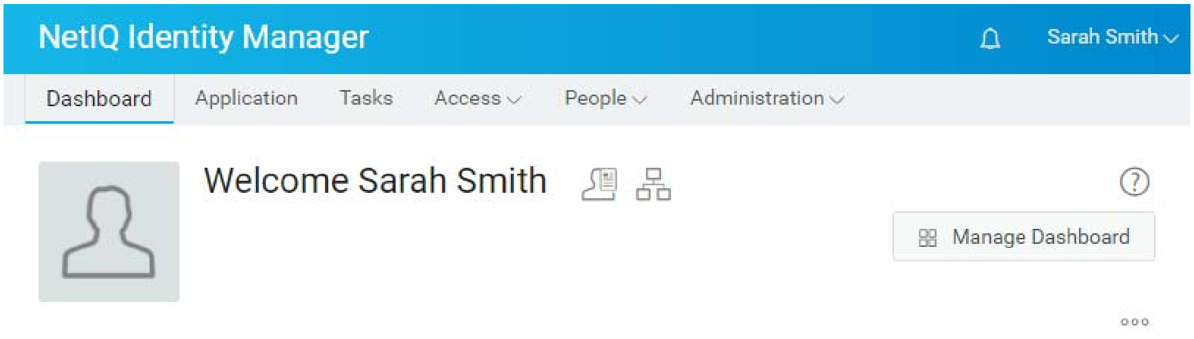
Saves your changes and applies to your Dashboard.

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*



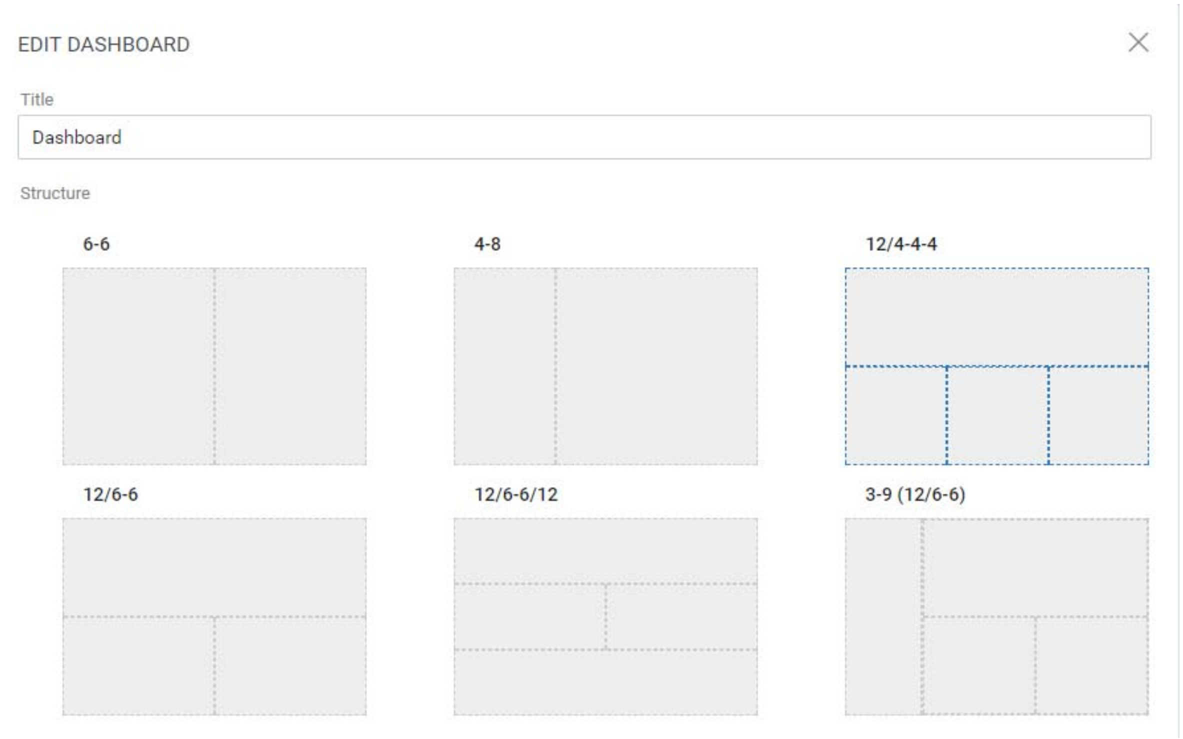
The administrator can add any user, group, container or role as a trustee to manage the global dashboard. To modify trustees to manage dashboard, go to **YourID > Settings > Access** and click **Global Dashboard** from the list. For more information about modifying configuration access, see Managing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



EDIT DASHBOARD

Title: Dashboard

Structure

6-6

4-8

12/4-4-4

12/6-6

12/6-6/12

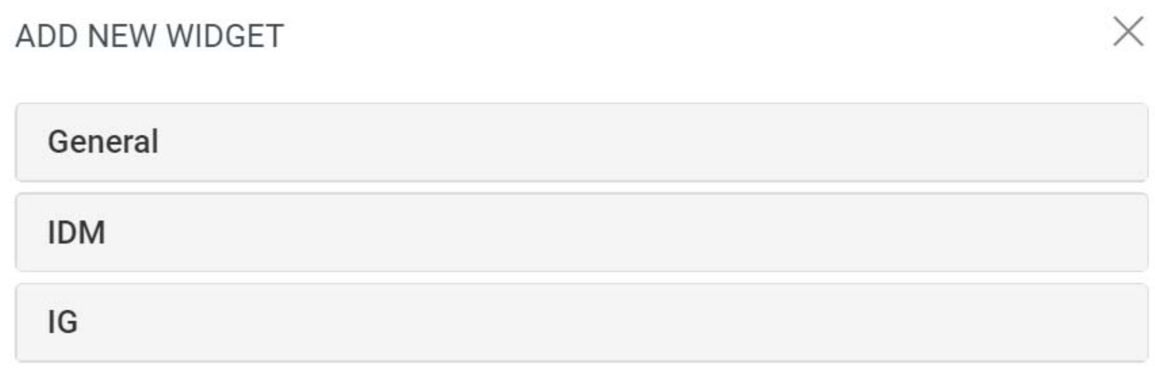
3-9 (12/6-6)

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 NEW WIDGET

General

IDM

IG

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"
                }
```

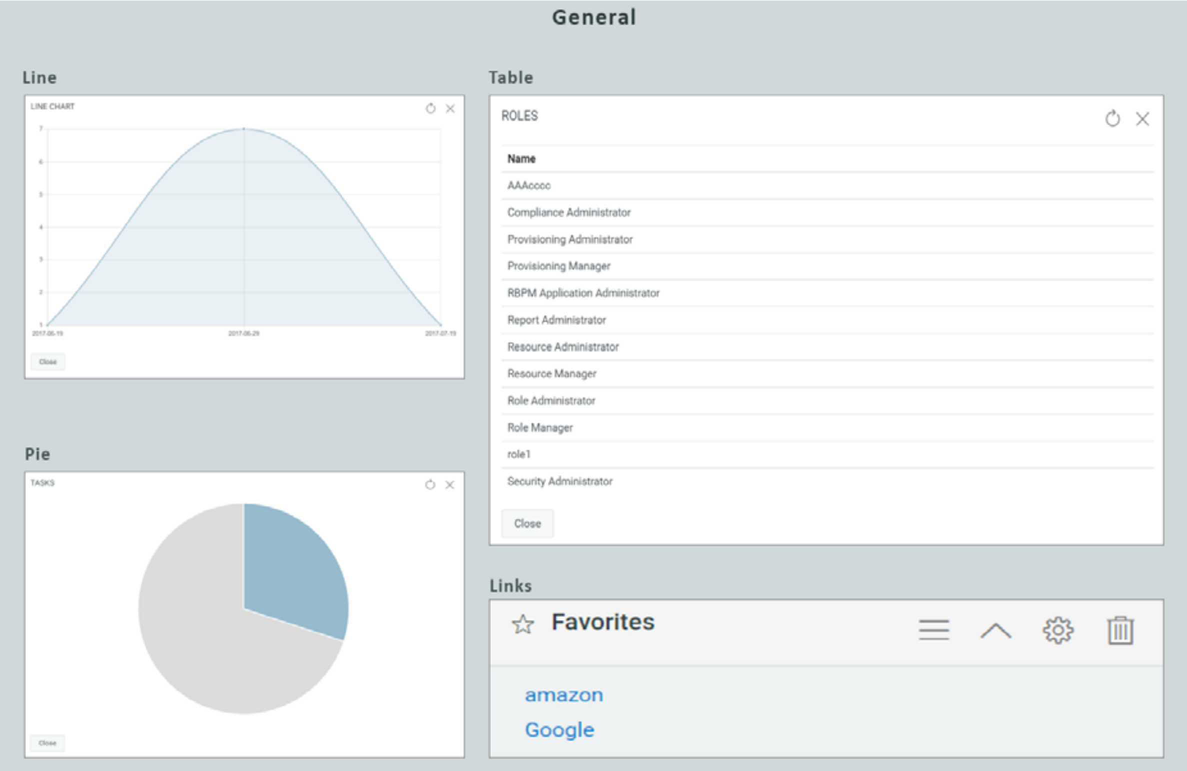
   In this sample, `assignments` is the Root element and `name` is the selected column to display that will be displayed on the widget. You can also bookmark any URL that you wish to access from your Dashboard

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*



ROLES

Name
AAAcccc
Compliance Administrator
Provisioning Administrator
Provisioning Manager
RBPM Application Administrator
Report Administrator
Resource Administrator
Resource Manager
Role Administrator
Role Manager
role1
Security Administrator

Close

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 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 33.

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

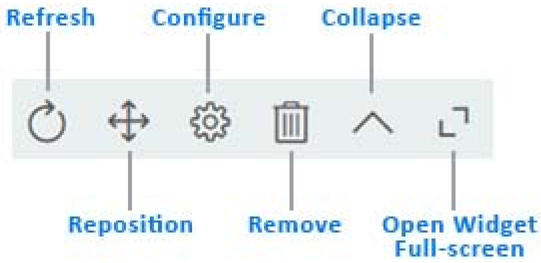
Displays the count of pending and completed reviews in the system.

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 33.

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

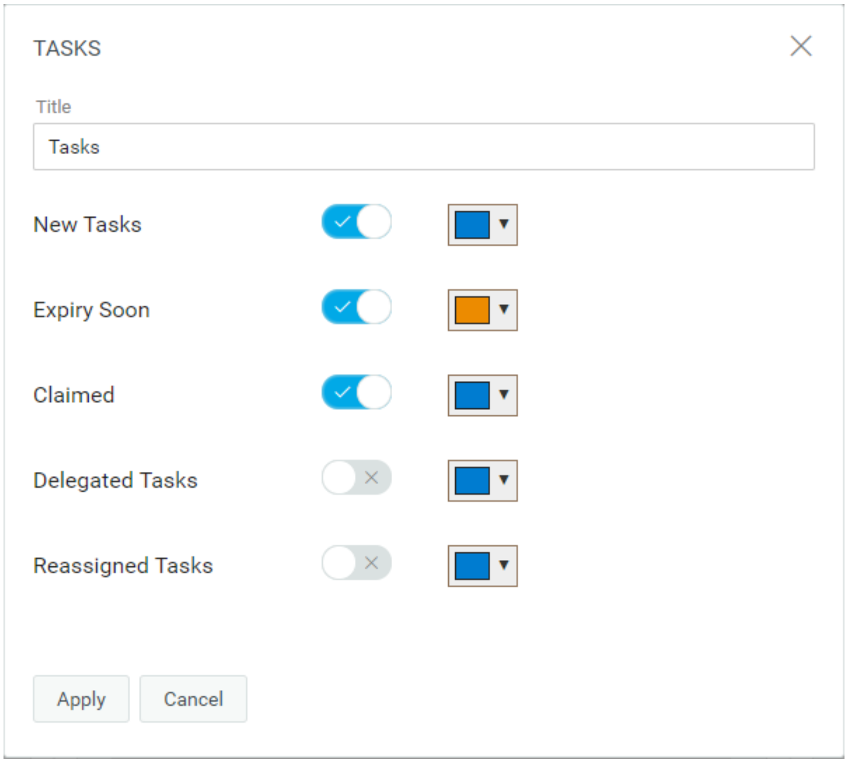
You can configure each widget that is added to your Dashboard. For example, you can enable or disable the fields of a widget or change the display color of the fields.

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*

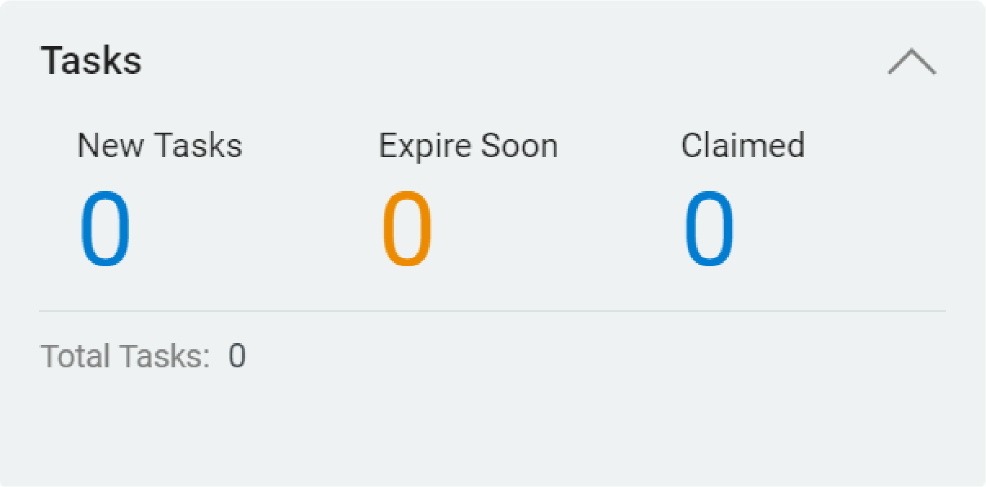


TASKS

Title: Tasks

New Tasks	✓	🟦 ▾
Expiry Soon	✓	🟧 ▾
Claimed	✓	🟦 ▾
Delegated Tasks	✕	🟦 ▾
Reassigned Tasks	✕	🟦 ▾

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



Tasks

New Tasks 0

Expire Soon 0

Claimed 0

Total Tasks: 0

To configure General widgets, modify the options that are displayed while adding widgets. See “Add General Widgets” on page 30.

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.

4 Managing Your Permission Requests

This section provides guidance for the following activities:

- “Viewing Your Permissions” on page 37
- “Requesting Permissions” on page 37
- “Viewing Requests” on page 38
- “Revoking Permissions” on page 39
- “Deep Linking to a Request” on page 40

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

Viewing Your Permissions

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, you can search by the name or description. You can also filter the list.

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

NOTE: By default, you can see the list of assigned or approved permissions. To see the child permissions mapped with the assigned or approved permissions, click ☰.

For more information, click ⓘ on the Dashboard.

Requesting Permissions

To request roles and resources, on the Dashboard select:

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.

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 39
- "Raising a Helpdesk Ticket" on page 39

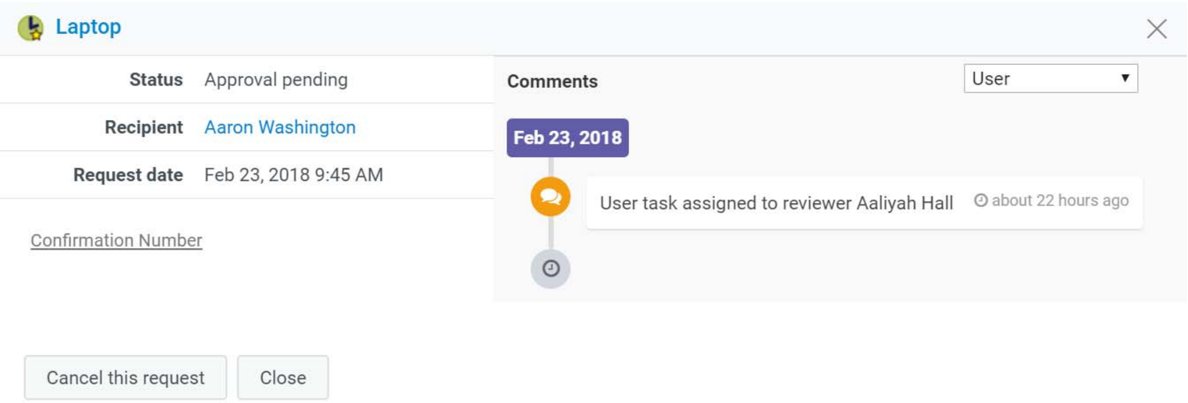
For more information, click ? on the Dashboard.

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.

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*



Laptop

Status	Approval pending
Recipient	Aaron Washington
Request date	Feb 23, 2018 9:45 AM

Confirmation Number

Comments — User ▾

Feb 23, 2018

User task assigned to reviewer Aaliyah Hall — about 22 hours ago

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, once the ticket is resolved or closed.

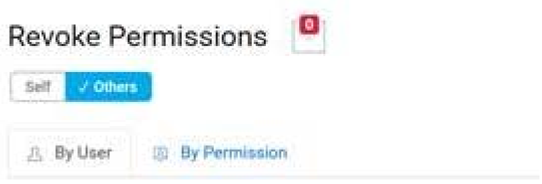
Revoking Permissions

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:

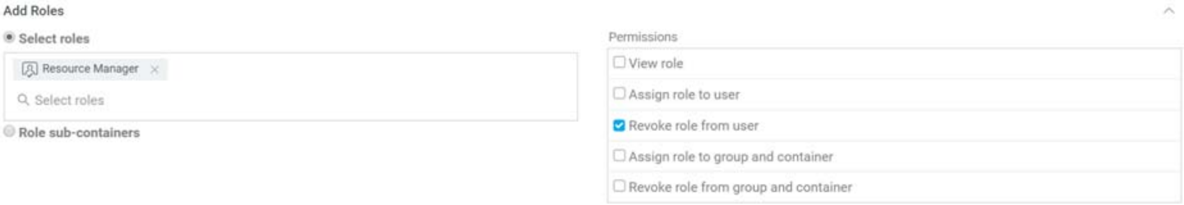


- **Search by user:** Allows you to search for a user and revoke permissions for that user. You can directly revoke a permission for the user or add the permission to a queue. A queue is a persistent work area where you can temporarily store permissions that you can review and revoke if required. You 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



Add Roles

● Select roles

Resource Manager ×

Select roles

○ Role sub-containers

Permissions

□ View role

□ Assign role to user

☑ Revoke role from user

□ Assign role to group and container

□ Revoke role from group and container

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.

Once 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 takes this form:

```
http://<server:port>/IDMProv/makeRequestDetail.do?requestId=<PRD
ID>&requestType=<requesttype>
```

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

```
http://testserver:8080/IDMProv/
makeRequestDetail.do?requestId=cn=EmailChange,cn=RequestDefs,cn=AppConfig,cn=Picas
soDriver,cn=TestDrivers,o=novell&requestType=PROV
```

NOTE: This feature is not supported in Identity Manager 4.1.1 and 4.7.2 versions. However, you can add applications to the **Applications** page by following the instructions from "Creating Featured Items" on page 43.

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 have 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 43 or "Adding a Permission" on page 44.

   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, in the Dashboard select:

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 checkbox. 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.

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.

- 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 65

    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 upto 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 18, 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 47
- “Acting as a Proxy” on page 47
- “Managing Proxy Assignments” on page 47

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.

NOTE: The tasks with 👥 icon indicates that task is delegated.

For more information, click ❔ on the Dashboard.

9 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.

10 Viewing an Organization Chart

The Dashboard provides an organization chart that shows the hierarchy of users in your organization.

By default, Security Administrator and Provisioning Administrator can view the organization chart for all the users in the system. You can navigate to the organization chart in one of the following ways:

- Go to **People > Organization Chart**, this page displays the organization chart of the logged in user. Type the name of other users in the system in the search bar, to find the organization chart of other users.
- Go to **People > Users** and select any user from the list and click 🖧 that is beside the user name.

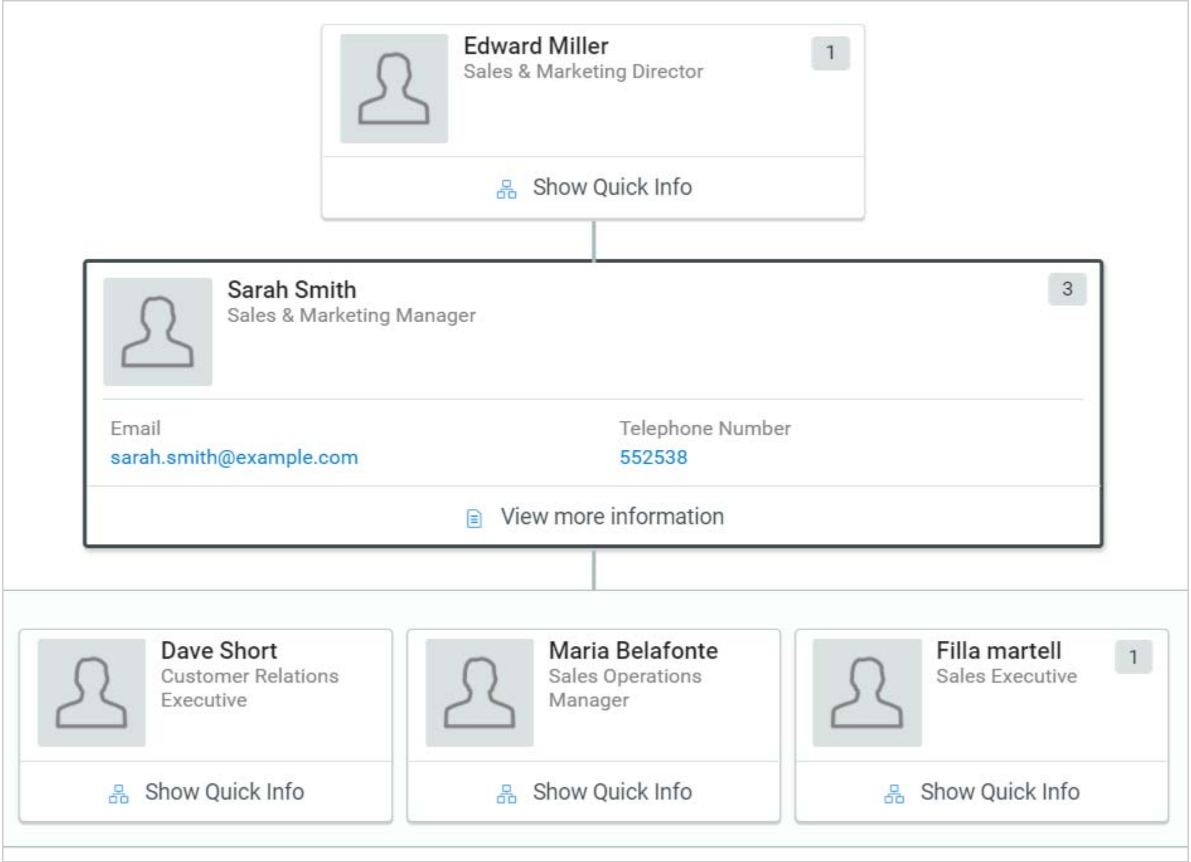
NOTE: You should have **Org Chart** access to view the **Organization Chart**. Contact your administrator to provide this access. For more information, see Managing User Access in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Understanding the Organization Chart

Organization chart displays the user information in the card format, these cards are arranged in a hierarchical order. The managers of the selected user is displayed on the top where direct reports at the bottom.

Following is an example of an organization chart for the user *Sarah Smith*:

***Figure 10-1** Example of the organization chart on the Dashboard*


Edward Miller
Sales & Marketing Director

Sarah Smith
Sales & Marketing Manager

Email
sarah.smith@example.com

Telephone Number
552538

Dave Short
Customer Relations Executive

Maria Belafonte
Sales Operations Manager

Filla martell
Sales Executive

In this example, *Edward Miller* is a manager of *Sarah Smith* where *Dave Short*, *Maria Belafonte*, and *Filla Martell* are the direct reports to *Sarah Smith*. The count that appears on the top-right corner of the user card signifies the number of reports for that user.

The selected user card and **Show Quick info** on the other users card displays the basic user information that are set by an administrator as primary attributes. For more information about how to customize the primary attributes, see Customizing the Views in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

To see more information about the user in a users list, click **View more information**.

11 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 55
- "Using the Legacy Password Management" on page 57

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 11-2, "Password Management Functions," on page 58:

Table 11-1 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)

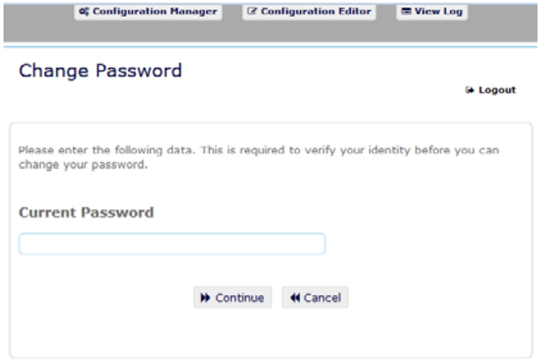
In Identity Manager 4.5, during the login process, the login page automatically redirects you to the Challenge-Response page. You set up the responses for challenge questions on this page. For more information, see "If You Forget Your Password" on page 24. When you login again and try to reset the forgotten 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.



Please enter the following data. This is required to verify your identity before you can change your password.

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 43.

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 58
- "Password Hint Change" on page 59
- "Change Password" on page 59
- "Password Policy Status" on page 60
- "Password Sync Status" on page 60

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 9, "Managing Your Profile," on page 51.

You can use the Password Management pages to do any of the functions listed in Table 11-2, "Password Management Functions," on page 58:

Table 11-2 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.

   From version 4.0.2, 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 59.

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.

To check which users or groups already exist, use the Directory Search page. See Appendix B, “Using the Directory Search in the User Application,” on page 79.

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 13, “Managing Teams,” on page 65.

12 Managing Users

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

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 > +

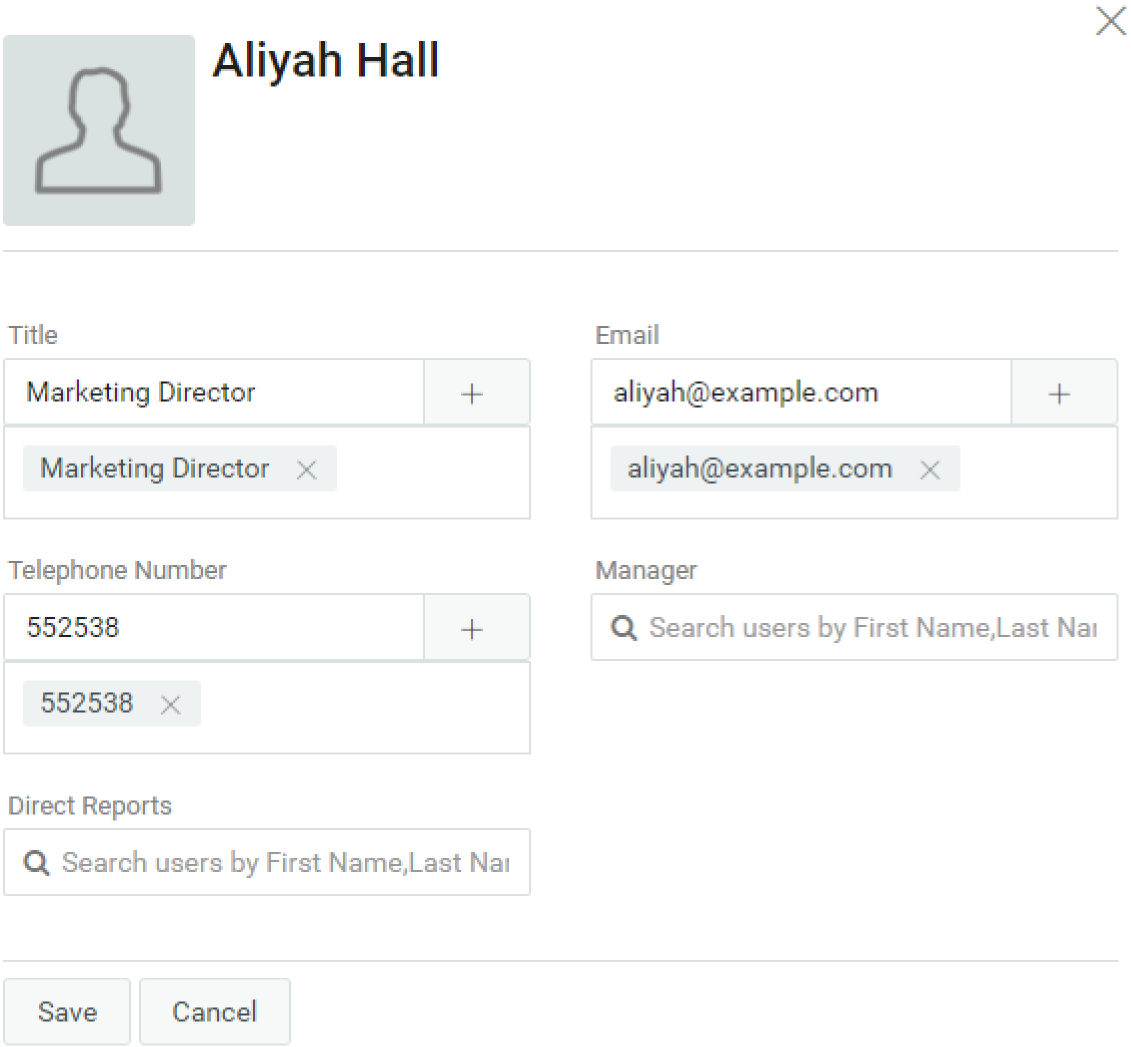
The identity administrator defines the values that you can specify for the user. Also, when creating a user, you can see the user **Container** but you cannot modify its value. This limitation ensures that all users are stored in the same container.

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. The following is an example of editing a user information:

***Figure 12-1** Editing User Information*



Aliyah Hall

Title: Marketing Director

Marketing Director ×

Email: aliyah@example.com

aliyah@example.com ×

Telephone Number: 552538

552538 ×

Manager: Search users by First Name,Last Nai

Direct Reports: Search users by First Name,Last Nai

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.

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 the 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 the 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 🗑.

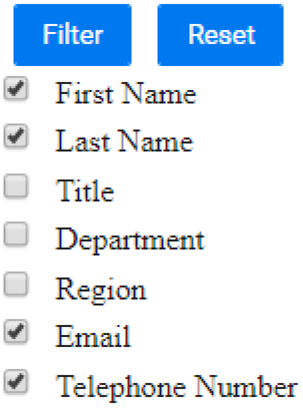
Finding Users

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:

     ☑ First Name
     ☑ Last Name
     ☐ Title
     ☐ Department
     ☐ Region
     ☑ Email
     ☑ Telephone Number

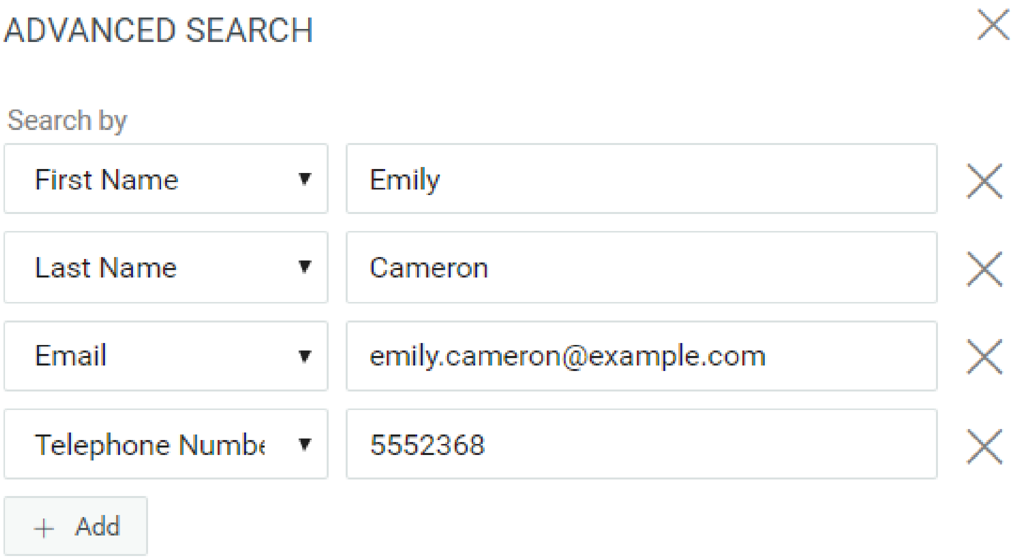
  3. Click **Filter**.

  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:



ADVANCED SEARCH

Search by

First Name: Emily

Last Name: Cameron

Email: emily.cameron@example.com

Telephone Numbe: 5552368

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 Setup 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.

13 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 65
- "Create a Team" on page 65
- "Modify a Team" on page 66

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.

14 Creating a Group

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

1 Log in to the User Application.

2 On the **Identity Self-Service** tab, click **Create User or Group** in the menu (under **Directory Management**, if displayed).

The **Select an object to create** panel displays.

3 Use the **Object type** drop-down list to select **Group**, then click **Continue**.

The **Set attributes for this Group** panel displays.

4 Specify values for the following required attributes:

Attribute	What to Specify
Group ID	The group name for this new group.
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 61. **NOTE:** You won't be prompted for **Container** if the system administrator has established a default create container for this type of object.
Description	A description of this new group.

5 Click **Continue**.

The group is created, then the **Review** panel displays to summarize the result.

The **Review** panel provides optional links that you might find handy:

- Click the new group's name to display the Profile page of detailed information for this group

  From the Profile page, you can edit the group's details to make changes or delete the group.

- Click **Create Another** to return to the initial panel of the Create User or Group page

V Appendix

The following appendix provide additional reference information and advanced topics for the Identity Manager User Application.

A Using the Identity Manager Approvals App

In addition to the User Application user interface used by Identity Manager customers, you can now use a new iOS app that allows Identity Manager users to remotely approve or deny requests through the Roles Based Provisioning Module for Identity Manager.

Once you install and configure the Approvals app, you can see the same approval tasks in the app that you would normally see in the User Application interface. All changes are synchronized between the Approvals app and the User Application.

You can also work in offline mode when disconnected from the Identity Manager Roles Based Provisioning Module server, and the Approvals app will automatically synchronize any changes once connectivity is restored.

This appendix provides information about installing and using the new Approvals app. For information about how Identity Manager administrators can configure their environment to allow users to use the app, see "Configuring the Identity Manager Approvals App" in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

For more detailed information about the Approvals app, see the following sections:

Product Requirements

The Approvals app requires an Apple iPhone or iPad with Apple iOS 6 or iOS 7 installed or any device with Android 5.0 or later.

NOTE: If your administrator has not enabled use of the Approvals app, you may not be able to configure the app after installation. For information on how administrators can configure the Identity Manager environment to enable use of the Approvals app, see "Configuring the Identity Manager Approvals App" in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Installing the Approvals App

You can install the NetIQ Identity Manager Approvals app from the Approvals app page (http://appstore.com/NetIQIdentityManagerApprovals) on the Apple App Store onto your device.

After you install the Approvals app, you must then configure the app to be able to connect with your Roles Based Provisioning Module server.

NOTE: If your User Application password has expired, we recommend change your password before installing and configuring the Approvals app. If the password policy in your environment allows a limited number of grace logins when a password expires, the Approvals app may use all of those logins in an attempt to sync your Identity Manager tasks to your device.

Configuring the Approvals App

You can configure the NetIQ Identity Manager Approvals app in several ways, depending on the needs of your environment and the way in which your administrator has configured Identity Manager:

- Make a request in the User Application interface for access to the Approvals app, and then launch the app on your device from the email link provided by your Identity Manager administrator. The link includes all the required configuration information.
- Click a configuration link or scan a configuration QR code using your device, where link or QR code provides either all required configuration information or generalized configuration information for your company.
- Manually enter the configuration information for your environment in the app itself.

IMPORTANT: In order for users to be able to automatically configure the Approvals app using either a link or QR code, the administrator for the Identity Manager environment must first enable the link or QR code.

Requesting Mobile Access Through the User Application

If configured by your administrator, you can request access to the Approvals app using the User Application. Identity Manager then sends an email that contains a customized link you can open on your device to automatically configure the app with your information.

To request mobile access through the User Application:

1. In a Web browser, log in to the Identity Manager User Application using the HTTPS (`https://`) protocol.

   NOTE: To request access to the Approvals app, you must log in to the User Application using the HTTPS protocol.

2. Click **Make a Process Request**.
3. Click the Process Request Category drop-down menu and select **Accounts**.
4. Click **Continue**.
5. Click **Request Mobile Approval App**.

   NOTE: The process request category and name may vary, depending on how your administrator has configured the Approvals app request process.

6. Provide the required information in process request form and click **Submit**.
7. When you receive an email from your Identity Manager administrator, open the email on your device and click the link provided to connect your device to the Roles Based Provisioning Module server.

NOTE: If you have previously installed the app, the app may display a warning message that existing settings will be overwritten. Ensure that the host name displayed in the warning message is the same host you accessed when you requested access to the app. If in doubt, do not click the link and contact your administrator.

If the host name is correct, click **Accept** to overwrite your existing settings.

8 When the app starts up, enter your password and click the Test Connection icon 🔗 to verify your settings.

Using a Configuration Link or QR Code

Your Identity Manager administrator may provide a configuration link to configure your Approvals app. Open the link in a browser on your device to automatically configure the app.

However, this link can only provide some of the required settings. Typically, a link or code can only provide the Roles Based Provisioning Module server details necessary for the Approvals app to function. After you click the link, you must manually configure your `Username` and `Password` settings, as well as any other settings not automatically configured.

In some environments, you may not be able to access your email from your device. If you cannot receive email on your device, you can instead use your device to scan a personalized QR code provided by the Identity Manager administrator.

Display the provided QR code on your computer or on a printed page, if necessary, and scan the code using a QR code reader on your device. After the QR code automatically configures the Approvals app for your environment, manually configure your `Username` and `Password` settings.

Manually Configuring the Approvals App

If the administrator of your Identity Manager environment does not provide a link or QR code to use when configuring the Approvals app, you can also configure the required configuration settings manually.

WARNING: Because manually configuring the app on your device requires in-depth knowledge of Identity Manager components, we recommend only advanced users knowledgeable about the Roles Based Provisioning Module and User Application environment in your enterprise manually configure app settings. Other users should contact their Identity Manager administrator for information about configuring the app.

In the app, click the Settings icon ⚙, specify the required settings, and then click the Test Connection icon 🔗 to verify your settings.

The Approvals app requires the following settings:

Login Setting Name	Login Setting Description
Username	Specifies the user name you use to access the Roles Based Provisioning Module server.
Password	Specifies the password you use to access the Roles Based Provisioning Module server.

Login Setting Name	Login Setting Description
Data Sync	Specifies if you want the app to actively sync data to the Roles Based Provisioning Module server.
Advanced > Server Details > Server	Specifies the fully qualified domain name or IP address of the Roles Based Provisioning Module server.
Advanced > Server Details > Secure Port	Specifies the HTTPS port the app uses to connect to the server.
Advanced > Server Details > Context	Specifies the context used when installing the User Application WAR file. The default value is `IDMProv`.
Advanced > Server Details > User Container	Specifies the full DN of the Identity Vault container that stores user information.
Advanced > Server Details > Timeout	Specifies the number of seconds the app waits when attempting to connect to the server before cancelling the connection. The default value is 5 seconds.
Advanced > Data Definition Settings > User Entity	Specifies the LDAP entity that represents a user in the Identity Vault. The default value is `user`.
Advanced > Data Definition Settings > Name Format	Specifies the DAL attribute representation the app uses to format a user's full name. The default value is `FirstName LastName`.
Advanced > Data Definition Settings > First Name Attr	Specifies the name of the DAL attribute that represents a user's first name. The default value is `FirstName`.
Advanced > Data Definition Settings > Last Name Attr	Specifies the name of the DAL attribute that represents a user's last name. The default value is `LastName`.
Advanced > Data Definition Settings > User Photo Attr	Specifies the name of the DAL attribute that contains a user's photo. The default value is `UserPhoto`. **NOTE:** If you do not have a picture configured in the Identity Manager or have configured your Identity Manager settings to not display a picture, the app displays a generic image instead.
Advanced > Data Definition Settings > Work Phone Attr	Specifies the name of the DAL attribute that represents a user's work phone number. The default value is `TelephoneNumber`.
Advanced > Data Definition Settings > Mobile Phone Attr	Specifies the name of the DAL attribute that represents a user's mobile phone number. The default value is `mobile`.
Advanced > Data Definition Settings > Email Attr	Specifies the name of the DAL attribute that represents a user's email address. The default value is `Email`.
Advanced > Data Definition Settings > Photo LDAP Attr	Specifies the name of the LDAP attribute that contains the photo of the user. The default value is `photo`.
Advanced > Data Definition Settings > Naming Attribute	Specifies the naming DAL attribute used in the Identity Vault to describe a name. The default value is `cn`.
Advanced > Data Definition Settings > Provisioning Admin	Specifies whether you are a Provisioning Administrator on the Roles Based Provisioning Module server.

Login Setting Name	Login Setting Description
Advanced > Accepted Certificates	Specifies any invalid or self-signed certificates from the Roles Based Provisioning Module server that you allow the Approvals app to accept. When the Approvals app detects a self-signed or invalid certificate, the app asks you to accept or reject the certificate. If you accept the certificate, the app adds a certificate to the Accepted Certificates list. You can remove a certificate from the Accepted Certificates list by clicking the name of the certificate and restarting the app. **NOTE:** If the Roles Based Provisioning Module server certificate is valid, the app does not add the certificate to the Accepted Certificates list. The app accepts valid certificates by default.
Advanced > Rejected Certificates	Specifies any invalid or self-signed certificates from the Roles Based Provisioning Module server that you do not want the Approvals app to accept. When the Approvals app detects a self-signed or invalid certificate, the app asks you to accept or reject the certificate. If you reject the certificate, the app adds a certificate to the Rejected Certificates list. If the server then presents a rejected certificate, the app cannot create a connection to the server. You can remove a certificate from the Rejected Certificates list by clicking the name of the certificate.

Overview of the Approvals App

This section provides an overview of the NetIQ Identity Manager Approvals app user interface. Topics include:

- "Tasks View" on page 75
- "Details View" on page 76
- "Bulk Mode" on page 76
- "Completed Tasks View" on page 76
- "Login Settings View" on page 77
- "Advanced Settings View" on page 77

Tasks View

The default view of the Approvals app is the Tasks view. This view displays all of the tasks currently assigned to or claimed by you, with the title of the task and the name and picture of the task recipient. The view lists tasks by expiration date, displaying the tasks due soonest at the top and tasks with no expiration date below.

NOTE

- If a user does not have a picture configured in the Identity Manager or has configured their Identity Manager settings to not display a picture, the app displays a generic image instead.
- Using Approval App you cannot approve or deny tasks that are using complex forms.

If you want to approve or deny a request, or if you want to view the details of a particular task, click the task or task recipient name. If you want to contact a task recipient, click the recipient's picture.

Details View

The Details view displays details for a particular task assigned to you. The fields displayed vary depending upon the request.

To approve or deny a task, provide any necessary information, and click either **Approve** or **Deny**.

Bulk Mode

If you need to approve or deny a large number of similar tasks, you can switch from the default single-task mode to bulk mode in the Tasks view.

NOTE: You cannot approve all tasks in bulk mode. For more complex tasks, like attestation tasks, you must approve each attestation task separately in single-task mode. When you click the Bulk Mode icon, the app displays only the tasks in your list that can be approved in bulk mode.

To approve or deny multiple tasks:

1. In the Tasks view, click the Bulk Mode icon.
2. Select the tasks you want to approve or deny. You cannot approve some tasks and deny other tasks at the same time.
3. (Optional) If you want to approve or deny all tasks, click **All**.
4. (Optional) If you change your mind and do not want to approve or deny any tasks, click the single-task mode icon.
5. Click **Approve** or **Deny**.
6. (Optional) Provide a comment regarding the bulk operation.
7. Click **Confirm**.

Completed Tasks View

To view your completed tasks, click the Completed Tasks icon. The view displays the completed task, as well as the time the task was approved or denied. You can click a completed task to view the details of that particular task. For more complex requests, you can click **Form Values** to view specific information for the request.

If necessary, you can delete one or more of your completed tasks from the Completed Tasks view. To delete tasks, click the Bulk Mode icon, select the tasks you want to delete, and click **Delete**.

NOTE: The Completed Tasks view only displays tasks completed on your device. You cannot view tasks completed in the User Application or on another device with the Approvals app installed.

Login Settings View

The Login Settings view allows you to view or modify your login settings.

WARNING: If your Identity Manager administrator provided a link or QR code to automatically configure your app settings, we recommend you do not modify those default settings unless your administrator instructs you to do so.

Advanced Settings View

The Advanced Settings view allows you to view or modify advanced settings that determine how you receive data from the Roles Based Provisioning Module server.

WARNING: If your Identity Manager administrator provided a link or QR code to automatically configure your app settings, we recommend you do not modify those default settings unless your administrator instructs you to do so.

If you accidentally change the Data Definition Settings in the Advanced Settings view, click **Restore Defaults** to restore the default settings provided by Identity Manager. **Restore Defaults** does not change your user name, password, or any of the Server Details settings.

Changing the Approvals App Display Language

The Approvals app includes localized text strings in multiple languages. To change the language the Approvals app uses, change the Language and Region Format settings on your iOS device. The Region Format settings configure how dates, times, and phone numbers are displayed on the device.

To modify language and region settings:

1. On your iOS device, click **Settings**.
2. Click **General**.
3. Click **International**.
4. (Optional) If you want to change the language your device uses, click **Language**, select the language you want to use, and then click **Done**.
5. (Optional) If you want to change the region format your device uses for dates and times, click **Region Format**, select the format you want to use and click **International**.
6. Go back to your device’s home screen.

B Using the Directory Search in the User Application

This section tells you how to use the Directory Search page on the **Identity Self-Service** tab of the User Application. Topics include:

- "Understanding Directory Search" on page 79
- "Performing Basic Searches" on page 80
- "Performing Advanced Searches" on page 80
- "Working with Search Results" on page 87
- "Using Saved Searches" on page 90

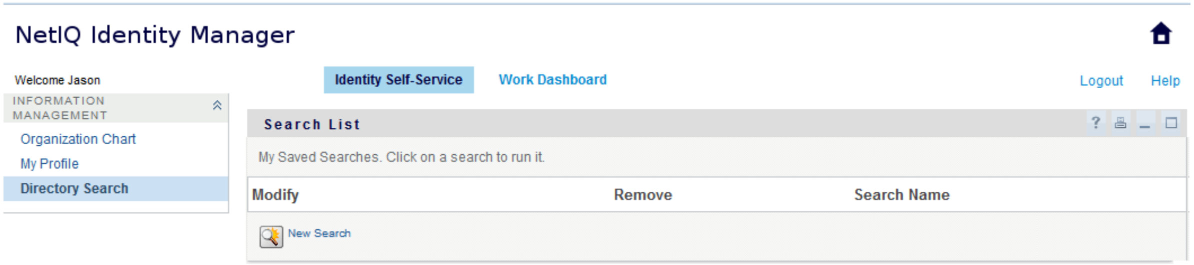
NOTE: This section describes the default features of the Directory Search page. You might encounter some differences because of your job role, your level of authority, and customizations made for your organization; consult your system administrator for details.

Understanding Directory Search

You can use the Directory Search page to search for users, groups, or teams by entering search criteria or by using previously saved search criteria.

For example, suppose Timothy Swan (Marketing Director) needs to search for information about someone in his organization. He goes to the Directory Search page and sees this by default:

Figure B-1 *Directory Search Page*



My Saved Searches. Click on a search to run it.

He doesn't yet have any saved searches to select from, so he selects **New Search**.

There's a user he wants to contact whose first name begins with the letter C, but he can't remember the full name. He just needs to specify a basic search with this criterion.

The search results display, enabling Timothy to examine and work with his requested information. By default, **Identity** tab information is displayed.

Timothy clicks the **Organization** tab in the search results to get another view of the information. He recalls that the person he seeks works for Kip Keller, so that narrows it down to Cal Central.

In addition to the tabs for different views, the search results page provides links and buttons for performing actions on its information. You can:

- Sort the rows of information by clicking the column headings
- Display details (Profile page) for a user or group by clicking its row
- Send new e-mail to a user by clicking the e-mail icon in that user's row
- Save the search for future reuse
- Export the results to a text file
- Revise the search by changing its criteria

When generating search results, you might sometimes need more than a basic search to describe the information you want. You can use an advanced search to specify complex criteria.

If there's an advanced search that you might need to perform again, you can retain it as a saved search. Saved searches are even handy for basic searches that you run frequently. For instance, Timothy Swan has added a couple of saved searches that he often uses.

Performing Basic Searches

1. Go to the Directory Search page and click **New Search**. The Basic Search page displays by default:
2. In the **Search for** drop-down list, specify the type of information to find by selecting **Group** or **User**.
3. In the **Item Category** drop-down list, select an attribute to search on. For example:

   ```
   Last Name
   ```

   The list of available attributes is determined by what you're searching for (users or groups).
4. In the **Expression** drop-down list, select a comparison operation to perform against your chosen attribute. For example:

   ```
   equals
   ```

   For more information, see "Selecting an Expression" on page 83.
5. In the **Search Term** entry box, specify a value to compare against your chosen attribute. For example:

   ```
   Smith
   ```

   For more information, see "Specifying a Value for Your Comparison" on page 84.
6. Click **Search**.

   Your search results display.

   To learn about what to do next, see "Working with Search Results" on page 87.

Performing Advanced Searches

If you need to specify multiple criteria when searching for users or groups, you can use an advanced search. For example:

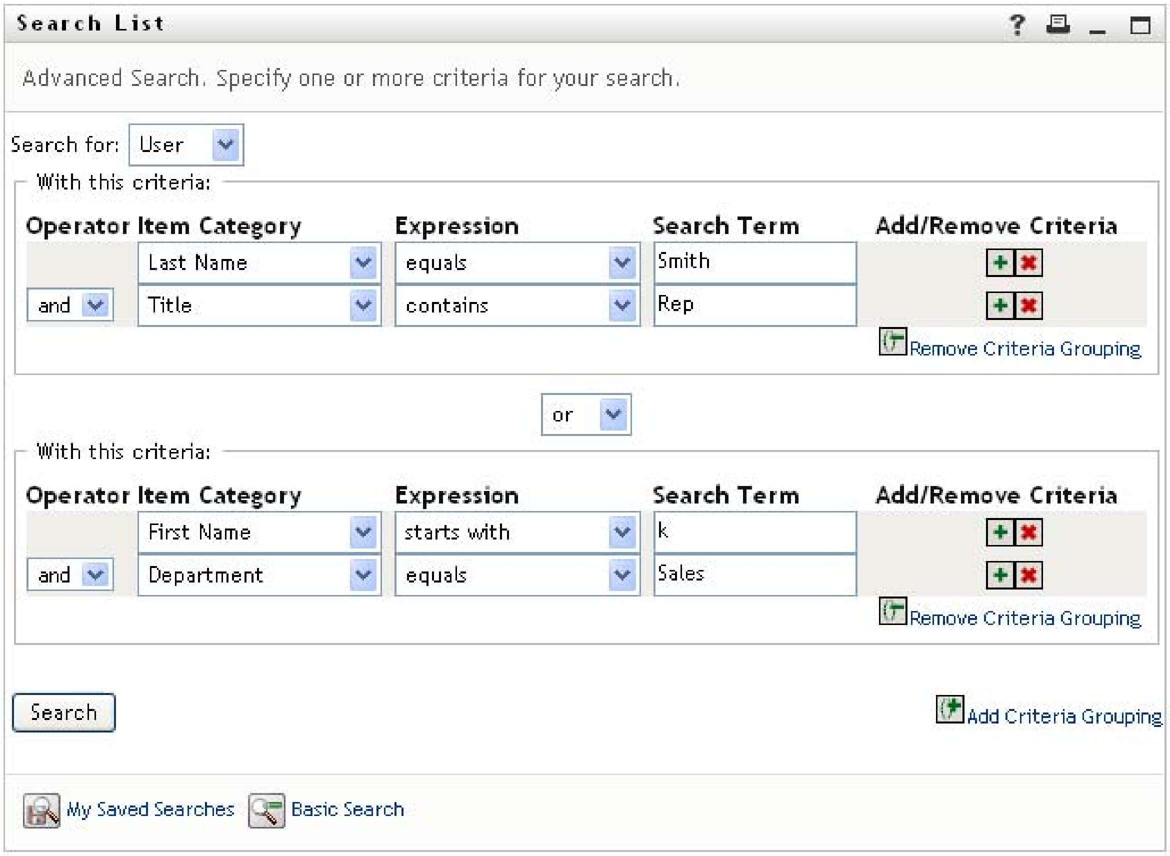
```
Last Name equals Smith AND Title contains Rep
```

If you specify multiple criteria groupings (to control the order in which criteria are evaluated), you'll use the same logical operations to connect them. For example, to perform an advanced search with the following criteria (two criteria groupings connected by an or):

`(Last Name` **`equals`** `Smith` **`AND`** `Title` **`contains`** `Rep)` **`OR`** `(First Name` **`starts with`** `k` **`AND`** `Department` **`equals`** `Sales)`

specify the following shown in Figure B-2 on page 81:

Figure B-2 Specifying an Advanced Search on the Search List Page



Search List

Advanced Search. Specify one or more criteria for your search.

Search for: User

With this criteria:

Operator	Item Category	Expression	Search Term
	Last Name	equals	Smith
and	Title	contains	Rep

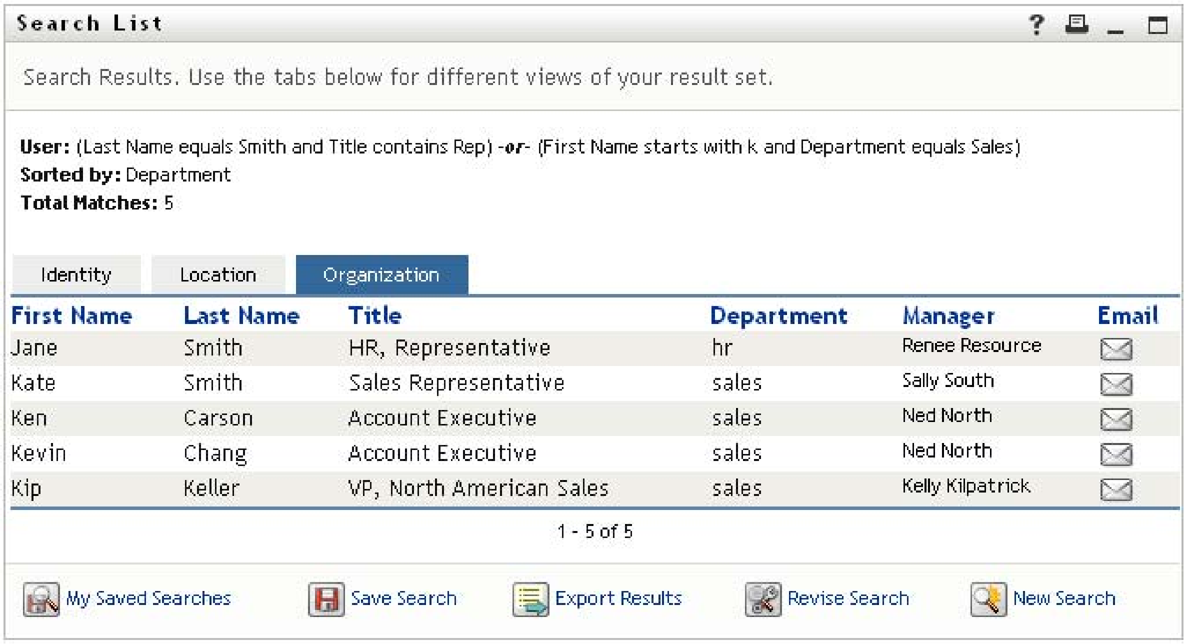
or

With this criteria:

Operator	Item Category	Expression	Search Term
	First Name	starts with	k
and	Department	equals	Sales

The result of this search is shown in Figure B-3 on page 82.

Figure B-3 Result of Advanced Search



Search Results. Use the tabs below for different views of your result set.

User: (Last Name equals Smith and Title contains Rep) *-or-* (First Name starts with k and Department equals Sales)
Sorted by: Department
Total Matches: 5

First Name	Last Name	Title	Department	Manager	Email
Jane	Smith	HR, Representative	hr	Renee Resource	✉
Kate	Smith	Sales Representative	sales	Sally South	✉
Ken	Carson	Account Executive	sales	Ned North	✉
Kevin	Chang	Account Executive	sales	Ned North	✉
Kip	Keller	VP, North American Sales	sales	Kelly Kilpatrick	✉

1 - 5 of 5

To perform an advanced search:

1 Go to the Directory Search page and click **New Search**. The Basic Search page displays by default.

2 Click **Advanced Search**. The Advanced Search page displays.

3 In the **Search for** drop-down list, specify the type of information to find by selecting one of the following:

- Group
- User

You can now fill in the **With this criteria** section.

4 Specify a criterion of a criteria grouping:

4a Use the **Item Category** drop-down list to select an attribute to search on. For example:

```
Last Name
```

The list of available attributes is determined by what you're searching for (users or groups).

4b Use the **Expression** drop-down list to select a comparison operation to perform against your chosen attribute. For example:

```
equals
```

For more information, see "Selecting an Expression" on page 83.

4c Use the **Search Term** entry to specify a value to compare against your chosen attribute. For example:

```
Smith
```

For more information, see "Specifying a Value for Your Comparison" on page 84.

5 If you want to specify another criterion of a criteria grouping:

5a Click **Add Criteria** on the right side of the criteria grouping:

⊞

5b On the left side of the new criterion, use the **Criteria Logical Operator** drop-down list to connect this criterion with the preceding one; select either **and** or **or**. You can use only one of the two types of logical operator within any one criteria grouping.

5c Repeat this procedure, starting with Step 4.

To delete a criterion, click **Remove Criteria** to its right: ☒

6 If you want to specify another criteria grouping:

6a Click **Add Criteria Grouping**.

6b Above the new criteria grouping, use the **Criteria Grouping Logical Operator** drop-down list to connect this grouping with the preceding one; select either **and** or **or**.

6c Repeat this procedure, starting with Step 4.

To delete a criteria grouping, click **Remove Criteria Grouping** directly above it.

7 Click **Search**.

Your search results display.

To learn about what to do next, see “Working with Search Results” on page 87.

Selecting an Expression

Click **Expression** to select a comparison criterion for your search. The list of comparison (relational) operations available to you in a criterion is determined by the type of attribute specified in that criterion:

Table B-1 *Comparison Operations for Searching*

If the attribute is a	You can select one of these comparison operations
String (text)	◆ starts with ◆ contains ◆ equals ◆ ends with ◆ is present ◆ does not start with ◆ does not contain ◆ does not equal ◆ does not end with ◆ is not present
String (text) with a predetermined list of choices User or group (or other object identified by DN) Boolean (true or false)	◆ equals ◆ is present ◆ does not equal ◆ is not present

If the attribute is a	You can select one of these comparison operations
User (item category: Manager, Group, or Direct Reports)	equals is present does not equal is not present
Group (item category: Members)	equals is present does not equal is not present
Time (in date-time or date-only format) Number (integer)	equals greater than greater than or equal to less than less than or equal to is present does not equal not greater than not greater than or equal to not less than not less than or equal to is not present

Specifying a Value for Your Comparison

The type of attribute specified in a criterion also determines how you specify the value for a comparison in that criterion:

Table B-2 Method of Entering Comparison Value

If the attribute is a	You do this to specify the value
String (text)	Type your text in the text box that displays on the right.
String (text) with a predetermined list of choices	Select a choice from the drop-down list that displays on the right.
User or group (or other object identified by DN)	Use the **Lookup, History,** and **Reset** buttons that display on the right.
Time (in date-time or date-only format)	Use the **Calendar** and **Reset** buttons that display on the right.
Number (integer)	Type your number in the text box that displays on the right.
Boolean (true or false)	Type `true` or `false` in the text box that displays on the right.

Don’t specify a value when the comparison operation is one of the following:

- is present
- is not present

Case in Text

Text searches are not case sensitive. You’ll get the same results no matter which case you use in your value. For example, these are all equivalent:

```
McDonald
```

```
mcdonald
```

```
MCDONALD
```

Wildcards in Text

You can optionally use the asterisk (*) as a wildcard in your text to represent zero or more of any character. For example:

```
Mc*
```

```
*Donald
```

```
*Don*
```

```
McD*d
```

Using the Lookup, History, and Reset Buttons

Some search criteria display Lookup, History, and Reset buttons. This section describes how to use these buttons:

Table B-3 Lookup, History, and Reset Buttons in Search Criteria

Button	What It Does
🔍	Looks up a value to use for a comparison
📋	Displays a **History** list of values used for a comparison
✎	Resets the value for a comparison

To look up a user:

1 Click **Lookup** to the right of an entry (for which you want to look up the user):

🔍

The Lookup page displays.

2 Specify search criteria for the user you want:

2a Use the drop-down list to select a search by **First Name** or **Last Name**.

2b In the text box next to the drop-down list, type all or part of the name to search for.

The search finds every name that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (*) as a wildcard in your text to represent zero or more of any character.

For instance, all of the following examples finds the first name Chip:

```
Chip
chip
c
c*
*p
*h*
```

3 Click **Search**.

The Lookup page displays your search results.

If you see a list of users that includes the one you want, go to Step 4. Otherwise, go back to Step 2.

You can sort the search results in ascending or descending order by clicking the column headings.

4 Select the user you want from the list.

The Lookup page closes and inserts the name of that user into the appropriate entry as the value to use for your comparison.

To look up a group as a search criterion for a user:

1 Add **Group** as a search criterion, then click **Lookup** 🔍 to the right of the **Search Term** field.

The Lookup page displays search results.

2 Specify search criteria for the group you want:

2a In the drop-down list, your only choice is to search by **Description**.

2b In the text box next to the drop-down list, type all or part of the description to search for.

The search finds every description that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (*) as a wildcard in your text to represent zero or more of any character.

For instance, all of the following examples find the description Marketing:

```
Marketing
marketing
m
m*
*g
*k*
```

3. Click **Search**.

   The Lookup page displays your search results.

   If you see a list of groups that includes the one you want, go to Step 4. Otherwise, go back to Step 2.

   You can sort the search results in ascending or descending order by clicking the column heading.

4. Select the group you want from the list.

   The Lookup page closes and inserts the description of that group into the appropriate entry as the value to use for your comparison.

To use the **History** list:

1. Click **History** to the right of an entry (whose previous values you want to see):

   The **History** list displays previous values for this criterion in alphabetical order.

2. Do one of the following:

If you want to	Do this
Pick from the **History** list	Select a value that you want from the list. The **History** list closes and inserts that value into the appropriate entry as the value to use for your comparison.
Clear the **History** list	Click **Clear History**. The **History** list closes and deletes its values for this entry. Clearing the **History** list does not change the current value of the entry in your comparison.

Working with Search Results

This section tells you how to work with the results that display after a successful search:

- "About Search Results" on page 88
- "Using the Search List" on page 88
- "Other Actions You Can Perform" on page 89

About Search Results

The content of your search results depends on the type of search you perform:

- "For a User Search" on page 88
- "For a Group Search" on page 88

On any search results page, you can select

- View My Saved Searches
- Save Search
- Revise Search
- Export Results
- Start a New Search

For a User Search

In the results of a user search, the list of users provides tabs for three views of the information:

- *Identity* (contact information)
- *Location* (geographical information)
- *Organization* (organizational information)

For a Group Search

The results of a group search provide only the Organization view of the information.

Using the Search List

You can do the following with the list of rows that displays to represent your results:

- "To Switch to a Another View" on page 88
- "To Sort the Rows of Information" on page 88
- "To Display Details for a User or Group" on page 89
- "To Send E-Mail to a User in the Search List" on page 89

To Switch to a Another View

1. Click the tab for the view you want to display.

To Sort the Rows of Information

1. Click the heading of the column that you want to sort.

   The initial sort is in ascending order.
2. You can toggle between ascending and descending order by clicking the column heading again (as often as you like).

To Display Details for a User or Group

1. Click the row for the user or group whose details you want to see (but don’t click directly on an e-mail icon unless you want to send a message instead).

   The Profile page displays, showing detailed information about your chosen user or group.

   This page is just like the My Profile page on the **Identity Self-Service** tab. The only difference is that, when you are viewing details about another user or group (instead of yourself), you might not be authorized to see some of the data or perform some of the actions on the page. Consult your system administrator for assistance.

2. When you’re done with the Profile page, you can close its window.

To Send E-Mail to a User in the Search List

1. Find the row of a user to whom you want to send e-mail.

2. Click **Send E-Mail** ✉ in that user’s row:

   A new message is created in your default e-mail client. The message is blank except for the **To** list, which specifies your chosen user as a recipient.

3. Fill in the message contents.

4. Send the message.

Other Actions You Can Perform

While displaying search results, you can also:

- “Save a Search” on page 89
- “Export Search Results” on page 89
- “Revise Search Criteria” on page 90

Save a Search

To save the current set of search criteria for future reuse:

1. Click **Save Search** (at the bottom of the page).

2. When prompted, specify a name for this search.

   If you’re viewing the results of an existing saved search, that search name displays as the default. This enables you to update a saved search with any criteria changes you’ve made.

   Otherwise, if you type a search name that conflicts with the name of an existing saved search, a version number is automatically added to the end of the name when your new search is saved.

3. Click **OK** to save the search.

   The Search List page displays a list of My Saved Searches.

   To learn more about working with saved searches, see “Using Saved Searches” on page 90.

Export Search Results

To export search results to a text file:

1. Click **Export Results** (at the bottom of the page).

The Export page displays.

By default, **View on screen** is selected, and **CSV** is chosen in the format drop-down list. Consequently, the Export page shows your current search results in CSV (Comma Separated Value) format.

2 If you want to see what those search results look like in Tab Delimited format instead, select **Tab Delimited** in the drop-down list, then click **Continue**.

3 When you're ready to export your current search results to a text file, select **Export to disk**.

The Export page displays.

4 Use the **Format** drop-down list to select an export format for the search results.

Export Format	Default Name of Generated File
CSV	SearchListResult.*date*.*time*.csv For example: `SearchListResult.27-Sep-05.11.21.47.csv`
Tab Delimited	SearchListResult.*date*.*time*.txt For example: `SearchListResult.27-Sep-05.11.20.51.txt`
XML (available if you are exporting to disk)	SearchListResult.*date*.*time*.xml For example: `SearchListResult.27-Sep-05.11.22.51.xml`

5 Click **Export**.

6 When prompted, specify where to save the file of exported search results.

7 When you're finished exporting, click **Close Window**.

Revise Search Criteria

1 Click **Revise Search** (at the bottom of the page).

This returns you to your previous search page to edit your search criteria.

2 Make your revisions to the search criteria according to the instructions in these sections:

- "Performing Basic Searches" on page 80
- "Performing Advanced Searches" on page 80

Using Saved Searches

When you go to Directory Search, the My Saved Searches page displays by default. This section describes what you can do with saved searches:

To List Saved Searches

1 Click the **My Saved Searches** button at the bottom of a Directory Search page. The My Saved Searches page displays.

To Run a Saved Search

1 In the **My Saved Searches** list, find a saved search that you want to perform.

2 Click the name of the saved search (or click the beginning of that row).

Your search results display.

To learn about what to do next, see "Working with Search Results" on page 87.

To Edit a Saved Search

1 In the **My Saved Searches** list, find a saved search that you want to revise.

2 Click **Edit** in the row for that saved search.

This takes you to the search page to edit the search criteria.

3 Make your revisions to the search criteria according to the instructions in these sections:

- "Performing Basic Searches" on page 80
- "Performing Advanced Searches" on page 80

4 To save your changes to the search, see "Working with Search Results" on page 87.

To Delete a Saved Search

1 In the **My Saved Searches** list, find a saved search that you want to delete.

2 Click **Delete** in the row for that saved search.

3 When prompted, click **OK** to confirm the deletion.