Identity Manager

Using the Identity Applications

October 2020

NetIQ

Legal Notice

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
Website:	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
Website:	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 website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** 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 community.netiq.com.

Welcome to Identity Manager

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

This application helps you with the following situations:

I want something

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

I need to do something

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

What do I have?

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

How did I get it?

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

For more information about this software product, see the NetIQ Identity Manager documentation.

1 Applications Page

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

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

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

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

However, to create or manage roles and resources, you must use Catalog Administrator. To create or manage groups, use the legacy User Application. For more information about this software product, see the NetIQ Identity Manager documentation.

Customize the Applications Page

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

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

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

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

2 Configure the Applications Page

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

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

For more information about this software product, see the NetIQ Identity Manager documentation.

Create and Edit Items and Permissions

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

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

   NOTE: You must specify a value for all fields that have an asterisk (*), such as the name and description for an application.
3. (Optional) Drag and drop the new application or permission to a category.
4. (Conditional) To modify an existing item, select the edit icon within the tile, then update the values.

Add, Modify, or Delete a Category

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

Add a Category

1. Select **New Category**.

   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.

Dashboard

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

- Chapter 3, “Customize Your Dashboard,” on page 13

3 Customize Your Dashboard

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

Manage the Global Dashboard

The global dashboard includes a set of widgets that will appear on the dashboard of every user in the system. Users can view these widgets based on their access provided by an administrator. For more information about provisioning dashboard widgets, see “Manage Dashboard Widgets” on page 73.

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

Administrator can add any user/group/container/role as a trustee to manage the global dashboard. To modify trustees to manage dashboard, go to **YourID > Settings > Access** and click **Global Dashboard** from the list. For more information about modifying configuration access, see “Configuring User Access” on page 68.

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

Manage Widgets and Layouts

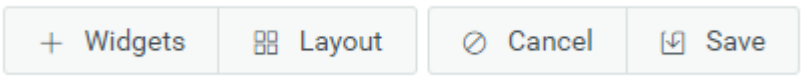
Widgets are Dashboard objects that are designed to provide specific details of a user for particular activity. For example, the Tasks widget provides details about new tasks, claimed tasks, or the tasks that are expected to expire shortly. Similarly, there can be many other widgets which can be configured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

Administrators who have access to the **Settings** page can provision widgets for a User, Group, Container, or a Role. For more information, see “Manage Dashboard Widgets” on page 73.

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

Use the following are options to personalize your Dashboard:

Figure 3-1 *Personalization Options*



Widgets

Allows you to add Widgets to your Dashboard. See “Add a Widget” on page 14.

Layout

Allows you to change the Dashboard layout. See “Change the Dashboard Layout” on page 17.

Cancel

Cancels all the changes made to your Dashboard.

Save

Saves your changes and applies to your Dashboard.

Add a Widget

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

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

Add General Widgets

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

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

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

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

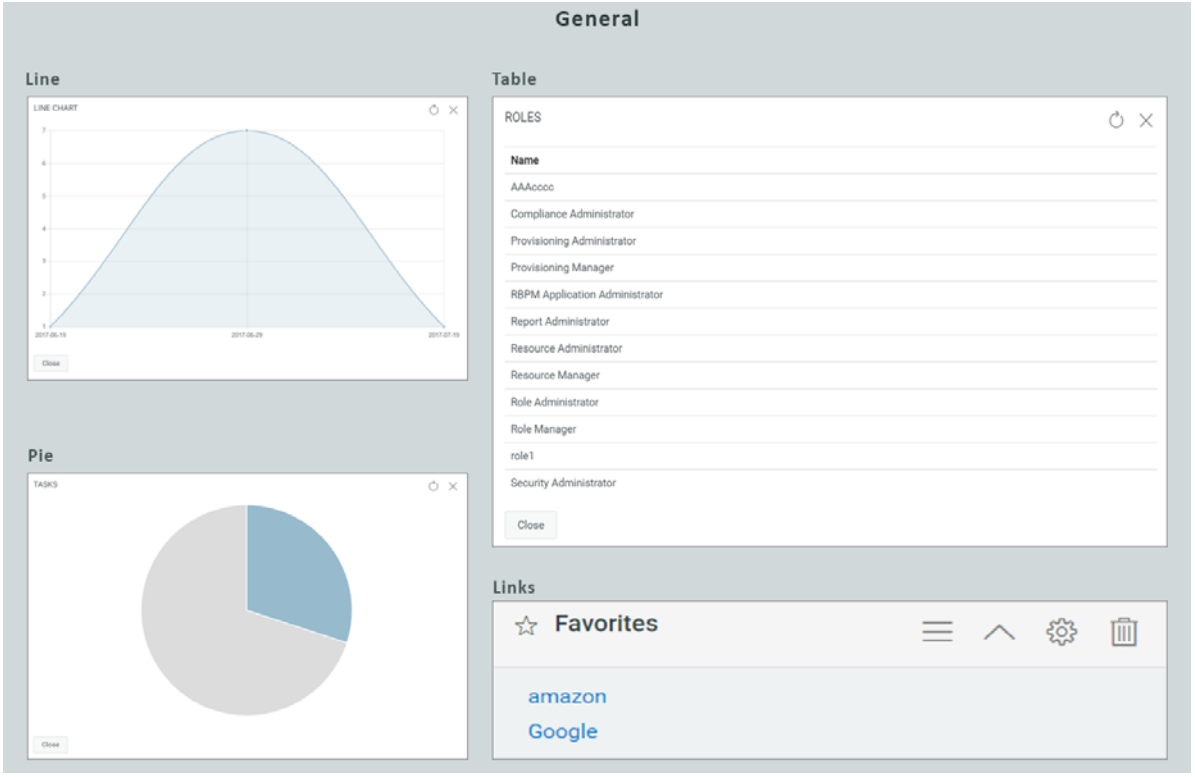
In this sample, assignments is the Root element and name is the selected column to display that will be displayed on the widget. You can also bookmark any URL that you wish to access from your Dashboard

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

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

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

Figure 3-2 *Example for General Widgets*



Add Identity Manager Widgets

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

For example,

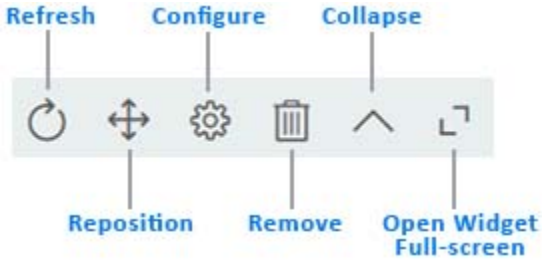
- **Access:** Displays the count of roles and resources, and other information about them.
- **Request For Others:** Displays pending and denied requests for other users and allows you to create request for these users.
- **Self Requests:** Displays the pending and denied requests count and also allows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

To configure these widgets, see “Configure a Widget” on page 17.

IMPORTANT: To apply your changes, click Save.

Widget Options

You can perform the following operations on widgets:



Refresh

Updates the widget content with the latest information.

Reposition

Allows you to move the widget across dashboard.

Configure

Allows you to configure the widget properties. For more information, see “Configure a Widget” on page 17.

Remove

Deletes the widget from the dashboard.

Collapse

Hides the widget information and shows only the widget title.

Open Widget Full-screen

Displays the widget information in full-screen mode.

NOTE

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

Configure a Widget

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

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

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

To configure **General** widgets, see “Add General Widgets” on page 14.

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

Change the Dashboard Layout

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

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

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

Permissions

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

4 Review Your Permissions

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

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

NOTE: The type of permissions listed on the permissions page may vary, depending on how the administrator has configured the settings for this page. For more information, see "User Settings" on page 70.

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

NOTE: **Permissions** allows you only to view and revoke permissions assigned to you. To request a role, resource, or PRD, go to **Access > Requests**. To view a history of your requests, go to **Access > Requests History**.

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

For more information about this software product, see the NetIQ Identity Manager documentation.

Review the Details of a Permission

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

The following table lists the fields displayed for individual permission:

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

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

Find a Permission of Self

By default, **Permissions** lists all of your assigned permissions under **Self** tab. To find a specific permission, change the search criteria to **Role** or **Resource**.

To filter the search for **roles**, specify any of the following criteria under **Role Filter(s)**:

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

To filter the search for **resources**, specify any of the following criteria under **Resource Filter(s)**:

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

Find a Permission of Others

If you are a team manager or supervisor, you can search and view permissions of other team members.

1. On the **Permissions** page, click **Others**.
2. You can search **By User** or **By Permission** names.
   - **2a** (Conditional) If you are searching **By User**, enter the user name.
   - **2b** (Conditional) If you are searching **By Permission**, enter the permission details.

Remove a Permission

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

To revoke any of your permissions:

1. Select the permissions that you want to revoke.
2. Click .
3. Specify a reason for removing the selected permissions.
4. Click **Revoke Permission(s)**.

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

1. In **Others**, search for the permissions that you want to revoke. You can search **By User** or **By Permission** names.
   - **1a** (Conditional) If you are searching **By User**, select the permission that you want to revoke.
   - **1b** (Conditional) If you are searching **By Permission**, select the user whose access to be revoked.

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

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

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

   You can save your selection in the queue and revoke the permissions anytime. To revoke the permissions in the queue, click .
4. Specify the reason for removing the selected permissions.
5. Click **Revoke Permission(s)**.

Customize Columns

You can customize columns and reorder the sequence of columns.

1. Click to customize the columns.

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

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

---

5 Request Permissions

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

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

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

To request permissions, select **Access > Requests**. For more information about this software product, see the NetIQ Identity Manager documentation.

Request Permission(s)

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

You can request permissions in the following ways:

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

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

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

To request only Identity Manager permissions:

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

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

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

3 Specify a reason for the request.

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

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

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

---

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

Secondary forms

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

Justification for Conflicting Roles

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

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

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

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

7 Select **Request**.

To request Identity Manager and Identity Governance permissions:

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

1 Select **New Request**.

- By default, the request for Self is displayed. The following tabs are displayed:

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

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

IG Technical Roles: Lists all the technical roles of the Identity Governance. Select the IG roles that you want to request for and specify a reason for requesting the role.

- (Conditional) To request access on behalf of other individuals, select **Others**, then specify the recipients (user, group, or team) and the permission associated with the selected recipient.

2 Click **Request** to complete the request.

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

Find a Permission to Request

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

Manage Featured Items

An administrator has access to create a category and add, delete, or edit permissions in that category. To create a category, click  .

Add a Permission

1 In **New items**, click **+**.

2 Select a **Permission** from the list that you want to add in the featured items list.

3 (Conditional) You can sort permissions by **Closest match** or **Alphabetical**.

4 In **Add to Category**, select a category that you want to add a permission.

If you do not specify the category, this item appears in the **New items** panel. Drag and drop this item on to any categories that you wish to add.

5 (Conditional) **Select image** for the specified permission, this image appears on the added permission.

6 Click **Add**.

Delete a Permission

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

Edit a Permission

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

6 Review a History of Requests

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

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

NOTE: **Requests History** shows the requests for access and to cancel pending requests. To gain permission for a role, resou100

rce, or process, go to **Access > Requests**. To revoke your access, go to **Access > Permissions**.

To view your history, select **Access > Requests History**. For more information about this software product, see the NetIQ Identity Manager documentation.

Review the Details of a Request

For each request, you can view not only your actions but also the workflow involved in approving or denying your request. Each step in the process has a timestamp.

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

User

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

System

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

User and System

Actions and comments by both users and the application.

Find a Request of Self

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

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

- Item requested
- Type of request: role, resource, or process
- Confirmation number of the request
- Specific date or range of dates

Find a Request of Others

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

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

   - Item requested
   - Type of request: role, resource, or process
   - Confirmation number of the request
   - Specific date or range of dates

Raise a Helpdesk Ticket

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

NOTE: You can also raise a helpdesk ticket in the **Request** page. See, Chapter 5, “Request Permissions,” on page 25.

Cancel a Request

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

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

Customize the View

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

To change the displayed categories:

1. In the view that you want to modify (table or list), select **Customize**.
2. Select the categories that you want to see.
3. (Optional) Change the display order of the categories.
4. Select **Apply**.

IV Tasks

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

- Chapter 7, "View and Manage Tasks," on page 33
- Chapter 8, "Act as or Assign a Proxy," on page 37
- Chapter 9, "Manage Approvals by Email," on page 39

For more information about this software product, see the NetIQ Identity Manager documentation.

7 View and Manage Tasks

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

Viewing your Tasks

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

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

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

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

- You can search your tasks using **Reassigned Tasks**, **Returned Tasks**, or **Delegated Tasks** filters. Using **Delegated Tasks** filter for the **Self** option displays only the tasks that are delegated to you.
- If you are an administrator, you can also filter tasks using **Assigned to me**, **Recipient as me** filter.
- If you are searching others tasks you can use **Returned Tasks**, **Reassigned Tasks**, or **Delegated Tasks** filter. Using **Delegated tasks** filter for **Others** shows all the tasks that are delegated to other users in the system.
- You can also refine your task search based on tasks occurred in the system:
  1. Select  .
  2. (Conditional) To see the tasks created for a certain period, specify the period in **Weeks**, **Days**, or **Hours**.
  3. (Conditional) Specify the task status that you wish to filter.
  4. Click **Filter**.
- If you are a helpdesk user, you can use **Helpdesk Tasks** filter to see the refined list. To manage helpdesk task, see the Dashboard help.

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

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

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

Approve and Deny Requests

One Request at a Time

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

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

Multiple Requests at the Same Time

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

   NOTE

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

Managing Requests for Approval or Denial

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

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

Claim Request

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

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

Release Request

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

Reassign Request

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

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

If you are a team manager, you can reassign the team tasks including yours to other team members through the **Others** tab. Go to **Others** tab, select the required request check box and click **Reassign**. On the modal window, select the team member whom you want to reassign the task from the **Assign to** drop-down menu, and provide a comment for reassignment. Click **Reassign**. The task is reassigned to the selected team member.

NOTE

- To reassign a claimed request, first release the request and then reassign it.
- You can reassign a task to the manager who belongs to the defined hierarchy. For more information, go to **Your ID > Settings > Customization > General**. An administrator who can access the **Settings** page has the permission to change the hierarchy. For more information, see "Customize the Views" on page 68.

Return Request

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

NOTE: Only a reassigned request can be returned.

Manage Helpdesk Tasks

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

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

---

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

   Update

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

   Complete

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

   Cancel

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

Customize Columns

You can customize and change the sequence of the columns.

1. Click  to customize the columns.

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

NOTE: If you want to restore the default columns, click **Restore Defaults**.

---

8 Act as or Assign a Proxy

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

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

For more information about this software product, see the NetIQ Identity Manager documentation.

Act as a Proxy

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

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

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

Manage Proxy Assignments

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

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

   Proxy assigned

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

   Proxy as

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

   Expiration

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

9 Manage Approvals by Email

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

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

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

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

Configuring Email-based Approvals

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

NOTE: Before enabling email-based approvals, ensure that you have configured the provisioning request definitions (PRDs) to support notifications and (optional) digital signatures. Also, configure the outgoing mail server. For more information, see the *NetIQ Identity Manager - Design Guide to the Identity Applications*.

- **Server Type**

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

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

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

  NOTE

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

- **Email**

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

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

  Specifies whether the incoming mail server requires authentication.

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

User ID

Specifies the account required for server authentication.

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

Password

Specifies the password for the account.

- **Folder**

  Required for an IMAP server

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

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

- **Enable SSL**

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

- **Use default port**

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

- **Polling Interval**

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

- **Token Expiration**

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

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

- **Cleanup Interval**

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

- **Email Content Options**

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

  Exclude action links

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

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

  Include action links without digital signature

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

  Include action links with digital signature

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

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

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

  You can also modify these terms for all supported languages.

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

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

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

- **Enable Socks Proxy**

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

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

  Proxy Host

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

  Proxy Port

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

  Authentication Required

  Specifies whether the proxy server requires authentication for incoming mail.

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

To configure email approvals, select **Administration > Email-based approval**. For more information about this software product, see the NetIQ Identity Manager documentation.

V Teams

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

Requester

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

Also manages the proxy assignments for team members.

Recipient

Member of the team on whose behalf requesters can act.

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

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

For more information about this software product, see the NetIQ Identity Manager documentation.

10 View Teams

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

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

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

Create a New Team

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

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

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

Modify an Existing Team

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

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

11 Add 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 about teams, see Teams. For more information about this software product, see the NetIQ Identity Manager documentation.

Create a New Team

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

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

   All Users

   Includes all user accounts in the directory.

   Relationship

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

   Members

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

Add Permissions to the Team

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

- "Add Resources and Roles" on page 48
- "Add Provisioning Request Definitions" on page 49
- "Enable Requesters to Make Proxy Assignments" on page 49

Add Resources and Roles

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

   All

   Applies only for resources

   Makes all resources available for assignment to team recipients

   Select

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

   Sub-containers

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

   Exclude Roles from Selected Containers

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

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

   Exclude Resources

   Applies only for resources

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

   View

   Allows the requester to view the resource or role

   Assign

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

   Revoke

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

   Assign role to group and container

   Applies only to roles

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

   Revoke role from group and container

   Applies only to roles

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

Add Provisioning Request Definitions

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

1. While in the **Create Team** page or when modifying an existing team, select **Add Permission**.
2. Select **Add Provisioning Request Definitions**.
3. Specify PRDs that you want to add:

   All

   Makes all PRDs available for assignment to team recipients

   Select

   Makes only the specified PRDs available for assignment to team recipients

   Exclude

   Makes the selected PRDs unavailable for assignment to team recipients
4. Select one or more permissions that you want to grant to team managers:

   Initiate PRD

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

   Retract PRD

   Requesters can stop a PRD on behalf of a team member

   Configure Delegate

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

   Manage Addressee Task

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

   Configure Availability

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

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

   ---
5. Select **Add**.

Enable Requesters to Make Proxy Assignments

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

1. While in the **Create Team** page or when modifying an existing team, select **Add Permission**.
2. Select **Add User Application Driver Permissions**.
3. Select **Configure Proxy**.
4. Select **Add**.

Use Case Example

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

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

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

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

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

12 Modify a Team

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

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

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

For more information about teams, see Teams. For more information about this software product, see the NetIQ Identity Manager documentation.

VI Users and Organization Chart

The application enables you to perform the following activity:

- Chapter 13, “View and Manage Users,” on page 55

13 View and Manage Users

You can view users in a list or as cards. You can also search and filter **Users** to find specific individuals.

To view and manage users, select **People > Users**. For more information about this software product, see the NetIQ Identity Manager documentation.

Find a User

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

Simple

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

Filtered

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

Advanced

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

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

Create a User Profile

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

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

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

Modify a User's Profile

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

NOTE: In this release, you can create and edit a user's profile and contact information only.

To change the user's roles, resources, attributes, or groups, you must use the legacy `IDMProv` portal. For example, `123.45.67.890:8180/IDMProv/portal/cn/DefaultContainerPage/CreateUserOrGroup`.

1. In the list view, select the user whose profile you want to edit.
2. Select the edit icon.
3. Change the profile and contact information as appropriate.
4. Select **Save**.

View a User's Organization Chart

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

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

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

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

VII Delegation

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

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

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

- Provisioning Administrator
- Provisioning Manager
- Team Manager

To view and manage delegations, see Chapter 14, “View and Manage Delegations,” on page 59.

14 View and Manage Delegations

To create or modify delegation, you must be a Provisioning Administrator, Provisioning Manager, or a Team Manager. The Provisioning Administrator and Provisioning Manager have the ability to define delegate assignments for any user in the organization. For creating delegations, see "Create a Delegation" on page 59.

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

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

List Delegations

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

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

Create a Delegation

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

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

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

     The list displays the delegation relationship that was earlier created in Designer. For more information, see *Administrators Guide to Designing the Identity Applications*.

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

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

   This option is displayed only if **Set Availability while creating a Delegation Assignment** is enabled in **Settings > Customization > Navigation Items > General**.

6. (Optional) Enable **Notify other users of these changes** and select the users to notify about this assignment.
7. Set **Effective Date**.
8. (Conditional) To set the expiry date for delegation, select **Specify Expiration** and **Expiration Date**.

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

   NOTE: By default, **No Expiration** option is selected.
9. In **Request Type Selection**, select the request type that you want to delegate.

   This list displays the delegation relationship that was earlier created in Designer. For more information see *Administrators guide to Designing the Identity Applications*.

   All

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

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

   Attestations

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

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

   Entitlements

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

   Groups

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

   Roles

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

   For example the **Resource Assignment/Revocation Approval**, **Role Assignment/ Revocation Approval**, or **SoD Conflict Approval**, **Resource Provisioning/Deprovisioning workflow**
10. Drag and drop the required request type from **Available Requests** to the **Selected Requests** list.
11. Click **Submit**.

Modify Delegations

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

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

VIII Availability

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

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

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

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

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

To create or modify availability, see Specifying Your Availability.

15 Specifying Your Availability

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

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

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

View Availability Status

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

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

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

Change the Availability Status

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

Available for All Requests

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

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

Not Available for Any Requests

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

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

Not Available for Specific Requests

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

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

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

Create an Availability Setting

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

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

Edit an Availability Setting

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

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

IX Client Customization

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

- Chapter 16, “Customize the User Interface,” on page 67

16 Customize the User Interface

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

Select ***Your ID*** **> Settings**, then select the **client** that you want to manage. For more information about this software product, see the NetIQ Identity Manager documentation.

Manage Clients

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

You can modify the name and LDAP attribute match for each client that connects to `idmdash`. You can also create a new client and delete any client except the default client.

LDAP Filter to match represents the user root container that stores the account(s) for the User Application Administrator role. This setting enables the administrator to log in simply by username (instead of requiring the fully distinguished name each time). The User Application Administrator account does not need special directory rights because this role controls application-level access.

Control User Access

Access settings allow you to specify which user accounts are **trustees** for the different Identity Applications pages within the client. When a trustee logs in, the application displays the page that has been provisioned. Otherwise, the page remains hidden to the logged in user. You can add users, groups, roles and containers as trustees.

To control user access, select the client, then **Access**.

Considerations for Configuring User Access

When configuring user access, you should consider the following conditions:

- Make sure that the users specified in **Trustees** are having sufficient Identity Vault rights to perform tasks within the Identity Applications. However, the trustees can access the page but operations on the page will fail if they do not have the proper Identity Vault rights.

- Each **Navigation item** has a set of default trustees suitable for the services that can be accessed through that page. However, if you remove all trustees for a navigation item, every user will be able to access that page.
- If a user does not have access to the default navigation (or to the default menu item within a navigation area), the application redirects the user to the **Dashboard** page. The application might also display an error message, such as when a user attempts to login to page without proper authorization. The user can log in but will be directed to the **Dashboard** page.
- When a user is in **proxy** mode, the application provides access according to the permissions for the account being proxied, as opposed to the permissions for the logged in user. The proxy can perform tasks on behalf of the other user but does not assume any of the role-type permissions. For example, a user cannot perform Domain Administrator functions on behalf of a Domain Administrator unless that user also has that role.

Configuring User Access

Before configuring user access, review Considerations for Configuring User Access.

1. Expand the required **Page** item that you want to provision access to the users, groups, roles, or containers.

   Navigation items are listed based on the look and accessibility of the page in Identity Applications user interface.
2. Specify one or more trustees for the selected **Page** item.

   For example, roles such as Helpdesk or IT Operators should be trustees for **Groups**. Expand **People > Groups** item and assign trustees to this page item.

   NOTE: **Password Sync Status** is listed under **People** item. You should expand **People** item to modify trustees for **Password Sync Status**.

   In some cases, you might specify a user as a trustee but the application does not display that user's name in the trustee list. This occurs because that user is a member of a group or a role that is already listed as a trustee. The application does not list the user twice.
3. Select **OK**.
4. To make one of the navigation items the default for that type of page item, enable **Area default** for that item.
5. Click **Save**.

Customize the Views

Enables you to configure the items displayed on the **Users** page for the selected client. You can also specify general settings for notifications and request forms.

- "General Settings" on page 69
- "User Settings" on page 70
- "Entity Settings" on page 71

To customize the views, select the client, then **Customization**.

General Settings

The **General** settings specify how the client responds upon user login and when the user initiates forms.

Notification Expiry

Specifies the number of days before a task or role expires that the application begins displaying a notification when the user logs in.

Enable Task Bulk Approval

Allows the client users to approve or deny multiple requests at a time.

Disable Implicit Claim of Task

Specifies whether it is mandatory for the user to claim a task before approving or denying it. By default, this flag is set as false; user can approve or deny the task without claiming it. If you set this flag as true, user must claim the task explicitly. In this case, the approval and deny options are not displayed until the task is claimed by a user. The functioning of **Disable Implicit Claim of Task** option also applies to bulk approval of tasks.

Set Availability while creating a Delegation Assignment

Specifies whether the application displays options for providing the availability details when the user creates a delegation. When selected, the application displays the availability options at the same time when the delegation is created. If you want to create delegation and specify availability details in separate actions, do not select this option.

Show Add Workflow in Roles Page

Enabling this setting displays the **Add Workflow** action in the **Roles** Page. By default, it is enabled.

Show Add Workflow in Resources Page

Enabling this setting displays the **Add Workflow** action in the **Resources** Page. By default, it is enabled.

Feedback Message Span

Specifies the period for a information message to appear on the page.

Identity Governance URL

Specifies the Identity Governance URL.

Managers Hierarchy

Specifies the manager's hierarchy. This helps the helpdesk users to reassign the helpdesk tickets to the managers of the specified level. You can set the hierarchy up to 3.

Organization Chart separator for multi-valued attributes

Specifies the character or symbol that the application will use to separate values when displaying a multi-valued attribute for an entity (user or custom) in the **Organization Chart** page. By default, comma is used.

Enable Eager Search Results in Roles and Resources Page

Enable this option to display the roles in the Roles page and the resources in the Resources page. By default, this option is enabled. Disabling this option will not display the roles and resources when the Roles and the Resources pages are loaded.

Organization Chart hierarchy depth

Specifies the maximum depth of the organization chart that the application can display for a user relationship in the **Organization Chart** page. An organization chart hierarchy depth of 3, for example will display the hierarchy of a user up to level 3 from the root user for a given relationship.

User Settings

The **User** settings enable you to configure the attributes displayed in the **Users** page for the selected client.

Card View

Represents the attributes that you want the application to display by default when the user selects **Card View** in the **Users** page.

Other Attributes

Represents additional attributes that provide details about a selected user.

Editable Attributes

Represents the attributes that can be modified for a user's details. For most attributes, you can also enter text to serve as default values or examples to aid in new user creation, as desired.

User Default Photo

Represents the image that you want the application to display by default when you enable the image toggle button in the **Card View** on **Users** page.

User Search Lookup Attribute

Represents the attributes that users can define when searching for a user entity. It applies to the fields that use the DN Lookup widget in Identity Applications Dashboard.

User Search Default Attribute

Represents the attributes that users can define when searching for a user or filtering search results in the **Users** page.

User General Settings

Represents the default container for storing users and how the application responds when displaying search results.

- **Base Container**

  Specifies the container in the Identity Vault that stores a newly created user.

  When creating a user, you can see this value but cannot modify it. This limitation ensures that all users are stored in the same container for that client.

- **User List Container**

  Specifies the container in the Identity Vault that you want the application to use for listing users in the **Users** page.

- **User Profile Entity**

  Specifies the entity that the application will display in the **My Profile** page. By default, the user entity is displayed.

- **Show All Permissions**

Enable this setting to list all permissions assigned to the user on the **Permissions** page. This include permissions directly assigned to the user and those assigned indirectly through groups or containers. By default, this settings is disabled, allowing the user to see the list of direct assigned permissions only.

- **User Search Limit**

  Specifies the maximum number of users that the application can list as a result of a user search.

- **Default Organization Chart Relationship**

  Specifies the relationship that the application will display by default in the **Organization Chart** page. By default, it is set as Manager-Employee.

  In addition to the default relationships provided with Identity Applications installation package, the administrator can also create custom relationship in the Directory Abstraction Layer using the Designer. For more information see Administrators Guide to Designing the Identity Applications.

- **View Permissions Type**

  Enable the permission types such as **Roles**, **Resources**, and **PRD**. This allows your client users to view or request the permission types that are selected.

  By default, all the permission types are enabled.

- **Enable Role Approval**

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

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

Entity Settings

You can configure the entities that are added to Identity Applications through Designer.

1. (Conditional) To configure an entity, Click **+**
2. (Conditional) If you want to modify the settings for a configured entity, select the required entity from the **Navigation items** list.
3. Specify the following details:

   View Attributes

   Drag and drop the required attributes into **Selected Attributes** from **Available Attributes**.

   These attributes are displayed when you select this entity from the **Entities** menu.

   Editable Attributes

   Specify the attributes that can be modified for an entity.

   You can specify one or more editable attributes.

   Search Attribute

   Specify the attributes to search records for an entity.

   You can specify one or more search attributes.

   Base Container

   Specify the container where you want to store the objects created for this entity.

For example,

If you select **data > group** container to the **group** entity, the groups created using this entity will be stored under **group** container.

Default Organization Chart Relationship

Specify the relationship that will be displayed in the organization chart page for this entity.

Organization Chart View

Drag and drop the required attributes into **Primary Attributes** and **Secondary Attributes** from **Attributes** field.

These attributes are displayed when you want to view the organization chart for this entity under the **Entities** menu.

Display Attributes for Organization Chart Search

Specify the display attributes for organization chart search results. A maximum of two attributes are allowed for selection.

Organization Chart Photo

Specify the attribute whose value will be used to display the image for this entity in the organization chart under the **Entities** menu. If an attribute has multiple values, the first value is selected for display by default.

4 Click **Save**.

Customize the Branding

For each client, you can customize the following look and feel attributes:

- Change the logo, title, and colors in the page header.
- Specify the URL that the application displays when a user clicks the page title or footer.
- Add links and contact information to the footer or disable the page footer.
- Localize the content in the header and footer.
- Specify a customized cascading style sheet (CSS).

To use a CSS, you can modify the sample under **Advanced Settings**.

1 Click **Download Sample CSS**, to download the sample `Custom.css` file.

2 Modify the `Custom.CSS` file values and click **Upload CSS**.

To customize the branding, select the client, then **Branding**. For more information, see the NetIQ Identity Manager documentation.

Client Helpdesk Settings

For each client, you can setup a **Helpdesk** to assist their users.

1 Specify **Helpdesk Name**.

2 Specify the **Email Address** of the helpdesk.

3 Specify the **Contact Number** of the helpdesk.

4 Click **Add** to add more contact numbers.

5 Enable **Show in Footer** to display the helpdesk information in the footer of user's page.

6 Enable **Show in Request History** to display the helpdesk information in the Request History page.

7 Enable **Show in Menu** to display the helpdesk information in the Dashboard menu.

8 Provide **Access Rights** to the selected users for the following Helpdesk resources:

Organization Chart Access

Selected users can view the organization chart of respective client.

Group Access

Selected users can view groups of respective client.

Reassign Access

Selected users can reassign the user's tasks to the approver's managers.

NOTE: You can configure **Managers Hierarchy** in **Customization**, this helps the helpdesk users to reassign the user's tasks to the managers of the specified level, if necessary.

Teams Access

Selected users are allowed to view teams and team members configured for respective client.

History Access

Selected users can view request history of any user of respective client.

User Catalog Access

Selected users can view details of any user of respective client.

Manage Dashboard Widgets

In **Dashboard Widgets**, you can provision widgets for a User, Group, Container, or a Role.

Widgets

Lists all widgets available in the system.

Trustees

Allows you to select Users, Group, Container, and Roles that you wish to provision this widget on their Dashboards.

Order

Specifies the order in which the widget should display on the dashboard. You can drag the widgets up and down to rearrange the order. By default, the widgets are displayed in the order mentioned in this page. Users can personalize the order after adding widgets to their dashboards.

Contents