Identity Manager

Using the Identity Applications

May 2020

NetIQ

Legal Notice

Roles and Resource Administration

This application enables you to perform the following activities:

1 View and Manage Roles

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

- Role Administrator
- Role Manager

List Roles

You can view roles in a list. You can also search and filter **Roles** to find specific roles. By default, all roles are displayed on this page. If you want to change the display settings, go to **Your ID** > **Settings** > **Customization** > **General** and select the **Enable Eager Search Results in Roles and Resources** Page as required.

Find a Role

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

Simple

Enter any role name or description.

Filtered

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

You can sort roles based on the columns.

Customize Columns

You can customize columns and reorder the sequence of columns.

1. Click  to customize the columns.

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

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

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

Create a Role

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

You can specify **Name** and **Description** for the role in different languages. See, “Change Language” on page 6.

IMPORTANT

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

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

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

4 Click **Create Role**.

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

Change Language

By default, user-defined locale is selected.

1 Click **Show Languages**.
2 Specify the value for required language.
3 Click **Apply**.

Edit Roles

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

Editing Individual Roles

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

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

Editing Multiple Roles at once

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

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

Change the Approval or Revocation Process

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

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

   Serial

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

   Quorum

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

   Custom

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

   Retain Existing Approval Process

   Retains the default process for the selected roles.

   Same as Grant Approval

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

   None

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

Map Resources to the Role

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

- **Edit Roles:** When you select a role to edit, it displays the mapped resources for the selected role under the **Map Resources to Role** tab. You can select the required resources or entitlements from the **Available Resources and Entitlements** list.
- **Roles:** Click  icon to map resources to the required roles and perform the following steps:
  1. Select the role from the roles list.
  2. Drag and drop the resources/entitlements that you want to map from the **Available Resources and Entitlements** list to **Mapped Resources**.
  3. Specify the **Mapping Description**.
  4. Click **Apply**.

Assign Role to the Users

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

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

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

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

Map Role to Role

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

Parent Roles

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

Child Roles

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

To add a parent role for the selected role:

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

To add a child role for the selected role:

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

Add Workflow to Roles

Add Workflow, a new option introduced in the Roles page, allows you to add a workflow to the role. By default, it is enabled.

To add a workflow, select the check box for the desired role and click **Add Workflow.** For more information, see Adding a Workflow in *NetIQ Identity Manager Administrator's Guide to the Identity Applications*.

2 View and Manage Resources

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

- Resource Administrator
- Resource Manager

List Resources

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

Find a Resource

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

Simple

Enter the resource name or description.

Filtered

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

You can sort the resources based on the columns.

Customize Columns

You can customize the columns and reorder the sequence.

1. Click  to customize the columns.

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

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

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

Create a Resource With Entitlement

1. Select **+**.
2. Select the **With Entitlement** option.

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

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

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

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

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

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

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

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

5 Click **Create Resource**.

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

6 (Conditional) Rename the **Resource Name** field to a valid name if it is containing any of these `[ < > , ; \ " + # = / | & * ' ! @ $ % ]` special characters or a whitespace.

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

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

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

8a Enable **Expiration Required**.

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

8c Click **Apply**.

Create a Resource Without Entitlement

1 Select **+**.

2 Select the **Without Entitlement** option.

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

You can specify **Name**, **ID**, and **Description** for a resource in different languages. See, “Change Language” on page 6.

IMPORTANT

- Do not use these `[ < > , ; \ " + # = / | & * ' ! @ $ % ]` special characters or a whitespace in the **ID** field.
- Do not use these `[ < > , ; \ " + # = / | & ]` special characters or a whitespace in the **Name** field.

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

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

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

5a Enable **Expiration Required**.

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

6 Click **Create Resource**.

Edit Resources

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

Editing Individual Resources

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

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

Editing Multiple Resources at once

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

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

Assign Weightage to the Resources

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

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

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

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

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

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

Change the Approval or Revocation Process

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

1. Select the necessary resources from the list that you want to change.

   NOTE: If you want the role approval to override the resource approval process. Enable **Role Approval overrides Resource Approval**.
2. (Optional) If you want the role approval to override the resource approval process. Enable **Role Approval overrides Resource Approval**.

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

   Serial

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

   Quorum

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

   Custom

   Select the customized workflow that you want to use from the list. The list displays the workflows that are defined using Designer. For more information about workflow, see Start workflow in *NetIQ Identity Manager - Using Designer to Create Policies*.
4. Select the **Revoke Approval Process** from the list.

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

5a Enable **Expiration Required**.

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

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

6 Click **Apply**.

Assign Resource to the Users

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

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

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

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

5 Click **Assign Resource**.

Resource Form

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

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

2 Change properties of the field.

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

NOTE: To modify the languages for the **Display Label**, see “Change Language” on page 6

4 Click **Apply**.

5 Click **Save**.

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

Add Workflow to Resource

Add Workflow, a new option introduced in the Resources page, allows you to add a workflow to the resource. By default, it is enabled.

To add a workflow, select the check box for the desired resource and click **Add Workflow.** For more information, see Adding a Workflow in *NetIQ Identity Manager Administrator’s Guide to the Identity Applications*.

Configuration

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

You can configure the default settings of the following components:

3 View and Configure Roles and Resources Settings

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

Role Settings

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

Role Container

The container where all the roles are stored.

Role Request Container

The container where all the role provisioning requests are stored.

Default Role Approval Definition

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

Role Assignment Grace Period

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

Role Level Display Names

You can change the display names of Role Levels for all supported languages. To change the language, see "Change Language" on page 6.

Click **Apply** to save your changes.

Resource Settings

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

Resource Container

The container where all the resources are stored.

Resource Request Container

The container where all the resource provisioning requests are stored.

Default Resource Approval Definition

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

Entitlement Query Settings

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

Default Query Timeout

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

Default Refresh Rate

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

Refresh Status

Indicates whether the entitlement values have been refreshed.

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

Click **Apply** to save your changes.

Separation of Duties Settings

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

SoD Container

The container where all the SoD constraints are stored.

SoD Approval Definition

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

This list displays the SoD approval definitions created using Designer. For more information, see *Administrators guide to Designing the Identity Applications*.

Default Approval Type

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

Default SoD Approvers

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

Click **Apply** to save your changes.

4 View and Configure Delegation and Proxy Settings

View and Configure Delegation Settings

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

- Provisioning Administrator
- Provisioning Manager

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

---

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

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

   This list displays the delegation templates created using Designer. For more information, see *Administrators guide to Designing the Identity Applications*.
5. Select the **Availability Notification Template** from the list.

   This list displays the availability templates created using Designer. For more information, see *Administrators guide to Designing the Identity Applications*.
6. Click **Submit**.

View and Configure Proxy Settings

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

Retention time for Proxy assignments

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

Proxy notification template

Select the proxy template from the list. This list displays the proxy templates that are created using Designer. For more information, see *Administrators guide to Designing the Identity Applications*.

Click **Apply** to save your changes.

View and Configure Synchronization and Cleanup Service

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

Synchronization Service Activation Interval

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

Cleanup Service Activation Interval

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

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

Click **Apply** to save your changes.

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

---

5 Enable and Configure Permission Reconciliation Service

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

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

To view system resources, go to **Administration > Resources**. For more information, see "View and Manage Resources" on page 9.

To add or modify the permission reconciliation settings of connected applications, go to **Administration > Permission Reconciliation**. For more information, see Part VI, "Controlled Permission Reconciliation Services," on page 57.

By default, Permission Reconciliation option is enabled.

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

Polling time for status checker

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

By default, this interval is set to 60 minutes.

Retention time for computed permission assignments

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

By default, this period is set to 7 days.

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

6 View and Configure Log Events

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

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

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

Change Auditing Service Settings

Auditing Configuration allows you to enable or disable CEF format.

Enable CEF format

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

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

Add an Identity Manager Package

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

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

To add a package:

1. In **Logging Configuration**, click +.
2. Search for the package name that you want to add.
3. Select the package from the list.

4 (Conditional) Select the **Log level** for the package. See, "Change the Log Levels for Identity Manager Packages" on page 24

5 Click **Add**.

Change the Log Levels for Identity Manager Packages

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

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

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

2 Select the log level from the list.

Table 6-1 *Types of Log Levels*

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

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

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

4 Click **Apply**.

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

7 View and Manage Cache Events

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

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

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

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

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

Flushing Caches

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

View and Manage Cache Settings

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

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

Basic Cache Settings

Settings	What to do
Lock Acquisition Timeout	Specify the time interval (in milliseconds) that the cache waits for a lock to be acquired on an object. You might want to increase this setting if the Identity Applications imposes a lot of lock timeout exceptions in the application log. The default value is 15000 ms.

Settings	What to do
Wake Up Interval Seconds	Specify the time interval (in seconds) that the cache eviction policy waits before invoking the following activities: ◆ Processes the evicted node events. ◆ Cleanup the size limit and expired nodes.
Eviction Policy Class	Specify the classname for the cache eviction policy that you want to use. The default is the LRU eviction policy that JBoss Cache provides: `org.jboss.cache.eviction.LRUPolicy` If appropriate, you can change this to another eviction policy that JBoss Cache supports.
TIP: In Local Settings, select Enable Local for the required settings to override the global settings and specify the values.	

Non Customizable Cache Settings

Settings	What to do
Max Nodes	Specify the maximum number of nodes allowed in the cache. If you don't want restrict the number of nodes, specify `0`.
Time To Live Seconds	Specify the time to idle (in seconds) before the node is swept away. If you don't want restrict the Time To Live Seconds, specify `0`.
TIP: In Local Settings, select Enable Local for the required settings to override the global settings and specify the values.	

Click Save to save your configuration values.

Customizable Cache Settings

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

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

   NOTE: The system clears the events in the cache according to the value specified for Max Age.
3. (Conditional) In Local Settings, select Enable Local for the required settings to override the global settings and specify the values.
4. Click Save.

View and Manage Cluster Cache Configuration

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

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

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

8 Assign Administrators in Identity Applications

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

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

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

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

Listing the Administrator Assignments

Administrator Assignments displays the existing administrator assignments in the system.

- "Find an Administrator Assignment" on page 29
- "Customize Columns" on page 30

Find an Administrator Assignment

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

All

Displays all administrator assignments in the system.

User

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

Group

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

Container

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

Role

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

Customize Columns

You can customize columns and reorder the sequence of columns.

1. Click ⚙ to customize the columns.

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

   By default, **Domain** and **Assignee** columns are displayed.
3. Click **Apply**.

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

Create a New Administrator Assignment

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

1. Click +.
2. Specify the **Initial Request Description** that describes the purpose of this assignment.
3. Select the **Domain Type** from the list.

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

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

   This displays the list of users, groups, container, or roles based on the selected assignment type.
5. Select the required user, group, container or a role on from the provided list to create an assignment.
6. (Conditional) Specify the **Effective Date** for this assignment. If you do not specify any date, creates an assignment immediately.
7. (Conditional) Specify the **Expiration Date** for this assignment. If you do not specify any date, the expiration date is set to never.
8. (Conditional) To create a domain administrator assignment for the selected domain, enable **All Permissions**.

NOTE: This option cannot be edited after creating the assignment. For a delegated administrator, you can assign permissions individually. See, “Assign Permissions to a Delegated Administrator” on page 31.

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

9 Click **Create**.

Assign Permissions to a Delegated Administrator

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

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

2 In Permissions, click +.

3 Click **Add Permissions**.

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

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

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

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

To delete the assigned permissions,

1 Select the permissions that you want to delete.

2 Click 🗑.

Delete an Administrator Assignment

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

You can select multiple check boxes to delete multiple assignments.

2 Click 🗑.

9 View and Configure the Workflow Engine and Cluster Settings

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

Configure the Workflow Engine Settings

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

Engine Setting	Description
Enable Email Notification	Enables or disables email notifications for the entire workflow engine. Defaults to enabled.
Web Service Activity Timeout (minute)	Specifies the default Web Service activity timeout in minutes. The default is `50` minutes.
User Activity Timeout (hour, 0 for no timeout)	Specifies the default user activity timeout. The default is `0` days, which indicates no timeout.
Completed Process Timeout (day)	Specifies the number of days that a completed process state is kept in the workflow database system. The default is `120` days.
Completed Process Cleanup Interval (hour)	Specifies how often the engine checks for and removes completed processes that have been in the workflow database system for longer than the completed process timeout. The default is `12` hours.
Pending Process Interval (second)	User activities that are executed on an engine which the process is not bound to are put into a pending state. This interval specifies how often to check for pending activities in order to continue their execution. The default is `30` seconds.
Retry Queue Interval (minute)	Activities that fail because of suspected database connectivity issues are put on a retry queue. This interval specifies how often the engine attempts to retry these activities. The default is `15` minutes.
Thread Keep Alive Time (second)	If the pool is larger than the minimum size, excess threads that have been idle for more than the keep-alive time will be destroyed. The default is `5` minutes.
Maximum Engine Shutdown Timeout (minute)	The engine attempts to shutdown gracefully. When shutting down it stops queuing new activities for execution and attempts to complete any activities already queued. This timeout specifies the maximum time that the engine waits for all queued activities and threads executing activities to complete. If this time is exceeded, the engine halts processing of queued activities and attempts to stop all threads executing activities. The default is `1` minute.

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

Configure Workflow Cluster Settings

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

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

View the Workflow Engines State

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

SHUTDOWN

Indicates that the engine is shutdown gracefully.

TIMEDOUT

Indicates that accessing the engine is timed-out. This state depends on the specified Heartbeat Interval. See, “Configure Workflow Cluster Settings” on page 34.

STARTING

Indicates that the engine is starting.

RUNNING

Indicates that the engine is active.

10 View User Application Driver Status

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

Driver Name

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

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

Driver Version

Displays the driver version used in Identity Manager.

Application Revision

Displays the revised version of Identity Applications.

Patch Level

Displays the patch applied for the driver.

Build Revision

Displays the updated build version.

Status

Displays the driver state.

11 View and Configure the Default Provisioning Display Settings

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

View and Manage General Display Settings

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

Default number of results displayed per page

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

Options for number of results displayed per page

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

View and Manage the Appearance of Tasks Page

Field	Description
Select Column to set default sort	By default, the task results in the **Tasks** page are sorted by **Assigned To**. You can select a different column from the list to sort the task results. Also, you can sort the results by ascending or descending order. Use **Sort by Descending Order** to sort the results in descending order. Disabling this option displays the results in ascending order.
Allow user to customize columns	By default, this option is enabled. Disabling this option restricts the user from customizing columns in the **Tasks** page. ◆ **Available columns:** Displays the columns which are disabled for user customization. ◆ **User default columns:** Displays the columns that are already showing on the **Tasks** page. ◆ **Available columns for User customization:** Displays the columns that can be customized by users.
Allow user to customize task detail open	By default, this option is enabled. This option allows you to change the preferences of opening the approval form in the **Tasks** page. Go to **Tasks** page and click ⚙ to change the preferences. Disabling this option will restrict the system users from changing the preferences of opening the approval form in the **Tasks** page. However, you can change this preferences in the **Settings > Customization** page.

Click **Save** to apply your changes.

View and Manage the Appearance of Request History Page

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

Click **Save** to apply your changes.

Organization Chart

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

An administrator defines the default relationship to display in the **Organization Chart** page from the **Settings** page. In addition to the default relationships provided with Identity Applications installation package, the administrator can create custom relationship in the Directory Abstraction Layer using the Designer. For more information see Administrators Guide to Designing the Identity Applications.

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

12 View and Manage the Organization Chart

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

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

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

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

- Go to **People** > **Users** and select any user from the list and click  icon that is beside the user name. For more information, see Administrators Guide to Designing the Identity Applications.

NOTE: You should have **Org Chart** access to view the **Organization Chart**. Contact your administrator to provide this access.

Working With the Organization Chart

In the organization chart, a user, group, or other entity is represented in a format that resembles a business card. Using the business card of an entity, you can perform the following tasks:

These procedures are applicable to both user entity as well as custom entity.

Reset the Root in the Organization Chart View

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

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

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

Switch to the Organization Chart View

If you want to view a user's organization chart, then perform the following actions:

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

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

Choose a Relationship to View

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

   The relationship is displayed inline in the existing organization chart.

If no object is found for a given relationship, then a warning message is displayed in the **Organization Chart** page. For example, Sara Smith is a team manager who does not have any direct reports defined under her. If you want to view Sara Smith's organization chart for a Manager - Employee relationship, then the following message is displayed:

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

Navigate to the Next Level in Relationship Hierarchy

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

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

   NOTE: Before you perform this step, ensure that you select an appropriate relationship from the  icon.
3. Select the user from the list.

   The organization chart of the selected user is displayed.

Send Email to Users from the Organization Chart

The **Send Email** option allows you to send an email to a user or to all users within a team in an organization. You can also share user details such as email address, manager, direct reports, and assigned roles and resources by sharing a user profile link on email.

This section guides you how to:

- "Send User Profile Link on Email" on page 45
- "Send Email to Team" on page 45
- "Send Email to a User" on page 45

Send User Profile Link on Email

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

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

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

Send Email to Team

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

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

Send Email to a User

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

View Detailed Information of a User

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

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

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

IV Entities

You can manage one or more entities in your organization using Identity Applications. You can add entities to Identity Applications using Designer. For more information, see Adding Entities in *NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications*. Identity Manager Dashboard lists all the configured entities under the **Entities** menu.

To configure entities:

1. Go to **Settings** > **Customization**.
2. Click +.

For more information on managing entities, see Chapter 13, "Managing Entities," on page 49.

To see trustees who can access entities, go to **Settings** > **Access**.

1. Go to **Settings** > **Access**.
2. Search for **Entities** and view **Trustees**.

13 Managing Entities

In the **Entities** tab, click the entity for which you wish to create and manage objects associated with it.

For example, **Entities > <entity_name>**

Creating an Object

1. Click +.
2. Specify the details for the fields marked with an asterisk (*).
3. Click **Create**.

Editing an Object

1. Select the object you want to edit.
2. Click **Edit**.
3. Edit the required fields.
4. Click **Save**.

Deleting an Object

1. Select the object you want to delete.
   You can select one or more objects at a time.
2. Click .

Exporting an Object to a CSV file

1. Select the object for which you require the results to be exported to a CSV file.
   You can select one or more objects at a time.
2. Click .
3. Click **Save**.

Viewing Organization Chart of an Object

1. Select the object to view the organization chart.
   You can view organization chart of only one object at a time.
2. Click .

The organization chart of the object is displayed based on the default relationship set for that entity.

3 (Optional) If the **Default Organization Chart Relationship** for the entity is not defined in the **Settings** page, then a prompt to select the required relationship is displayed. Select the organization chart relationship from the drop-down list and click **View**.

14 Configure Identity Governance Settings

This page allows you to configure the Identity Governance settings:

Application URL

Displays the Identity Governance URL.

Administrator Username

Displays the username of the administrator.

Administrator Password

Specifies the administrator password.

Show IG Approvals in tasks page

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

Show IG Catalog in request page

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

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

Click **Apply** to save the changes.

V Groups

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

15 Manage Groups

To view the groups to which you belong, select **People > Groups**. For more information about this software product, see the NetIQ Identity Manager documentation.

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

Create a Group

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

Edit a Group

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

Delete a Group

Select the group that you want to delete and click .

You can only delete only one group at a time.

VI Controlled Permission Reconciliation Services

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

16 View and Manage Permission Reconciliation

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

To view system resources, go to **Administration > Resources**. For more information, see “View and Manage Resources” on page 9.

To configure the default behavior of Permission Reconciliation service, go to **Administration > Configuration > Permission Reconciliation**. For more information, see Chapter 5, “Enable and Configure Permission Reconciliation Service,” on page 21.

Controlled permission reconciliation allows you to perform the following tasks:

Monitor Permission Assignment Updates

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

Manage Permission Reconciliation

Click to manage permissions from the connected applications. This page displays all the configured resource details which are migrated from connected applications. For more information, see “Manage Permission Reconciliation” on page 60.

Compute selected driver/entitlement assignments

Click to compute the changes in permission assignments between Resource Catalog and connected applications on the selected driver or entitlement. The difference or changes in permission assignments between Resource catalog and connected applications is called as *Delta*. For more information, see “Compute the Selected Driver or Entitlement Assignments” on page 60.

Publish All

Click to initiate the migration from connected application to Resource Catalog. This migrates the permissions based on the settings defined in **Permission Reconciliation Settings** page. For more information, see “Publish Assignments for the Selected Driver or Entitlement” on page 60.

View the process status for the selected entitlement

Click to view the process status of all the new permissions that are added to the entitlement on the connected application. For more information, see “View the Process Status for the Selected Entitlement Assignments” on page 61.

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

Manage Permission Reconciliation

1 Click ⚙.

Displays all configurations made for permission reconciliation.

2 Click ✎.

3 Select the **Entitlement** that you wish manage.

4 (Conditional) To list the resources that allow users to choose entitlement values at the time of request, select **List Resources With Dynamic Value**.

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

5 Click **Save**.

This configuration is saved for the selected entitlement.

Compute the Selected Driver or Entitlement Assignments

1 In **Driver or Entitlement**, select the driver or entitlement that you want to initiate delta computation.

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

All Assignments

Shows all the assignments associated with the selected entitlement.

New Assignments

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

Revoked Assignments

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

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

Publish Assignments for the Selected Driver or Entitlement

1 In **Driver or Entitlement**, select the driver or entitlement that you want to initiate migration.

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

All Assignments

Shows all the assignments associated with the selected entitlement.

New Assignments

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

Revoked Assignments

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

3 (Conditional) To migrate only the selected assignments, click in **CPRS Assignments**.

4 Click to migrate all permissions for the selected driver or entitlement assignments.

View the Process Status for the Selected Entitlement Assignments

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

1 In **Driver or Entitlement**, select the entitlement for which you want to see the process status.

2 (Conditional) Select the required **CPRS Assignments** to see their process status. You can search for the CPRS assignments by name or permission or you can use the following filters to refine the search results:

All Assignments

Displays all the assignments associated with the selected entitlement.

New Assignments

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

Revoked Assignments

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

3 Click to view the process status of the selected entitlement assignments.

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

Process Type

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

Start Time

Specifies the start time of the process.

Completion Time

Specifies the completion time of the process.

Status

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

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

VII Separation of Duties (SoD)

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

17 Manage SoD

You can create a SoD and edit the SoD, if necessary. To edit the SoD, click the SoD and edit the necessary fields and click **Apply**.

- “Create SoD” on page 65

Create SoD

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

You can specify **Name**, **ID**, and **Description** for the SoD in different languages. See, “Change Language” on page 6.

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

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

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

2b (Optional) Enable **Use Default Approvers**.

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

2d Click **Create SoD**.