Identity Console

Administration Guide

January 2024

Legal Notice

Contents

24 Managing Driver Properties 153

About this Book and the Library

The *Administratin Guide* provides conceptual information about the NetIQ Identity Console (Identity Console) product. This book defines terminology and includes implementation scenarios.

For the most current version of the *NetIQ Identity Console Administration Guide*, see the English version of the documentation at the NetIQ Identity Console online documentation site.

Intended Audience

This guide is intended for network administrators.

Other Information in the Library

The library provides the following information resources:

Installation Guide

Describes how to install Identity Console. The book is intended for network administrators.

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions 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

Qmunity, 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, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 What Is Identity Console?

Identity Console is a state-of-the-art Web-based administration console that provides virtual, secure and customized access to network administration utilities from anywhere over the Internet and Web browser. Identity Console makes the decentralization of the administrative tasks much easier.

Features of Identity Console

Identity Console provides the following features:

- Administering eDirectory objects, users, schema, partitions, replicas, rights etc.
- Managing Identity Manager Drivers and Driver Sets
- Manage and view driver’s performance statistics
- Inspecting objects, viewing driver’s data flow, managing entitlements, work orders etc.
- Managing password synchronization status and settings for drivers
- Managing Password Policies and Login Methods
- Managing Certificates
- Administering various network resources
- Improved security measure to protect your data
- Improved scalability to manage larger eDirectory objects
- Secured login to the Identity Console portal via One SSO Provider (OSP)
- Built upon the latest UI technology in the Industry
- Easy to install and configure via Docker containers

2 How to Access Identity Console?

You can access the Identity Console and the complete set of features that it provides from any supported web browser. Although you might be able to access identity Console via a web browser not listed, we do not guarantee or support full functionality with any browser that is not officially supported.

IMPORTANT: For information about supported web browsers, see the *Identity Console Installation Guide*.

- "Accessing Identity Console" on page 17

Accessing Identity Console

To access the server-based Identity Console, perform the following steps:

1 Enter the following in the address (URL) field of a supported web browser.

Secure login: `https://<server-ip-address/hostname>:<port>/identityconsole/`

In the examples, the IP address in *<server-ip-address>* should be IPv4. The default port to use is 9000.

2 Login using your user dn and password.

3 Specify the eDirectory tree IP or DNS with or without ldap secure port.

NOTE:

- Refreshing any tab in Identity Console will logout the user for security reasons. If you want to change the browser refresh settings see: Configure Browser Refresh.
- Opening duplicate Identity Console tabs in browser will logout the user for security reasons.
- The dn should be specified in `cn=admin,ou=sa,o=system` format.
- When eDirectory is configured with non default port, you must specify the port number.

3 Navigating the Identity Console Interface

This section describes how to navigate through Identity Console web interface.

- “Identity Console Interface” on page 19

Identity Console Interface

The Identity Console Interface comprises of eDirectory and Identity Manager modules.

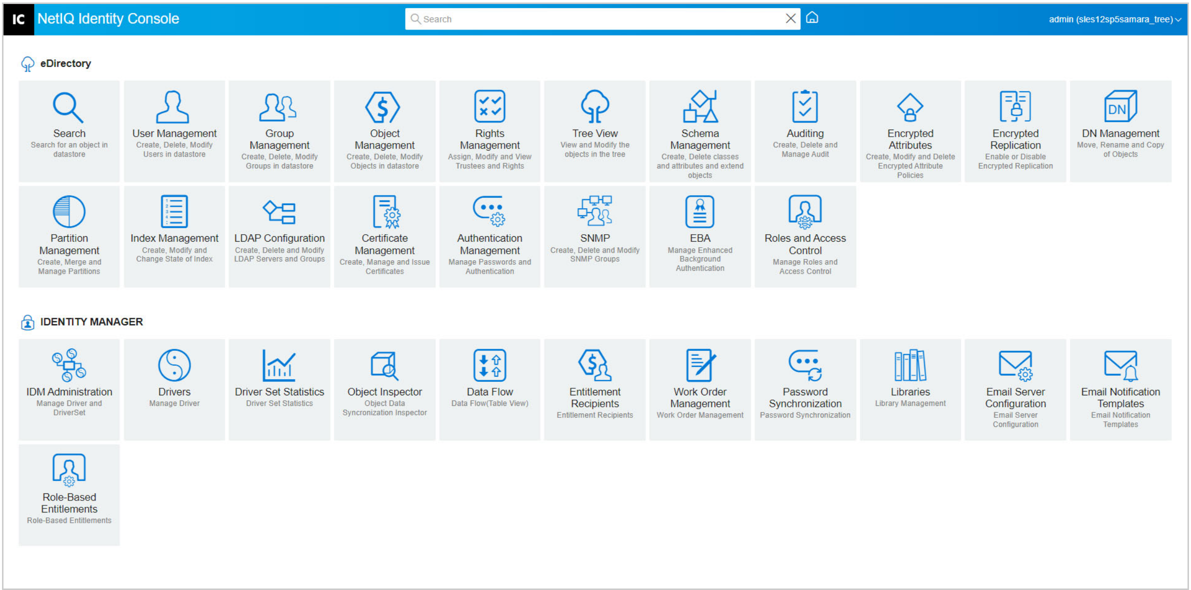

IC
NetIQ Identity Console
Search
admin (sles12sp5samara_tree)
eDirectory
Search
Search for an object in datastore
User Management
Create, Delete, Modify Users in datastore
Group Management
Create, Delete, Modify Groups in datastore
Object Management
Create, Delete, Modify Objects in datastore
Rights Management
Assign, Modify and View Trustees and Rights
Tree View
View and Modify the objects in the tree
Schema Management
Create, Delete classes and attributes and extend objects
Auditing
Create, Delete and Manage Audit
Encrypted Attributes
Create, Modify and Delete Encrypted Attribute Policies
Encrypted Replication
Enable or Disable Encrypted Replication
DN Management
Move, Rename and Copy of Objects
Partition Management
Create, Merge and Manage Partitions
Index Management
Create, Modify and Change State of Index
LDAP Configuration
Create, Delete and Modify LDAP Servers and Groups
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
Roles and Access Control
Manage Roles and Access Control
IDENTITY MANAGER
IDM Administration
Manage Driver and DriverSet
Drivers
Manage Driver
Driver Set Statistics
Driver Set Statistics
Object Inspector
Object Data Syncronization Inspector
Data Flow
Data Flow(Table View)
Entitlement Recipients
Entitlement Recipients
Work Order Management
Work Order Management
Password Synchronization
Password Synchronization
Libraries
Library Management
Email Server Configuration
Email Server Configuration
Email Notification Templates
Email Notification Templates
Role-Based Entitlements
Role-Based Entitlements

Figure 3-1 *Identity Console Interface*

IMPORTANT: Several GIF animations used in this guide work with the Online documentation only. In case you decide to switch over to the PDF, only screen shots will be visible.

Table 3-1 *Explanation of Various Modules of the Identity Console Web Portal*

Module Name	Description
Search	Search for an object in the datastore. For more information, see Chapter 4, “Performing Searches,” on page 25.
User Management	Create, delete and modify users in datastore. For more information, see Chapter 5, “Managing Users,” on page 27.

Module Name	Description
Group Management	Create, delete and modify groups in datastore. For more information, see Chapter 6, “Managing Groups,” on page 35.
Object Management	Create, delete and modify objects in datastore. For more information, see Chapter 7, “Managing Objects,” on page 41.
Rights Management	Assign, modify and view trustees and rights. For more information, see Chapter 8, “Managing Rights,” on page 47.
Tree View	View and modify the objects in the tree. For more information, see Chapter 9, “Tree View,” on page 51.
Schema Management	Create, delete classes, aux-classes, attributes and extend objects. For more information, see Chapter 10, “Managing Schema,” on page 55.
Auditing	Enable, disable and manage CEF auditing. For more information, see Chapter 11, “Managing Audit Events,” on page 63.
Encrypted Attributes	Create, modify, delete and view the encrypted attributes policy. For more information, see Chapter 12, “Managing Encrypted Attributes,” on page 69.
Encrypted Replication	Enable, disable and view the encrypted replication. For more information, see Chapter 13, “Managing Encrypted Replication,” on page 73.
DN Management	Move, rename and copy objects. For more information, see Chapter 7, “Managing Objects,” on page 41.
Partition Management	Create, merge and move partitions and replicas. For more information, see Chapter 14, “Managing Partitions and Replicas,” on page 75.
Index Management	Create, modify and change state of Indexes. For more information, see Chapter 15, “Managing Indexes,” on page 79.
LDAP Configuration	Create, delete and modify LDAP objects. For more information, see Chapter 16, “Configuring LDAP Objects,” on page 83.
Certificate Management	Create and manage server and CA certificates. FOr more information, see Chapter 17, “Managing Certificates,” on page 87.
Authentication Management	Create and manage login.post-login methods and sequences. You can also manage Password policies and Challenge sets using this module. For more information, see Chapter 18, “Managing Authentication Framework,” on page 105.

Module Name	Description
SNMP	Create, delete and modify SNMP groups. For more information, see Chapter 19, “Managing SNMP Group Objects,” on page 121.
EBA	Manage enhanced background authentication. For more information, see Chapter 20, “Managing the Enhanced Background Authentication,” on page 125.
IDM Administration	Manage Identity Manager Drivers and Driver Sets. For more information, see Chapter 22, “Managing Drivers and Driver Sets,” on page 135. You can also manage the Driver Set properties using this module. For more information, see Chapter 23, “Managing Driver Set Properties,” on page 141.
Driver’s Properties	Manage the properties of various Drivers. For more information, see Chapter 24, “Managing Driver Properties,” on page 153.
Driver Set Statistics	Manage and view driver set statistics. For more information, see Chapter 25, “Managing Driver Set Statistics,” on page 181.
Object Inspector	Manage object association and data synchronization. For more information, see Chapter 26, “Inspecting Identity Manager Objects,” on page 183.
Data Flow	Manage and view data flow of drivers. For more information, see Chapter 27, “Managing Data Flow,” on page 185.
Entitlement Recipients	Manage the entitlement recipients. For more information, see Chapter 28, “Managing Entitlement Recipients,” on page 187.
Work Order Management	Manage the work orders. For more information, see Chapter 29, “Managing Work Orders,” on page 189.
Password Synchronization	Manage password synchronization and status. For more information, see Chapter 30, “Managing Password Status and Synchronization,” on page 193.
Library Management	Manage libraries. For more information, see Chapter 31, “Managing Libraries,” on page 197.
Email Server Configuration	Manage email server options. For more information, see Chapter 32, “Managing Email Server Options,” on page 199
Email Notification Templates	Manage email templates. For more information, see Chapter 33, “Managing Email Templates,” on page 203
Role Based Entitlement	Manage the Entitlements based on your role. For more information, see “Role-based Entitlement” on page 207

Module Name	Description
Role and Access Control	Role and Access Control helps the administrators to grant a user access to tasks based on the user's role in the organization. For more information, see: Chapter 35, “Managing Roles and Access,” on page 219
Custom Forms Management	The Custom Forms Management feature offers quick and easy way to streamline the tasks and dynamically create tasks for your most frequently used operations. For more information, see: Chapter 36, “Managing Custom Forms,” on page 233

Managing eDirectory Using Identity Console

This section describes various tasks that you can perform to manage your eDirectory server(s) using the Identity Console portal.

4

Performing Searches

The Search tile lets you specify a search operation to perform on the directory tree and display the results. This option let's you search for various objects, users, groups and several others. To perform a search operation for various objects in your data store, follow the below steps:

1. Specify the object name for the search. Use the asterisk wild-card to specify a partial name. For example: `ldap*`, `*cert`, `*server*` etc. If you use only asterisk in this field, Identity Console will return all the search results based on the selected **Type** and **Context**.

   NOTE: Using the Context Browser, you can browse through the entire eDirectory tree by specifying asterisk (*) in the search field. You can also filter the objects in Context Browser by using the wild-card search. For example, `admin*`. This behavior of the Context Browser is supported across various modules in Identity Console.

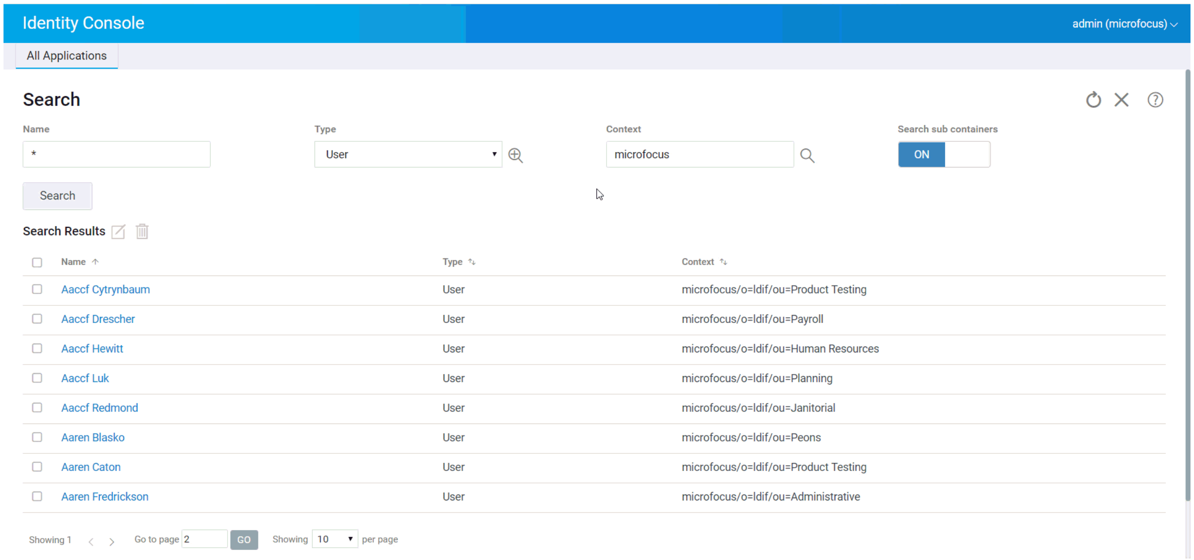
   ---

2. Select the object type for the search in the **Type** field. Identity Console displays objects of the specified type only. **User** type is selected by default in this field.

   Click 🔍 icon to define additional, attribute-level search settings. For more information, see "Configuring Advanced Search" on page 26.

3. Specify the starting container for the search operation in the **Context** field.
4. If you want the search to include subordinate containers, select **ON** for the Search sub containers option.
5. Click the Search button.

Figure 4-1 Performing a Search Operation



Name: *

Type: User

Context: microfocus

Search sub containers: ON

Go to page 2

Showing 10 per page

☐	Name	Type	Context
☐	Aaccf Cytrynbaum	User	microfocus/o=ldif/ou=Product Testing
☐	Aaccf Drescher	User	microfocus/o=ldif/ou=Payroll
☐	Aaccf Hewitt	User	microfocus/o=ldif/ou=Human Resources
☐	Aaccf Luk	User	microfocus/o=ldif/ou=Planning
☐	Aaccf Redmond	User	microfocus/o=ldif/ou=Janitorial
☐	Aaren Blasko	User	microfocus/o=ldif/ou=Peons
☐	Aaren Caton	User	microfocus/o=ldif/ou=Product Testing
☐	Aaren Fredrickson	User	microfocus/o=ldif/ou=Administrative

Configuring Advanced Search

Advanced Selection provides a more configurable environment for searching the directory for the desired objects.

Object Type: Specifies the object base class for which you are searching. For example, User.

Aux Classes: Click the + icon to specify an Auxiliary Class to include in the search.

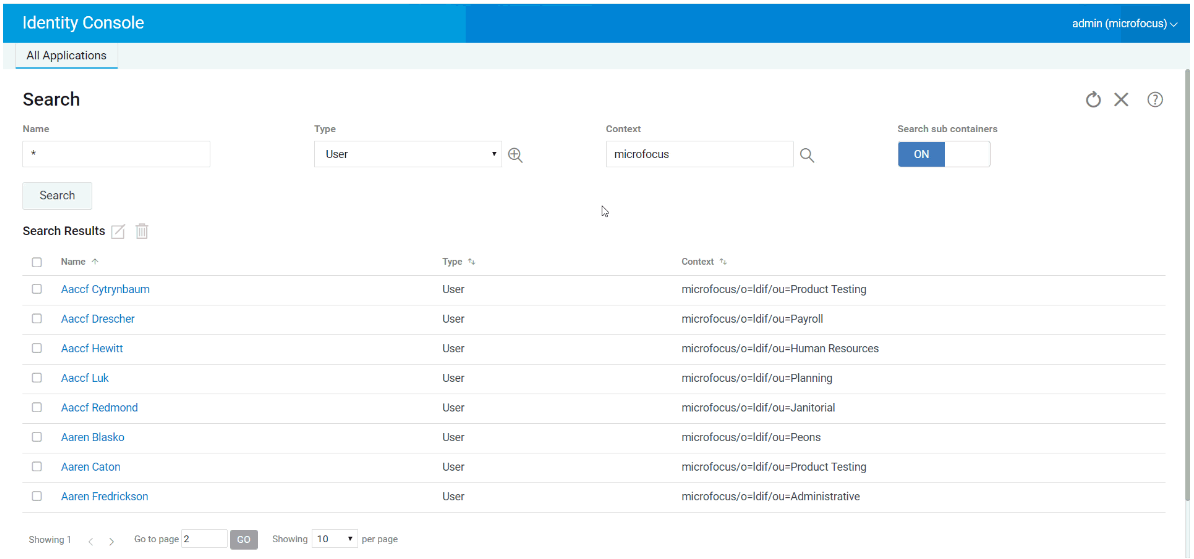
Attribute: Specifies an attribute (property) that you want to utilize as part of the filter.

Operator: Specifies the logical operator to apply to the filter. Options include.

Value: Specifies the attribute value you are using as a filter. You can use the asterisk (*) as a wildcard to indicate part of a value. For example, smi*, *th, and *mit*.

Additionally, you can chain multiple attribute filters together into a filter group by using the + Rule icon to add a second attribute to the list. When using multiple attribute filters, link them together with a logical AND or logical OR.

Figure 4-2 Configuring Advanced Search



Name: *

Type: User

Context: microfocus

Search sub containers: ON

☐	Name	Type	Context
☐	Aaccf Cytrynbaum	User	microfocus/o=ldif/ou=Product Testing
☐	Aaccf Drescher	User	microfocus/o=ldif/ou=Payroll
☐	Aaccf Hewitt	User	microfocus/o=ldif/ou=Human Resources
☐	Aaccf Luk	User	microfocus/o=ldif/ou=Planning
☐	Aaccf Redmond	User	microfocus/o=ldif/ou=Janitorial
☐	Aaren Blasko	User	microfocus/o=ldif/ou=Peons
☐	Aaren Caton	User	microfocus/o=ldif/ou=Product Testing
☐	Aaren Fredrickson	User	microfocus/o=ldif/ou=Administrative

Showing 1 Go to page 2 GO Showing 10 per page

5

Managing Users

Managing users and their network access is a central purpose of the datastore. Using the Identity Console web portal, you can perform the following user-related tasks:

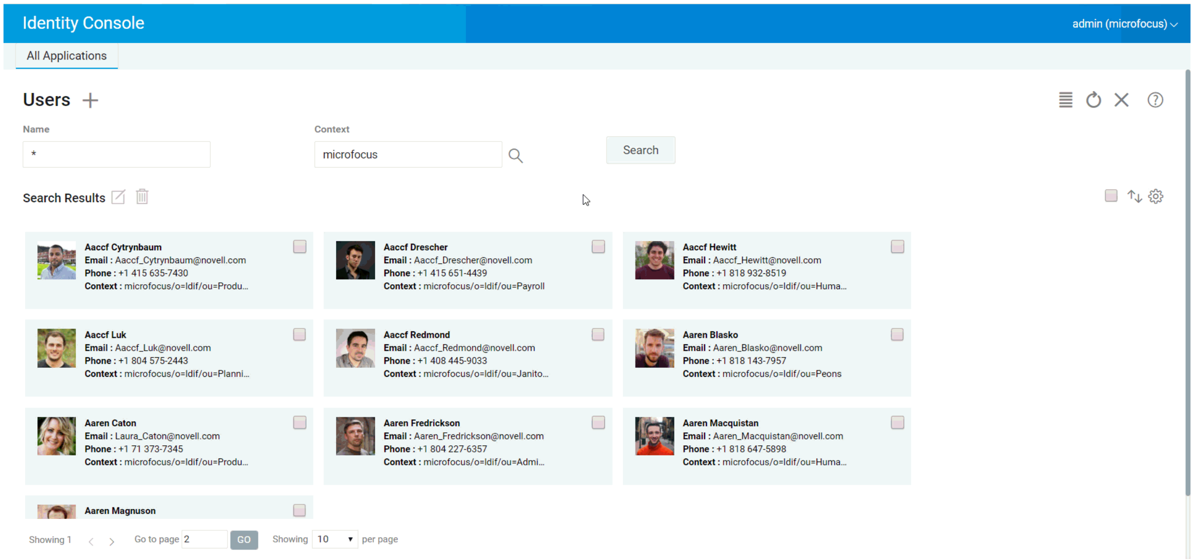
- "Creating a User" on page 27
- "Deleting a User" on page 28
- "Modifying Users" on page 29
- "Searching for a User" on page 29
- "Setting Password Restrictions" on page 30
- "Login Time Restrictions for Remote Users" on page 31
- "Disabling and Enabling a User Account" on page 32
- "Setting the Account Expiration Date" on page 32
- "Checking and Clearing the Intruder Lockout" on page 33

Creating a User

To create a new user object:

1. Click the **User Management** option from the Identity Console landing page.
2. Click the + icon.
3. In the Create User page, provide, at a minimum, the required user-related information, then click the Create button.
    - **Username**
    - **Context**
    - **Last name**
    - **Password**
4. A confirmation appears indicating the user object has been created.

Figure 5-1 *Creating Users*



Name: *

Context: microfocus

Aaccf Cytrynbaum
Email : Aaccf_Cytrynbaum@novell.com
Phone : +1 415 635-7430
Context : microfocus/o=Idif/ou=Produ...

Aaccf Drescher
Email : Aaccf_Drescher@novell.com
Phone : +1 415 651-4439
Context : microfocus/o=Idif/ou=Payroll

Aaccf Hewitt
Email : Aaccf_Hewitt@novell.com
Phone : +1 818 932-8519
Context : microfocus/o=Idif/ou=Huma...

Aaccf Luk
Email : Aaccf_Luk@novell.com
Phone : +1 804 575-2443
Context : microfocus/o=Idif/ou=Planni...

Aaccf Redmond
Email : Aaccf_Redmond@novell.com
Phone : +1 408 445-9033
Context : microfocus/o=Idif/ou=Janito...

Aaren Blasko
Email : Aaren_Blasko@novell.com
Phone : +1 818 143-7957
Context : microfocus/o=Idif/ou=Peons

Aaren Caton
Email : Laura_Caton@novell.com
Phone : +1 71 373-7345
Context : microfocus/o=Idif/ou=Produ...

Aaren Fredrickson
Email : Aaren_Fredrickson@novell.com
Phone : +1 804 227-6357
Context : microfocus/o=Idif/ou=Admi...

Aaren Macquistan
Email : Aaren_Macquistan@novell.com
Phone : +1 818 647-5898
Context : microfocus/o=Idif/ou=Huma...

Aaren Magnuson

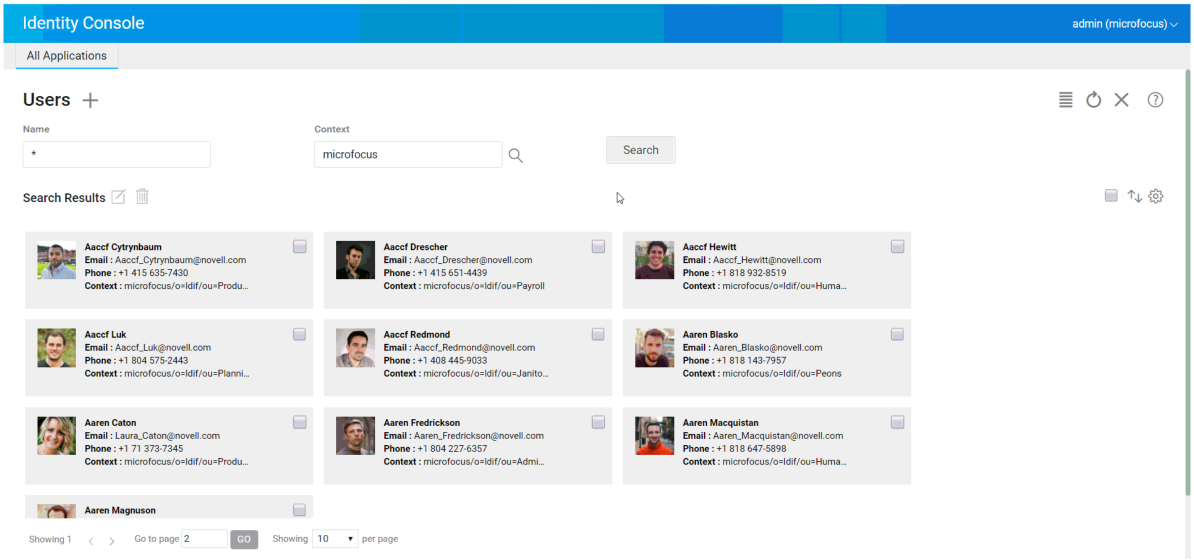
Showing 1 Go to page 2 Showing 10 per page

Deleting a User

To delete a user object:

1. Click the **User Management** option from the Identity Console landing page.
2. Type the name and context of the object or use the search feature to find it, then click the Search button.
3. Select the user object from the users list and click the 🗑 icon.
4. A confirmation appears indicating the user object has been deleted.

Figure 5-2 *Deleting a User*



Name: *

Context: microfocus

Aaccf Cytrynbaum
Email : Aaccf_Cytrynbaum@novell.com
Phone : +1 415 635-7430
Context : microfocus/o=Idif/ou=Produ...

Aaccf Drescher
Email : Aaccf_Drescher@novell.com
Phone : +1 415 651-4439
Context : microfocus/o=Idif/ou=Payroll

Aaccf Hewitt
Email : Aaccf_Hewitt@novell.com
Phone : +1 818 932-8519
Context : microfocus/o=Idif/ou=Huma...

Aaccf Luk
Email : Aaccf_Luk@novell.com
Phone : +1 804 575-2443
Context : microfocus/o=Idif/ou=Planni...

Aaccf Redmond
Email : Aaccf_Redmond@novell.com
Phone : +1 408 445-9033
Context : microfocus/o=Idif/ou=Janito...

Aaren Blasko
Email : Aaren_Blasko@novell.com
Phone : +1 818 143-7957
Context : microfocus/o=Idif/ou=Peons

Aaren Caton
Email : Laura_Caton@novell.com
Phone : +1 71 373-7345
Context : microfocus/o=Idif/ou=Produ...

Aaren Fredrickson
Email : Aaren_Fredrickson@novell.com
Phone : +1 804 227-6357
Context : microfocus/o=Idif/ou=Admi...

Aaren Macquistan
Email : Aaren_Macquistan@novell.com
Phone : +1 818 647-5898
Context : microfocus/o=Idif/ou=Huma...

Aaren Magnuson

Showing 1 Go to page 2 Showing 10 per page

Modifying Users

To modify a user object:

1 Click on the User Management option from the Identity Console landing page.

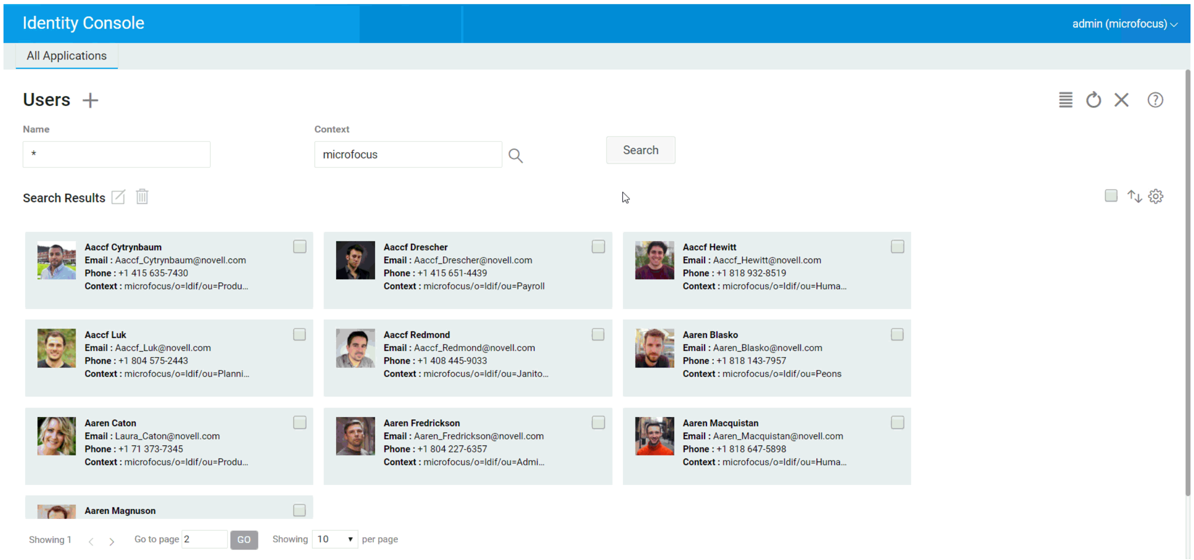
2 Type the name and context of the object or use the search feature to find it, then click on the Search button.

3 Select the user object from the users list and click on the ✎ icon.

4 Make your changes, then click on the Save button.

5 A confirmation appears indicating the user object has been modified.

***Figure 5-3** Modifying a User*



Name: *
Context: microfocus

Aaccf Cytrynbaum
Email : Aaccf_Cytrynbaum@novell.com
Phone : +1 415 635-7430
Context : microfocus/o=ldif/ou=Produ...

Aaccf Drescher
Email : Aaccf_Drescher@novell.com
Phone : +1 415 651-4439
Context : microfocus/o=ldif/ou=Payroll

Aaccf Hewitt
Email : Aaccf_Hewitt@novell.com
Phone : +1 818 932-8519
Context : microfocus/o=ldif/ou=Huma...

Aaccf Luk
Email : Aaccf_Luk@novell.com
Phone : +1 804 575-2443
Context : microfocus/o=ldif/ou=Planni...

Aaccf Redmond
Email : Aaccf_Redmond@novell.com
Phone : +1 408 445-9033
Context : microfocus/o=ldif/ou=Janito...

Aaren Blasko
Email : Aaren_Blasko@novell.com
Phone : +1 818 143-7957
Context : microfocus/o=ldif/ou=Peons

Aaren Caton
Email : Laura_Caton@novell.com
Phone : +1 71 373-7345
Context : microfocus/o=ldif/ou=Produ...

Aaren Fredrickson
Email : Aaren_Fredrickson@novell.com
Phone : +1 804 227-6357
Context : microfocus/o=ldif/ou=Admi...

Aaren Macquistan
Email : Aaren_Macquistan@novell.com
Phone : +1 818 647-5898
Context : microfocus/o=ldif/ou=Huma...

Aaren Magnuson

Go to page 2 · Showing 10 per page

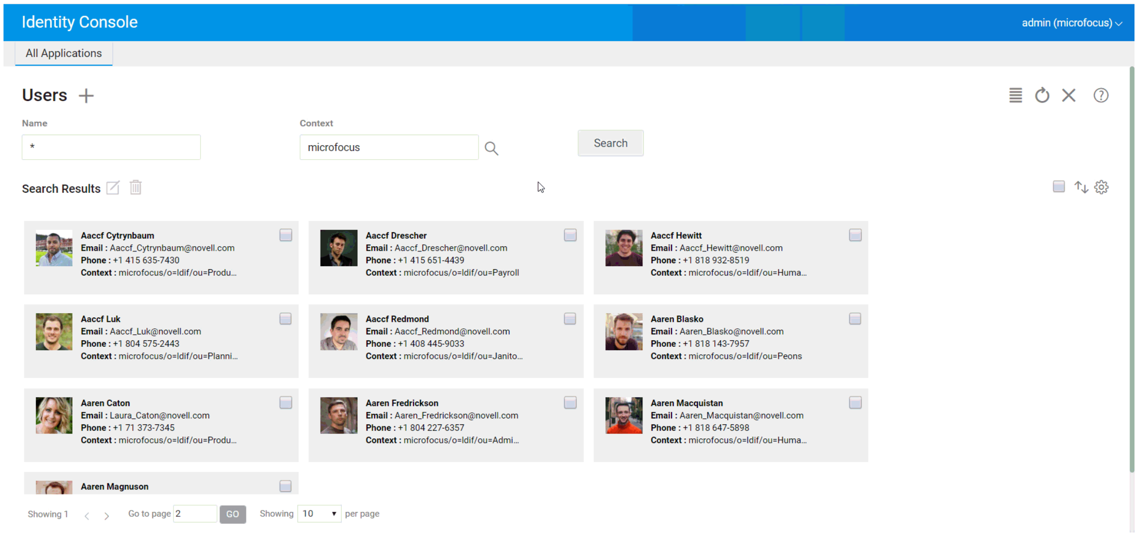
Searching for a User

To search a user object:

1 Click on the User Management option from the Identity Console landing page.

2 You can either search a user by the name of by both name and context. After specifying the necessary details, click on the Search icon.

Figure 5-4 *Searching a User*



Name: *

Context: microfocus

Aaccf Cytrynbaum
Email : Aaccf_Cytrynbaum@novell.com
Phone : +1 415 635-7430
Context : microfocus/o=ldif/ou=Produ...

Aaccf Drescher
Email : Aaccf_Drescher@novell.com
Phone : +1 415 651-4439
Context : microfocus/o=ldif/ou=Payroll

Aaccf Hewitt
Email : Aaccf_Hewitt@novell.com
Phone : +1 818 932-8519
Context : microfocus/o=ldif/ou=Huma...

Aaccf Luk
Email : Aaccf_Luk@novell.com
Phone : +1 804 575-2443
Context : microfocus/o=ldif/ou=Planni...

Aaccf Redmond
Email : Aaccf_Redmond@novell.com
Phone : +1 408 445-9033
Context : microfocus/o=ldif/ou=Janito...

Aaren Blasko
Email : Aaren_Blasko@novell.com
Phone : +1 818 143-7957
Context : microfocus/o=ldif/ou=Peons

Aaren Caton
Email : Laura_Caton@novell.com
Phone : +1 71 373-7345
Context : microfocus/o=ldif/ou=Produ...

Aaren Fredrickson
Email : Aaren_Fredrickson@novell.com
Phone : +1 804 227-6357
Context : microfocus/o=ldif/ou=Admi...

Aaren Macquistan
Email : Aaren_Macquistan@novell.com
Phone : +1 818 647-5898
Context : microfocus/o=ldif/ou=Huma...

Aaren Magnuson

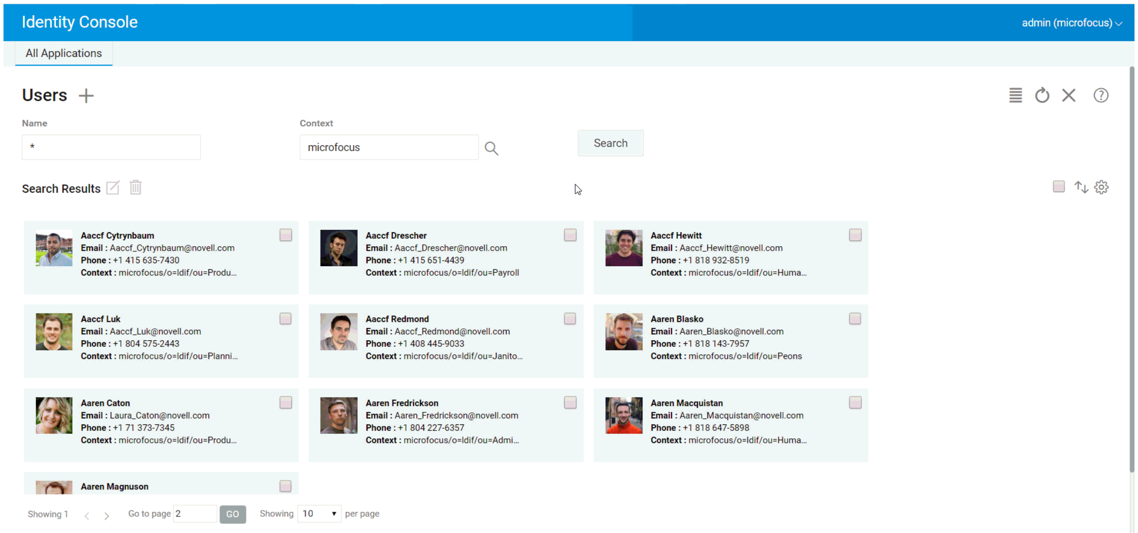
Go to page 2 · Showing 10 per page

Setting Password Restrictions

Password restrictions allows you to perform the following actions:

- Allows users to change their respective passwords
- Enforce a password for login
- Specify the password strength
- Enforce periodic password change
- Specify the password expiration date
- Enforce unique password creation
- Specify the grace login period in case the password has expired.

Figure 5-5 *Password Restrictions*



Name: *

Context: microfocus

Aaccf Cytrynbaum
Email : Aaccf_Cytrynbaum@novell.com
Phone : +1 415 635-7430
Context : microfocus/o=ldif/ou=Produ...

Aaccf Drescher
Email : Aaccf_Drescher@novell.com
Phone : +1 415 651-4439
Context : microfocus/o=ldif/ou=Payroll

Aaccf Hewitt
Email : Aaccf_Hewitt@novell.com
Phone : +1 818 932-8519
Context : microfocus/o=ldif/ou=Huma...

Aaccf Luk
Email : Aaccf_Luk@novell.com
Phone : +1 804 575-2443
Context : microfocus/o=ldif/ou=Planni...

Aaccf Redmond
Email : Aaccf_Redmond@novell.com
Phone : +1 408 445-9033
Context : microfocus/o=ldif/ou=Janito...

Aaren Blasko
Email : Aaren_Blasko@novell.com
Phone : +1 818 143-7957
Context : microfocus/o=ldif/ou=Peons

Aaren Caton
Email : Laura_Caton@novell.com
Phone : +1 71 373-7345
Context : microfocus/o=ldif/ou=Produ...

Aaren Fredrickson
Email : Aaren_Fredrickson@novell.com
Phone : +1 804 227-6357
Context : microfocus/o=ldif/ou=Admi...

Aaren Macquistan
Email : Aaren_Macquistan@novell.com
Phone : +1 818 647-5898
Context : microfocus/o=ldif/ou=Huma...

Aaren Magnuson

Go to page 2 · Showing 10 per page

Login Time Restrictions for Remote Users

This module provides an option to restrict the individual user's application login time. By default Identity Console does not impose any login restrictions. You can, however, set the restrictions by accessing the Time Restrictions property page.

If a user logs in remotely from a different time zone than the server processing the login request, any login time restrictions that have been set for the user are adjusted for the time difference. For example, if you restrict a user from logging in Mondays from 1:00 a.m. to 6:00 a.m. and the user logs in remotely from a time zone that is one hour later than the server, the restriction effectively becomes 2:00 a.m. to 7:00 a.m. for that user. The session timeout default value is 15 minutes, and the user can change the value.

To set login time restrictions for remote users, perform the following steps:

1. On the Identity Console home page, click **Roles and Tasks**.
2. Click **Users** > **Modify User.**
3. Specify the name and context of the User or Users you want to modify, then click OK.
4. On the **Restrictions** tab, click **Time Restrictions**.
5. Select from the following options:

Table 5-1

Option	**Description**
Time Grid	Each cell in the time grid represents a half hour on a particular day of the week. Red cells represent restricted times (when this object cannot be logged in). Gray cells represent unrestricted times (when the object can be logged in). To create a time restriction, click the desired times to make them dark gray. You can also select multiple times by holding down the Shift key, clicking a cell, then dragging across the corresponding cells. The login time restrictions you set are stored in the Login Allowed Time Map property of this object.
Add Time Restrictions	To add a time restriction, select a gray cell, then select this option.
Remove Time Restrictions	To remove a time restriction, select a red cell, then select this option.
Update	Click this button to enable the selection.
Reset	Click this button to reset the time grid to the way it was before you opened this property page.

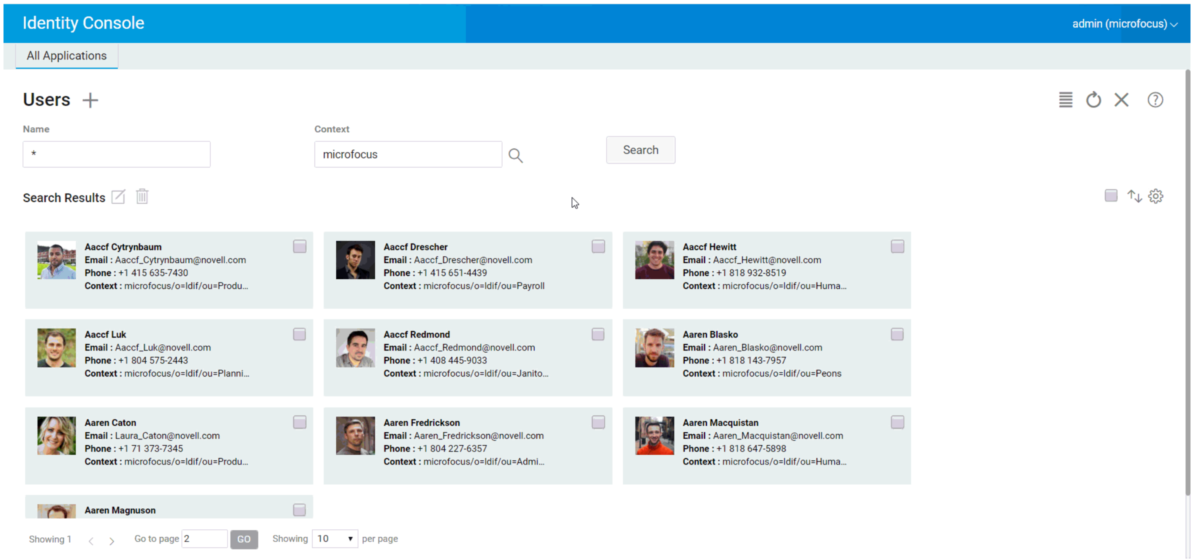
6. Click **Apply** > **Save**.

Disabling and Enabling a User Account

To disable a user account, perform the following steps:

1. Select the user whose account needs to be disabled and click the ✎ icon.
2. Click the **Restrictions** tab in the **Modify User** page.
3. Expand the **Login Restrictions** tab and select the **Account Disabled** check box.
4. Click the Save icon.
5. Now the user account is disabled. To enable any disabled user account, deselect the **Account Disabled** check box.

Figure 5-6 *Disabling and Enabling a User Account*



Name: *
Context: microfocus

Aaccf Cytrynbaum
Email : Aaccf_Cytrynbaum@novell.com
Phone : +1 415 635-7430
Context : microfocus/o=ldif/ou=Produ...

Aaccf Drescher
Email : Aaccf_Drescher@novell.com
Phone : +1 415 651-4439
Context : microfocus/o=ldif/ou=Payroll

Aaccf Hewitt
Email : Aaccf_Hewitt@novell.com
Phone : +1 818 932-8519
Context : microfocus/o=ldif/ou=Huma...

Aaccf Luk
Email : Aaccf_Luk@novell.com
Phone : +1 804 575-2443
Context : microfocus/o=ldif/ou=Planni...

Aaccf Redmond
Email : Aaccf_Redmond@novell.com
Phone : +1 408 445-9033
Context : microfocus/o=ldif/ou=Janito...

Aaren Blasko
Email : Aaren_Blasko@novell.com
Phone : +1 818 143-7957
Context : microfocus/o=ldif/ou=Peons

Aaren Caton
Email : Laura_Caton@novell.com
Phone : +1 71 373-7345
Context : microfocus/o=ldif/ou=Produ...

Aaren Fredrickson
Email : Aaren_Fredrickson@novell.com
Phone : +1 804 227-6357
Context : microfocus/o=ldif/ou=Admi...

Aaren Macquistan
Email : Aaren_Macquistan@novell.com
Phone : +1 818 647-5898
Context : microfocus/o=ldif/ou=Huma...

Aaren Magnuson

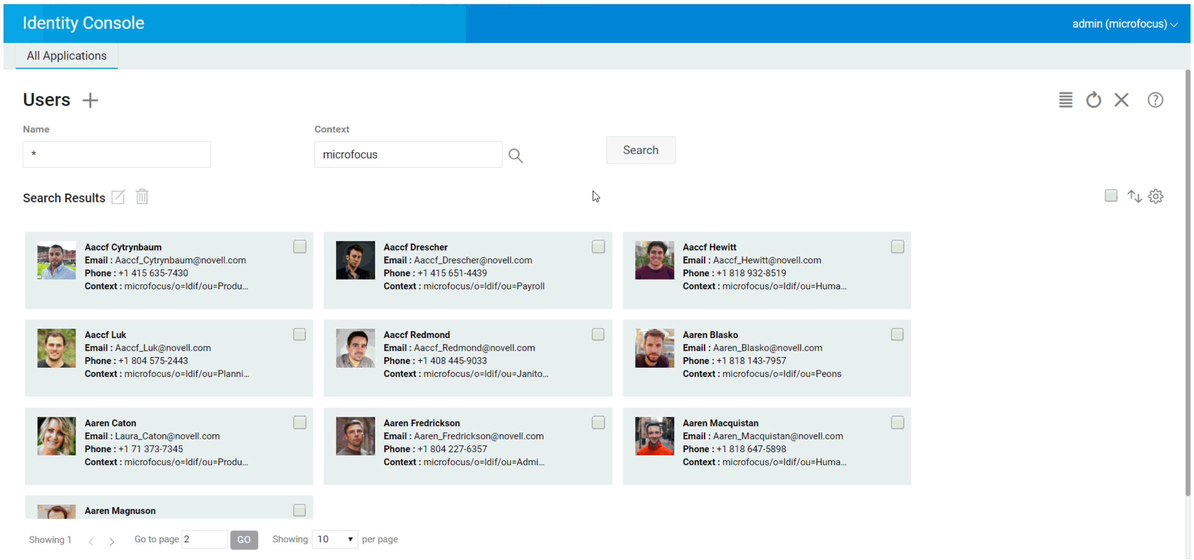
Showing 1 ‹ › Go to page 2 GO Showing 10 ▾ per page

Setting the Account Expiration Date

To set account expiration date for users, perform the following steps:

1. Select the user for whom account expiration date needs to be set and click the ✎ icon.
2. Click the **Restrictions** tab in the **Modify User** page.
3. Expand the **Login Restrictions** tab and select the **Account has expiration date** check box and specify the **Expiration date**.
4. Click the Save icon.

Figure 5-7 *Setting the Account Expiration Date*



Name: *

Context: microfocus

Aaccf Cytrynbaum
Email : Aaccf_Cytrynbaum@novell.com
Phone : +1 415 635-7430
Context : microfocus/o=ldif/ou=Produ...

Aaccf Drescher
Email : Aaccf_Drescher@novell.com
Phone : +1 415 651-4439
Context : microfocus/o=ldif/ou=Payroll

Aaccf Hewitt
Email : Aaccf_Hewitt@novell.com
Phone : +1 818 932-8519
Context : microfocus/o=ldif/ou=Huma...

Aaccf Luk
Email : Aaccf_Luk@novell.com
Phone : +1 804 575-2443
Context : microfocus/o=ldif/ou=Planni...

Aaccf Redmond
Email : Aaccf_Redmond@novell.com
Phone : +1 408 445-9033
Context : microfocus/o=ldif/ou=Janito...

Aaren Blasko
Email : Aaren_Blasko@novell.com
Phone : +1 818 143-7957
Context : microfocus/o=ldif/ou=Peons

Aaren Caton
Email : Laura_Caton@novell.com
Phone : +1 71 373-7345
Context : microfocus/o=ldif/ou=Produ...

Aaren Fredrickson
Email : Aaren_Fredrickson@novell.com
Phone : +1 804 227-6357
Context : microfocus/o=ldif/ou=Admi...

Aaren Macquistan
Email : Aaren_Macquistan@novell.com
Phone : +1 818 647-5898
Context : microfocus/o=ldif/ou=Huma...

Aaren Magnuson

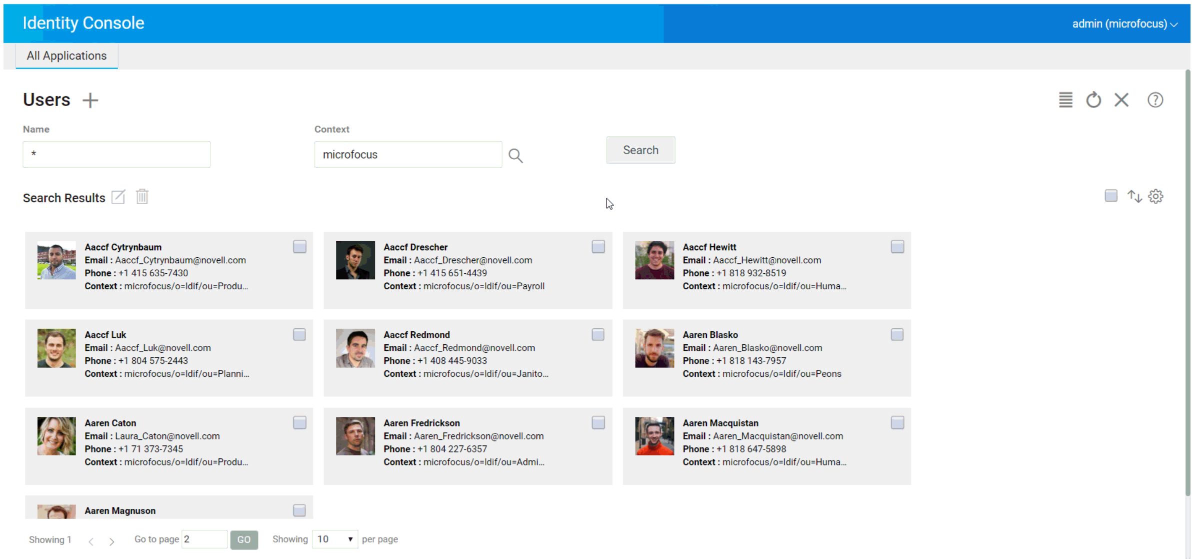
Showing 1 Go to page 2 Showing 10 per page

Checking and Clearing the Intruder Lockout

You can view the details of the intruder lockout for any user account using the Identity Console web portal. To view the Intruder Lockout details:

1. Select the user for whom intruder lockout details needs to be checked and click the ✎ icon.
2. Click the **Restrictions** tab in the **Modify User** page.
3. Expand the **Intruder Lockout** tab and view the details of the intruder lockout.
4. Now select the **Clear lockout** tab and click the Clear button.
5. Click the Save button.

***Figure 5-8** Checking and Clearing the Intruder Lockout*



Name: *

Context: microfocus

Go to page 2

Showing 10 per page

Aaccf Cytrynbaum
Email : Aaccf_Cytrynbaum@novell.com
Phone : +1 415 635-7430
Context : microfocus/o=ldif/ou=Produ...

Aaccf Drescher
Email : Aaccf_Drescher@novell.com
Phone : +1 415 651-4439
Context : microfocus/o=ldif/ou=Payroll

Aaccf Hewitt
Email : Aaccf_Hewitt@novell.com
Phone : +1 818 932-8519
Context : microfocus/o=ldif/ou=Huma...

Aaccf Luk
Email : Aaccf_Luk@novell.com
Phone : +1 804 575-2443
Context : microfocus/o=ldif/ou=Planni...

Aaccf Redmond
Email : Aaccf_Redmond@novell.com
Phone : +1 408 445-9033
Context : microfocus/o=ldif/ou=Janito...

Aaren Blasko
Email : Aaren_Blasko@novell.com
Phone : +1 818 143-7957
Context : microfocus/o=ldif/ou=Peons

Aaren Caton
Email : Laura_Caton@novell.com
Phone : +1 71 373-7345
Context : microfocus/o=ldif/ou=Produ...

Aaren Fredrickson
Email : Aaren_Fredrickson@novell.com
Phone : +1 804 227-6357
Context : microfocus/o=ldif/ou=Admi...

Aaren Macquistan
Email : Aaren_Macquistan@novell.com
Phone : +1 818 647-5898
Context : microfocus/o=ldif/ou=Huma...

Aaren Magnuson

6

Managing Groups

Groups usually contain a number of members. Any user who creates a group automatically becomes the owner of the group. The following operations can be performed using the Groups Management feature:

- "Creating a Group" on page 35
- "Deleting Groups" on page 36
- "Modifying Groups" on page 37
- "Adding or Modifying Group Members" on page 37
- "Searching for Groups" on page 38

For more information about using and configuring Group objects, see the *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

Creating a Group

To create a group:

1. Click the **Groups Management** option from the Identity Console landing page.
2. Click the + icon.
3. In the Create Group page, enter the following details:
   - Specify the group name
   - Specify the Context

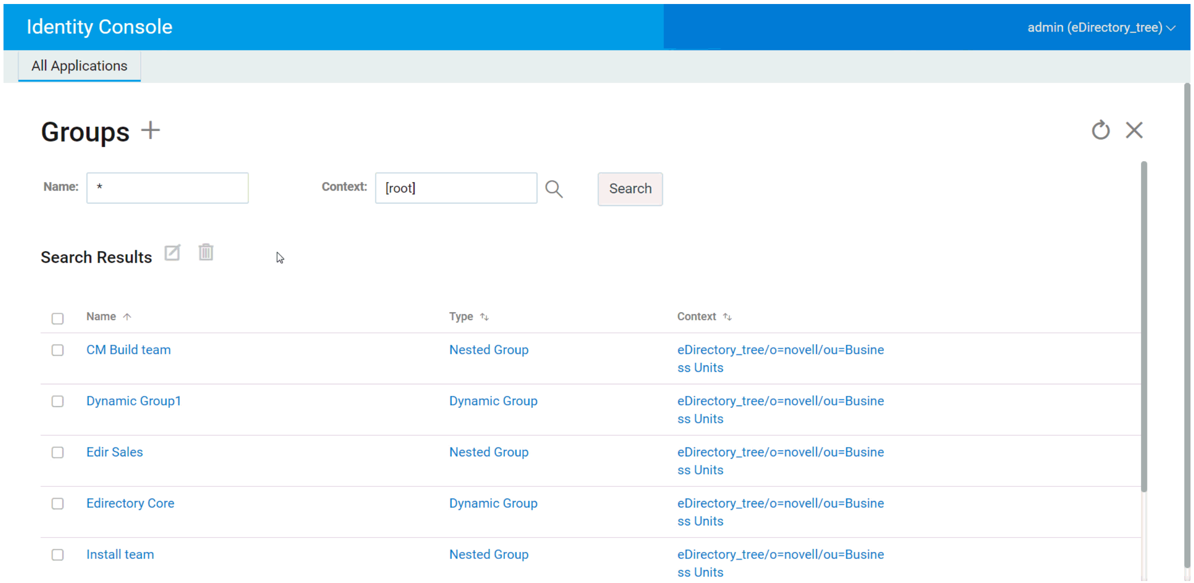
   Select **Dynamic Group** to make the new group a dynamic group, of the class `dynamicGroup`. Otherwise, the group is created as a static group.

   Select **Nested Group** to make the new group a nested group so that the group is created with auxiliary class `nestedGroupAux`.

   NOTE: You can convert a static group to a dynamic group or nested group by using the procedure mentioned in Modifying Objects. This extends the selected Group object to belong to the `dynamicGroupAux` class or `nestedGroupAux` class respectively.

   A group can be either nested or dynamic. You cannot create a group that is both nested and dynamic.
4. After specifying the necessary details, click the Create button.
5. A confirmation appears indicating the group has been created.

***Figure 6-1** Creating a Group*



Name: *

Context: [root]

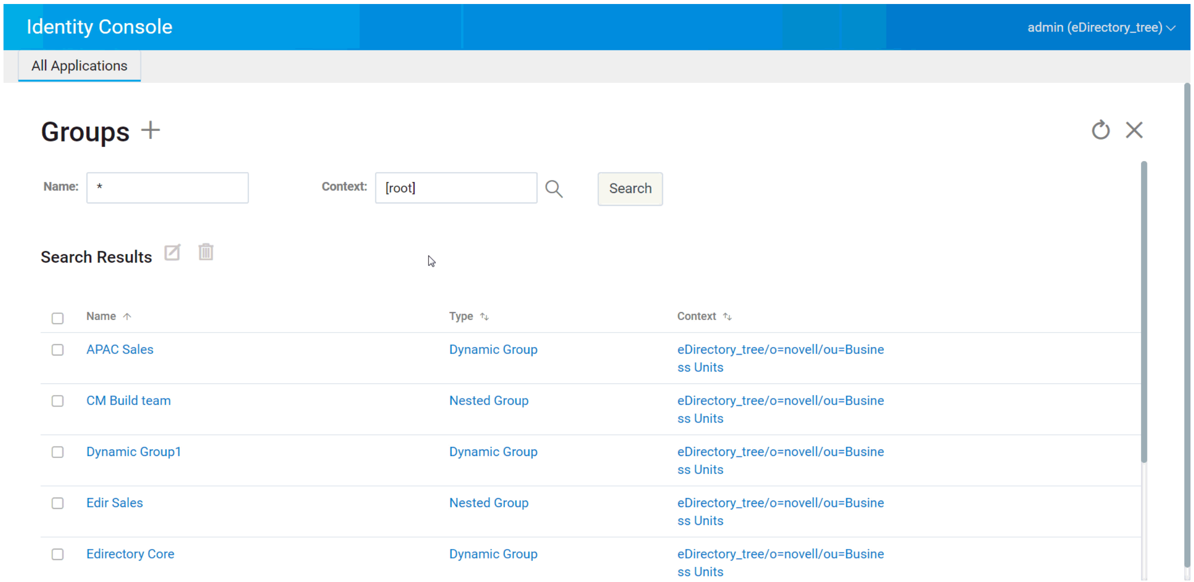
☐	Name	Type	Context
☐	CM Build team	Nested Group	eDirectory_tree/o=novell/ou=Business Units
☐	Dynamic Group1	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units
☐	Edir Sales	Nested Group	eDirectory_tree/o=novell/ou=Business Units
☐	Edirectory Core	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units
☐	Install team	Nested Group	eDirectory_tree/o=novell/ou=Business Units

Deleting Groups

To delete groups:

1. Click the **Groups Management** option from the Identity Console landing page.
2. Specify the name, and context of the group or use the search feature to find it, then click the Search button.
3. Select the group that needs to be deleted and click the 🗑 icon.
4. A confirmation appears indicating the group has been deleted.

***Figure 6-2** Deleting Groups*



Name: *

Context: [root]

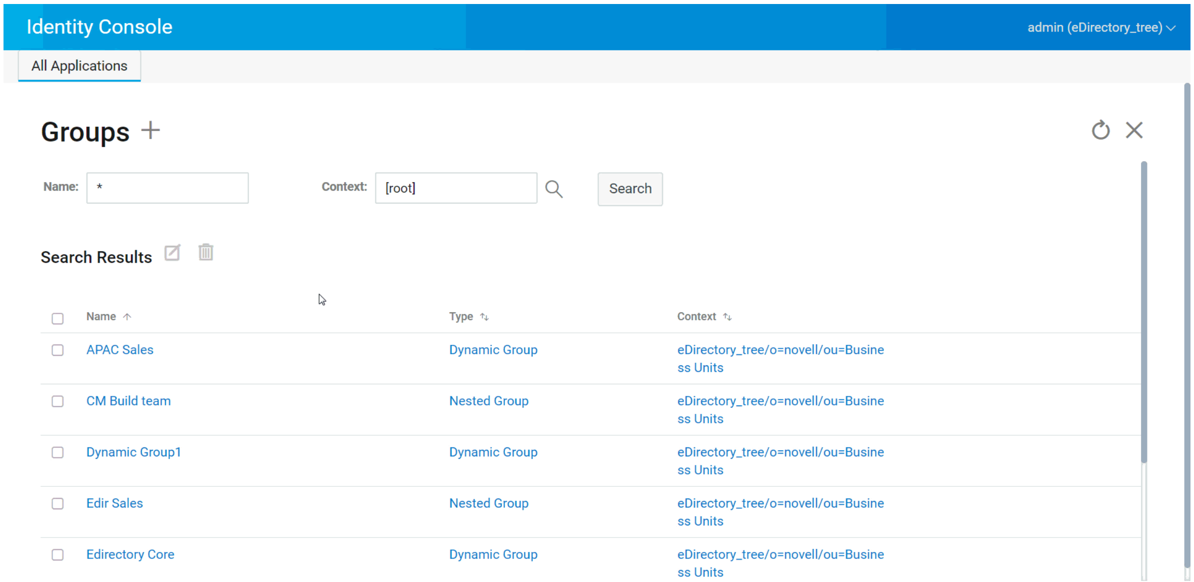
☐	Name	Type	Context
☐	APAC Sales	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units
☐	CM Build team	Nested Group	eDirectory_tree/o=novell/ou=Business Units
☐	Dynamic Group1	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units
☐	Edir Sales	Nested Group	eDirectory_tree/o=novell/ou=Business Units
☐	Edirectory Core	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units

Modifying Groups

To modify groups:

1. Click on the **Groups Management** option from the Identity Console landing page.
2. Type the name, and context of the group, then click on the Search button.
3. Select the group that needs to be modified and click on the ✎ icon.
4. Make your changes, then click on the Save button.
5. A confirmation appears indicating the group has been modified.

Figure 6-3 *Modifying Groups*



Name: *

Context: [root]

☐	Name	Type	Context
☐	APAC Sales	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units
☐	CM Build team	Nested Group	eDirectory_tree/o=novell/ou=Business Units
☐	Dynamic Group1	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units
☐	Edir Sales	Nested Group	eDirectory_tree/o=novell/ou=Business Units
☐	Edirectory Core	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units

Adding or Modifying Group Members

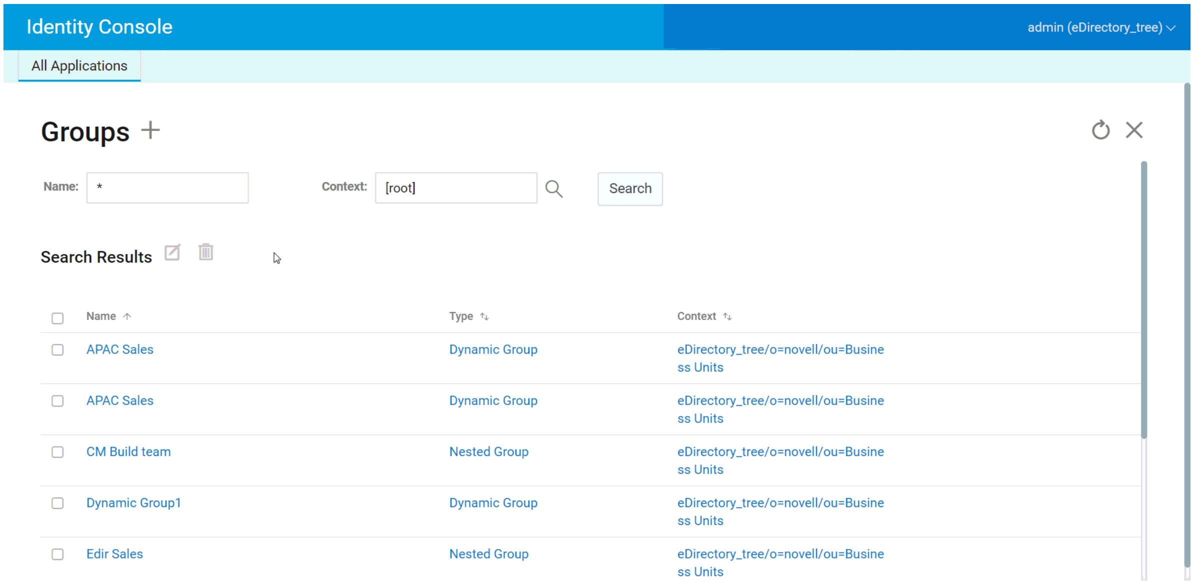
To add r modify group members:

1. Click the **Groups Management** option from the Identity Console landing page.
2. Type the name, and context of the group, then click the Search button.
3. Select the group and click the ✎ icon.
4. Click the **Members** tab in the **Modify Group** page.
5. Use the + icon to add a new member to the group. In case you decide to remove members from the group, click the 🗑 icon.

6 After making the changes, click the **Save** button.

7 A confirmation appears indicating the group has been modified.

Figure 6-4 Adding or Modifying Group Members



Identity Console

admin (eDirectory_tree)

All Applications

Groups +

Name: *

Context: [root]

Search

Search Results

☐	Name	Type	Context
☐	APAC Sales	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units
☐	APAC Sales	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units
☐	CM Build team	Nested Group	eDirectory_tree/o=novell/ou=Business Units
☐	Dynamic Group1	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units
☐	Edir Sales	Nested Group	eDirectory_tree/o=novell/ou=Business Units

Searching for Groups

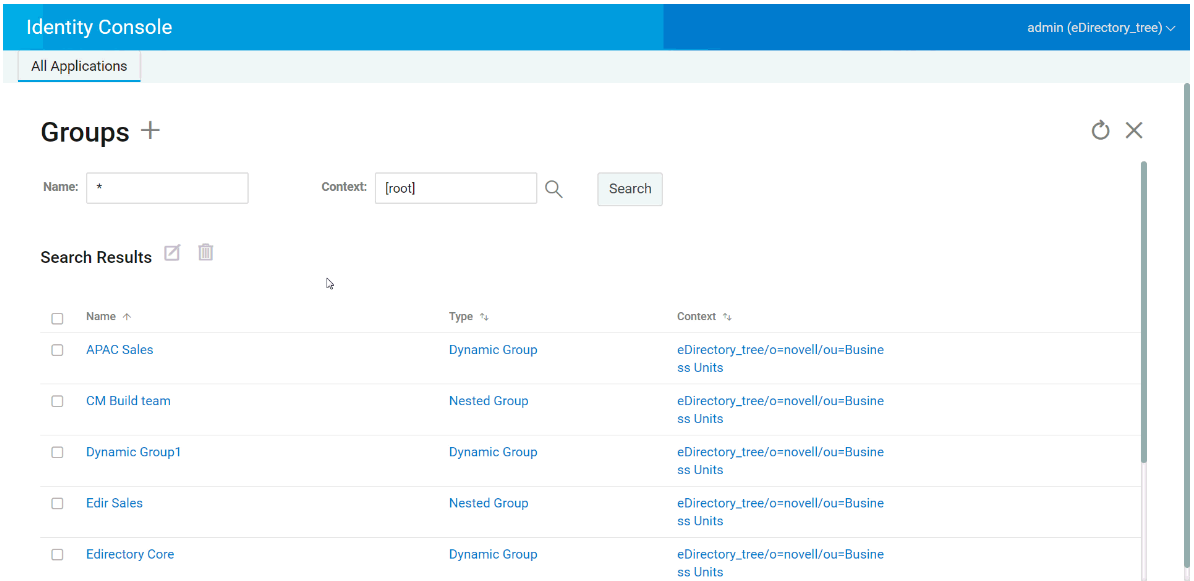
To search for groups:

1 Click the **Groups Management** option from the Identity Console landing page.

2 You can either search for a group by the name of by both name, and context.

3 After specifying the necessary details, click the **Search** icon.

***Figure 6-5** Searching for Groups*



Name: *

Context: [root]

☐	Name	Type	Context
☐	APAC Sales	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units
☐	CM Build team	Nested Group	eDirectory_tree/o=novell/ou=Business Units
☐	Dynamic Group1	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units
☐	Edir Sales	Nested Group	eDirectory_tree/o=novell/ou=Business Units
☐	Edirectory Core	Dynamic Group	eDirectory_tree/o=novell/ou=Business Units

7

Managing Objects

Identity Console allows you to manage various objects in your data store. Using this module, you can create, modify, delete and search for objects.

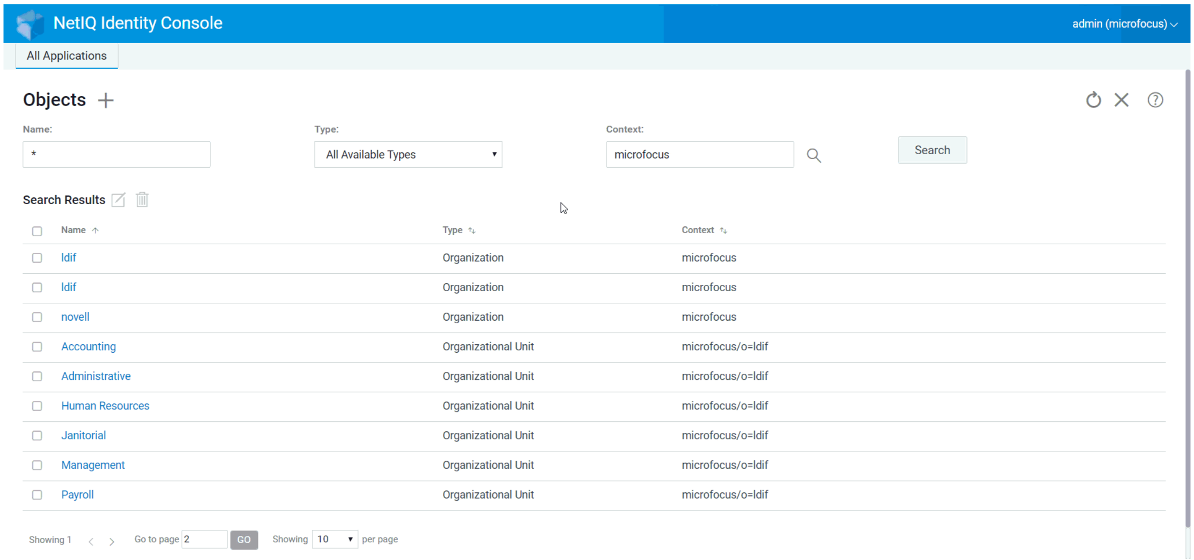
- “Creating an Object” on page 41
- “Deleting Objects” on page 42
- “Modifying Objects” on page 43
- “Searching for an Object” on page 43
- “Moving an Object” on page 44
- “Renaming an Object” on page 45

Creating an Object

To create a new object:

1. Click the **Object Management** option from the Identity Console landing page.
2. Click the + icon.
3. In the Create Object page, enter the following details:
    - Specify an object name
    - Specify the Type
    - Specify the Context
4. After entering all the required details, click **Next** > **Create**.
5. A confirmation appears indicating the object has been created.

Figure 7-1 *Creating an Object*



Name: *

Type: All Available Types

Context: microfocus

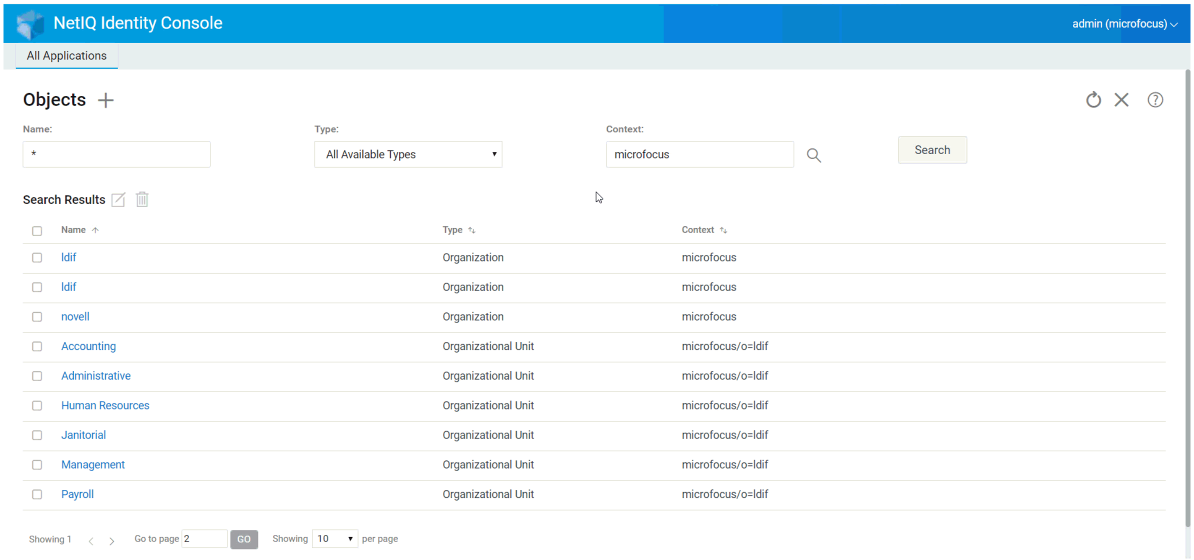
☐	Name	Type	Context
☐	ldif	Organization	microfocus
☐	ldif	Organization	microfocus
☐	novell	Organization	microfocus
☐	Accounting	Organizational Unit	microfocus/o=ldif
☐	Administrative	Organizational Unit	microfocus/o=ldif
☐	Human Resources	Organizational Unit	microfocus/o=ldif
☐	Janitorial	Organizational Unit	microfocus/o=ldif
☐	Management	Organizational Unit	microfocus/o=ldif
☐	Payroll	Organizational Unit	microfocus/o=ldif

Deleting Objects

To delete objects:

1. Click the **Object Management** option from the Identity Console landing page.
2. Specify the name, type and context of the object or use the search feature to find it, then click the Search button.
3. Select the object from the search list and click the 🗑 icon.
4. A confirmation appears indicating the object has been deleted.

Figure 7-2 *Deleting Objects*



Name: *

Type: All Available Types

Context: microfocus

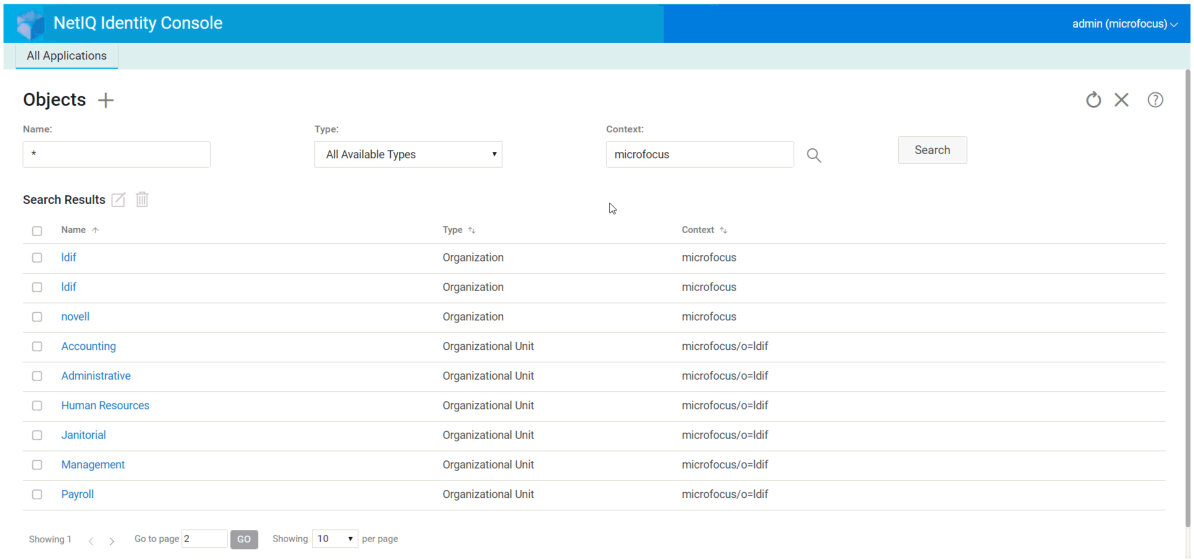
☐	Name	Type	Context
☐	ldif	Organization	microfocus
☐	ldif	Organization	microfocus
☐	novell	Organization	microfocus
☐	Accounting	Organizational Unit	microfocus/o=ldif
☐	Administrative	Organizational Unit	microfocus/o=ldif
☐	Human Resources	Organizational Unit	microfocus/o=ldif
☐	Janitorial	Organizational Unit	microfocus/o=ldif
☐	Management	Organizational Unit	microfocus/o=ldif
☐	Payroll	Organizational Unit	microfocus/o=ldif

Modifying Objects

To modify objects:

1. Click the **Objects Management** option from the Identity Console landing page.
2. Type the name, type and context of the object, then click the Search button.
3. Select the object from the search list and click the ✎ icon.
4. Make your changes, then click the Save button.
5. A confirmation appears indicating the object has been modified.

Figure 7-3 *Modifying Objects*



Name: *

Type: All Available Types

Context: microfocus

☐	Name	Type	Context
☐	ldif	Organization	microfocus
☐	ldif	Organization	microfocus
☐	novell	Organization	microfocus
☐	Accounting	Organizational Unit	microfocus/o=ldif
☐	Administrative	Organizational Unit	microfocus/o=ldif
☐	Human Resources	Organizational Unit	microfocus/o=ldif
☐	Janitorial	Organizational Unit	microfocus/o=ldif
☐	Management	Organizational Unit	microfocus/o=ldif
☐	Payroll	Organizational Unit	microfocus/o=ldif

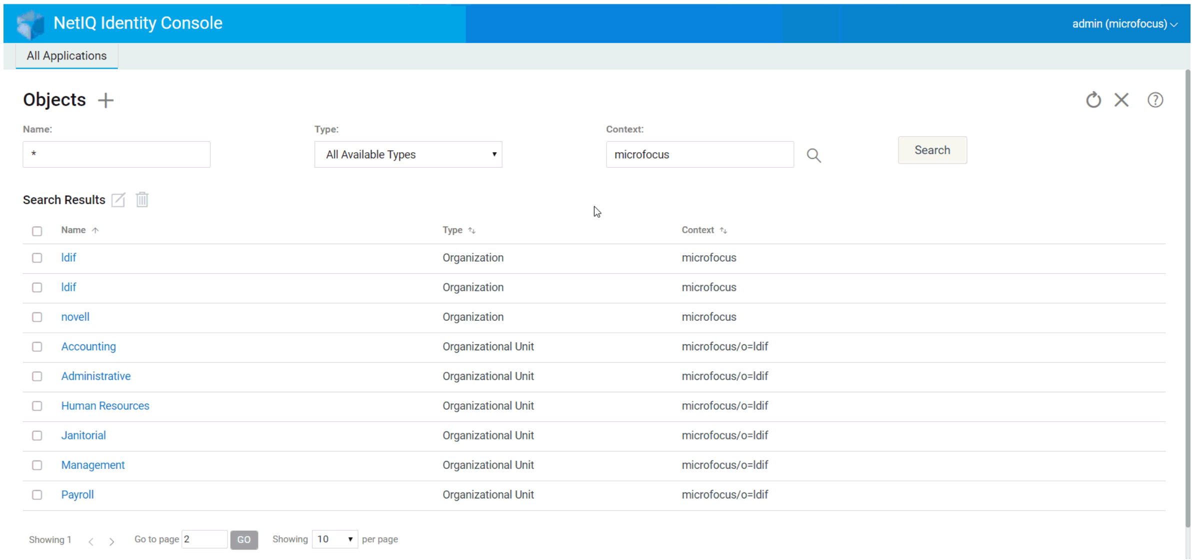
Showing 1 < > Go to page 2 GO Showing 10 per page

Searching for an Object

To search for an object:

1. Click the **Object Management** option from the Identity Console landing page.
2. You can either search for an object by the name or by both name, type and context.
3. After specifying the necessary details, click the Search button.

Figure 7-4 Searching for an Object



NetIQ Identity Console

admin (microfocus)

All Applications

Objects +

Name: *

Type: All Available Types

Context: microfocus

Search

Search Results

☐	Name	Type	Context
☐	ldif	Organization	microfocus
☐	ldif	Organization	microfocus
☐	novell	Organization	microfocus
☐	Accounting	Organizational Unit	microfocus/o=ldif
☐	Administrative	Organizational Unit	microfocus/o=ldif
☐	Human Resources	Organizational Unit	microfocus/o=ldif
☐	Janitorial	Organizational Unit	microfocus/o=ldif
☐	Management	Organizational Unit	microfocus/o=ldif
☐	Payroll	Organizational Unit	microfocus/o=ldif

Showing 1 < > Go to page 2 GO Showing 10 per page

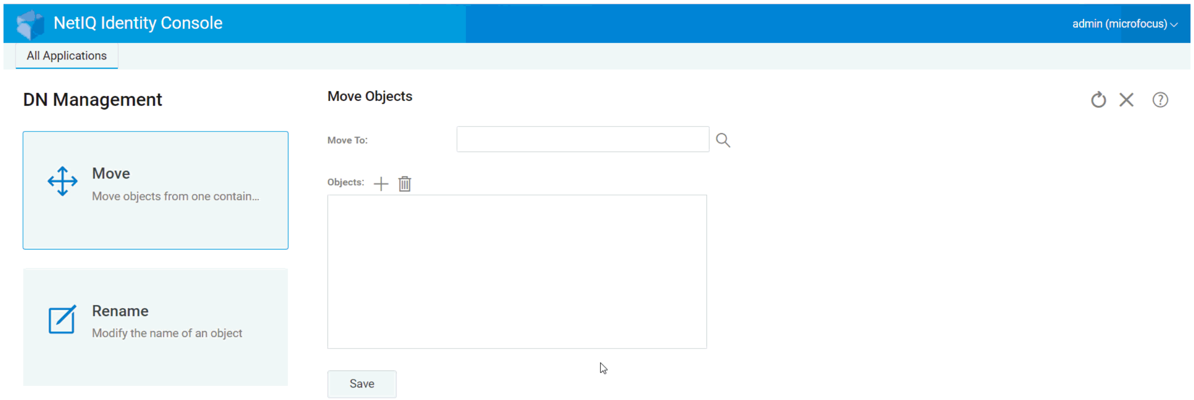
Moving an Object

To move an object:

1. Click the **DN Management** option from the Identity Console landing page.
2. The **Move Object** option will be selected by default.
3. In the **Move To** field, select the container to which you want to move the object.
4. Click the + icon to add the object that you want to move to a different container.

   If you want to remove a selected object, click the 🗑 icon.
5. Click the Save button.
6. A confirmation message appears indicating the move object operation was successful.

Figure 7-5 Moving an Object

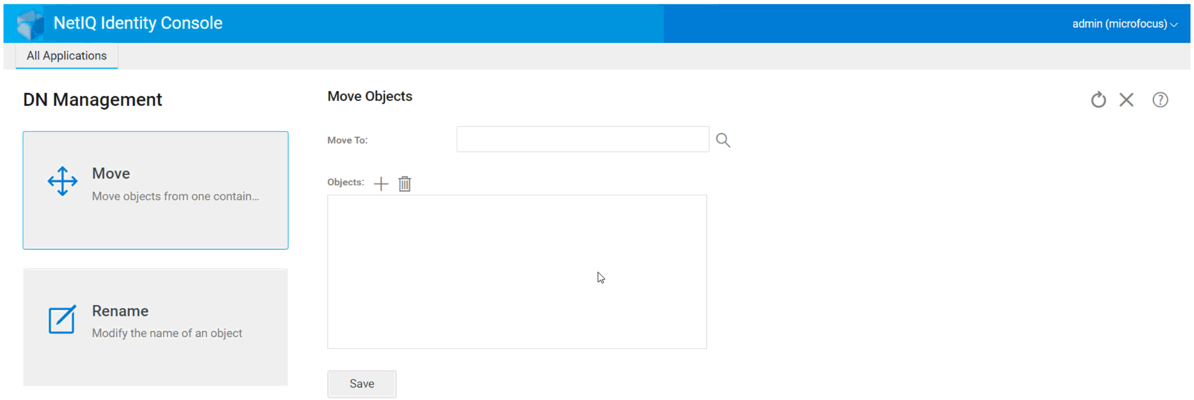


Renaming an Object

To rename an object:

1. Click the **DN Management** option from the Identity Console landing page.
2. Select the **Rename Object** option.
3. Use the search feature to find the object which needs to be renamed in the **Object name** field.
4. Specify only the new name of the object in the **New Name** field. Do not specify the Context.
5. Select to save the old name, if you want to save it.
6. Click the Save button.
7. A confirmation message appears indicating the rename object operation was successful.

Figure 7-6 Renaming an Object



8

Managing Rights

Rights refers to eDirectory trustee rights and trustees. When you create a tree, the default rights assignments provide your network a generalized access and security. Identity Console lets you perform the following rights-related tasks:

- "Modifying the Inherited Rights Filter" on page 47
- "Modifying the Trustee Rights" on page 48
- "Viewing the Effective Rights" on page 49

For more information about eDirectory rights, see the *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

Modifying the Inherited Rights Filter

eDirectory provides an Inherited Rights Filter (IRF) mechanism to block rights inheritance on individual subordinate items.

For more information about Inherited Rights Filters, see the *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

1. Click the **Rights Management** option from the Identity Console landing page
2. Select **Inherited Rights Filter**.

   NOTE: Inherited Rights Filter is selected by default.

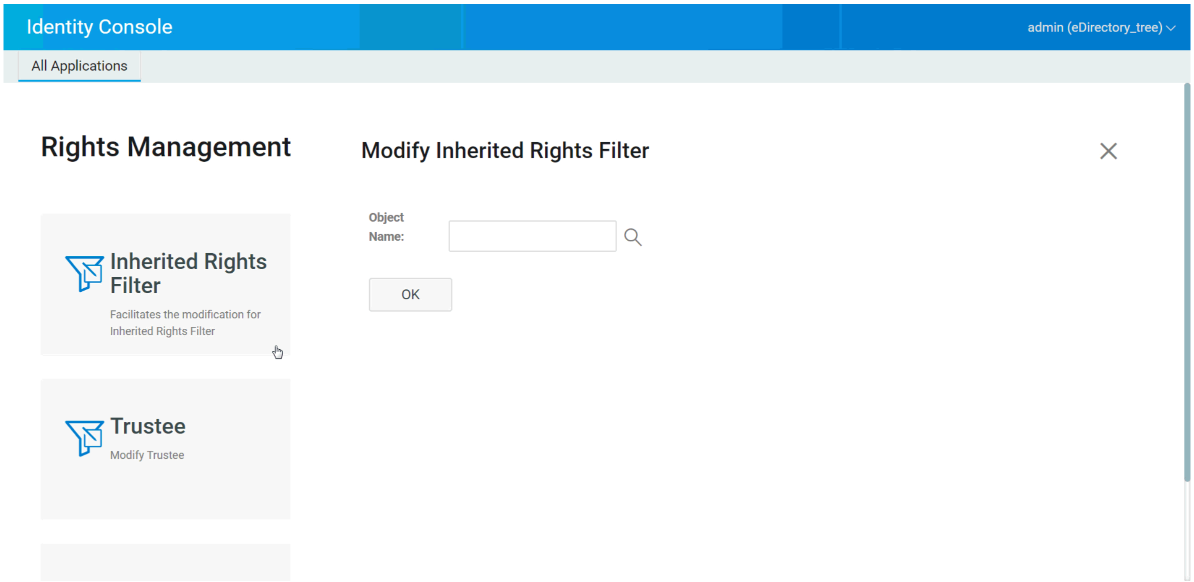
   ---

3. Specify the full name of the object whose inherited rights filter you want to modify, or use the Object Selector 🔍 icon to find it, then click **OK**.

   This displays a list of the inherited rights filters that have already been set on the object.
4. Under **Properties**, edit the list of inherited rights filters as needed, then click **Apply**.

   To edit the list of filters, you must have the Supervisor or Access Control right to the ACL property of the object. You can set filters that block inherited rights to the object as a whole, to all the properties of the object, and to individual properties.

Figure 8-1 Modifying the Inherited Rights Filter



Modifying the Trustee Rights

A trustee is one object that has been granted explicit rights to another object in your directory tree. To modify the trustee list for a given object:

1 Click the **Rights Management** option from the Identity Console landing page

2 Select **Trustee**.

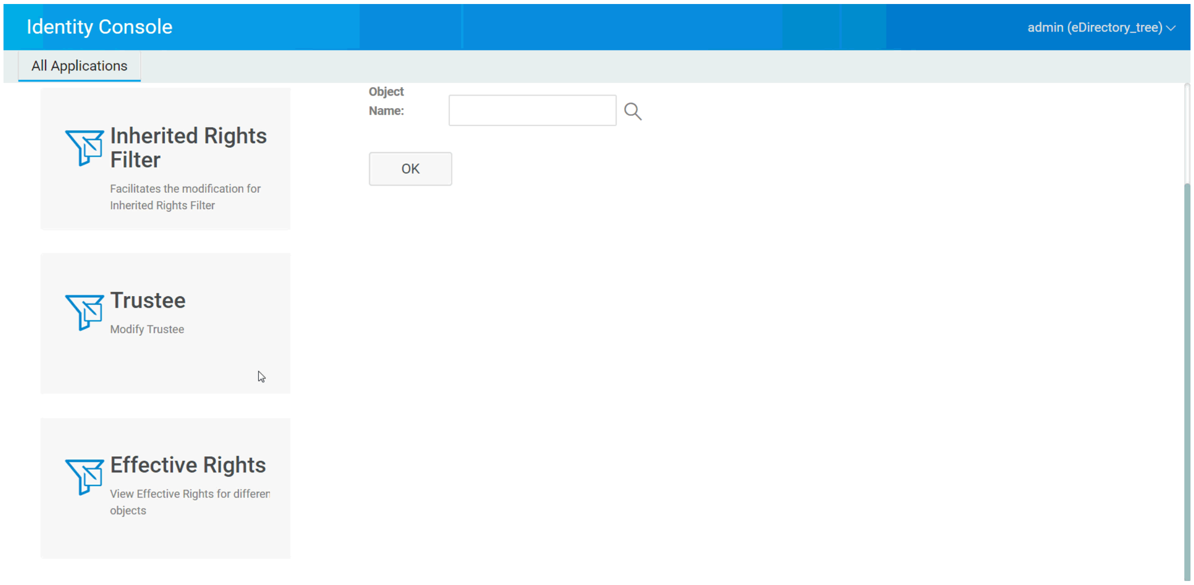
3 Specify, or use the Object Selector 🔍 icon to find, the name of the object whose trustee list you want to view, then click **OK**.

This opens a list of the object's currently assigned trustees.

4 Modify the trustee list as needed, then click **OK**.

- Add a trustee by clicking the + icon.
- Remove a trustee by selecting its check box and clicking the 🗑.icon.
- Modify a trustee's rights assignment by selecting the **Assigned Rights** link for that trustee.

Figure 8-2 Modifying the Trustee Rights



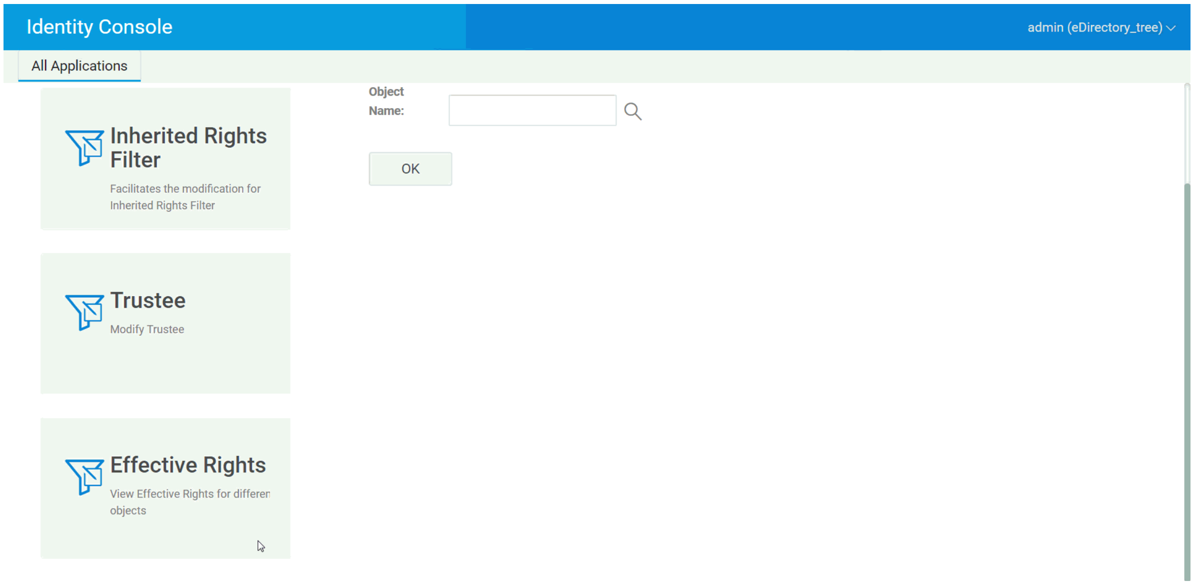
Viewing the Effective Rights

Effective rights is the combination of explicit and inherited rights that an object has at any point in the directory tree. To view an object's effective rights to another object:

1. Click the **Rights** Management option from the Identity Console landing page
2. Select **Effective Rights**.
3. Specify, or use the Object Selector 🔍 icon to find, the name of the trustee whose rights you want to view, then click **OK**.
4. In the Object name field, specify the name of the object for which you want to view the trustee's effective rights.

   eDirectory calculates the effective rights and displays them in the **Effective Rights** field.

Figure 8-3 Viewing the Effective Rights



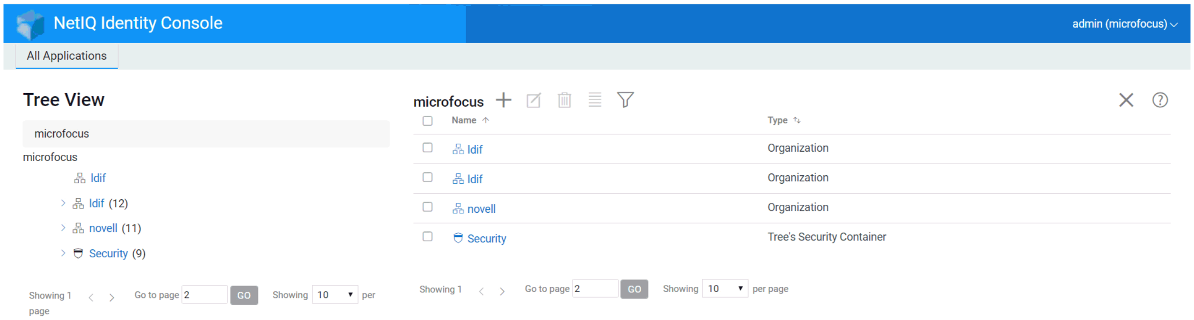
9 Tree View

Tree view lets you browse a directory tree and create, delete and modify various objects in that tree. Tree view has a navigation frame and a content frame.

Tree View Navigation Frame

In the Tree view, the navigation frame displays the directory structure. The navigation frame displays Containers including Volume (file system), objects etc. All the options displayed under the navigation frame are click-able to help you to browse the directory structure. By default, navigation frame displays up to 10 subordinate objects per container but you can change this setting below the navigation frame panel in Tree View.

Figure 9-1 *The Navigation Frame in Tree View*



☐	Name	Type
☐	ldif	Organization
☐	ldif	Organization
☐	novell	Organization
☐	Security	Tree's Security Container

Tree View Content Frame

Selecting one of the container objects in the Navigation frame causes the Content frame to display all the objects in that container. The Content frame is where you actually view and modify directory objects. The Content frame includes a header which has several available actions:

Title Bar: The Content frame’s title bar displays the name of the currently selected container object.

Object List Header: The object list header provides access to the following:

- Add: Click the + icon to add a new object.

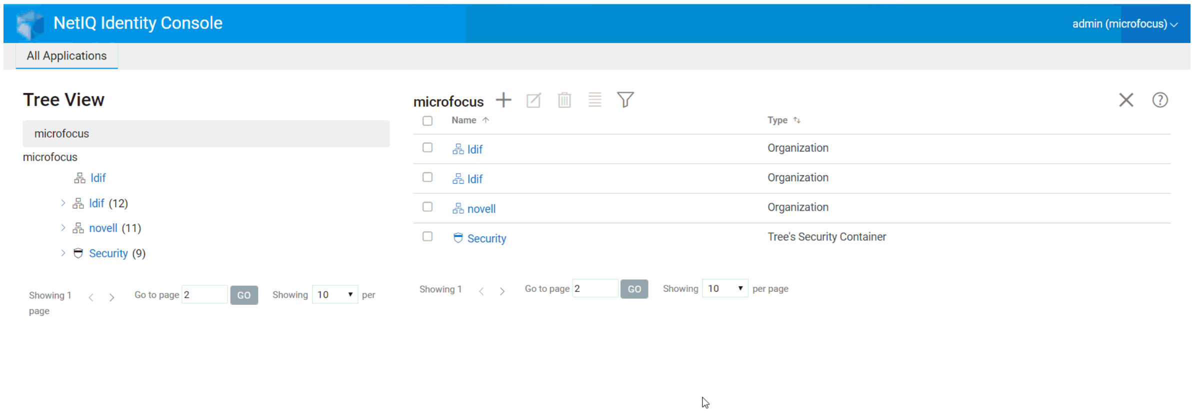
- **Modify**: Select an object and click the ✎ icon to modify.This opens the property book for the selected object so you can modify their attributes. Multiple objects can not be modified together.
- **Delete**: Select an object and click the 🗑 icon to delete the selected objects. Multiple objects can be deleted together. Nonleaf objects can not deleted.
- **Actions**: Select an object and click the ≡ icon which opens a drop-down menu of supported tasks for the selected objects. To perform a task, select it from the drop-down menu and provide the required information.
- **Object Count**: Tree view lists the number of objects in the current page at the bottom of the page. By default, content frame displays up to 20 subordinate objects per container but you can change this setting.
- **Select All**: The checkbox in the header functions as a “select all” checkbox for the current page of objects.
- **Sort**: Both **Name** and **Type** columns are sortable. Click either of these to toggle the object sort between ascending and descending alphabetical order.
- **Search Filter**: Click the ▽. icon to launch the filter pop-up window. Using this option, you can create a filter that limits the objects displayed in the object list. You can filter on object type and object name, as needed.

  Select ⊕ option to open the Advanced Filter dialog that lets you create a filter using almost any object attribute. For more information, see “Configuring Advanced Search” on page 26.

To perform an action on an object, select its checkbox, then select the action icon ≡ from the Object List header. Select the (current level) object to perform an action on the container in which you are currently browsing. The following actions can be performed using this option:

- “Modifying the Inherited Rights Filter” on page 47
- “Modifying the Trustee Rights” on page 48
- “Extending an Object” on page 60
- “Renaming an Object” on page 45
- Set Password
- “Viewing the Effective Rights” on page 49

Figure 9-2 *Content Frame in Tree View*



☐ Name	Type
☐ ldif	Organization
☐ ldif	Organization
☐ novell	Organization
☐ Security	Tree's Security Container

10 Managing Schema

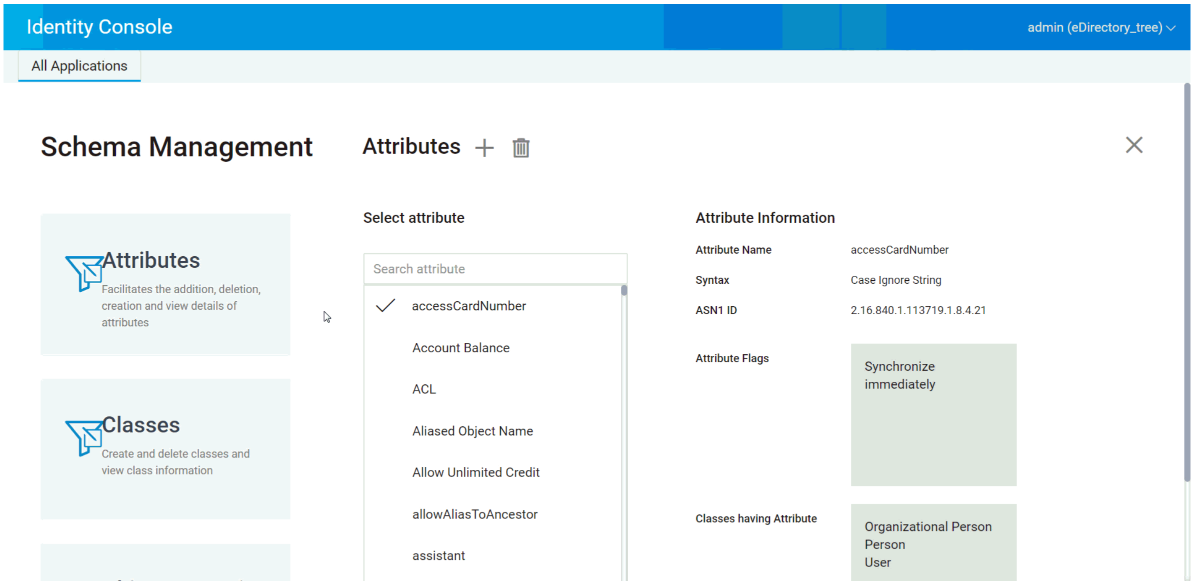
The directory schema defines the types of objects that can be created in your tree (such as Users, Printers, Groups etc.) and what information is required or optional at the time the object is created. Identity Console provides the following schema-related tasks:

Creating an Attribute

You can define your own custom types of attributes and add them as optional attributes to existing object classes. However, you cannot add mandatory attributes to existing classes. To create an attribute:

1. Click the **Schema Management** option from the Identity Console landing page.
2. Click the + icon.
3. In the Create Attribute page, enter the following details:
    - Attribute Name
    - ASN1 ID (optional)
    - Syntax
    - Attribute Flags
4. After entering all the required details, click the Create button.
5. A confirmation appears indicating the attribute has been created.

Figure 10-1 Creating an Attribute



Attribute Name: accessCardNumber

Syntax: Case Ignore String

ASN1 ID: 2.16.840.1.113719.1.8.4.21

Attribute Flags: Synchronize immediately

Classes having Attribute: Organizational Person, Person, User

Creating a Class

Using the **Schema Management** option you can define your own classes. You can then extend individual objects with the properties defined in your classes. To create a class:

1. Click the **Schema Management** option from the Identity Console landing page and select **Classes**.
2. Click the + icon.
3. In the Create Attribute page, enter the following details:
   - Class Name
   - ASN1 ID (optional)
   - Class Flags: Select one of the following Class flags:
     - **Effective Class:** Set this flag if you want to create an effective class, which can be used to create objects.
     - **Non-Effective Class:** Used as a placeholder for a group of attributes. A non-effective class cannot be used to create objects but can be specified as a class from which other classes can inherit attributes. For example, the Person class is a non-effective class that holds attributes inherited by the User class.
     - **Auxiliary Class:** A collection of attributes that can be associated only with individual objects, not with entire classes.
     - **Container Class:** Set this flag if you want to make this a container class. When it is used to create objects, those objects become container objects (such as OU). Do not set this flag for a leaf object class.

   NOTE: If you select Effective and Non-Effective Classes, you also have to specify values for Super Class. In case you choose the Auxiliary Class, Super Class will be optional for you.

4. After entering all the required details, click **Next**.

5. In the next screen, select the optional, mandatory and naming attributes and click **OK**.
6. A confirmation appears indicating the class has been created.

Assigning Attributes to a Class

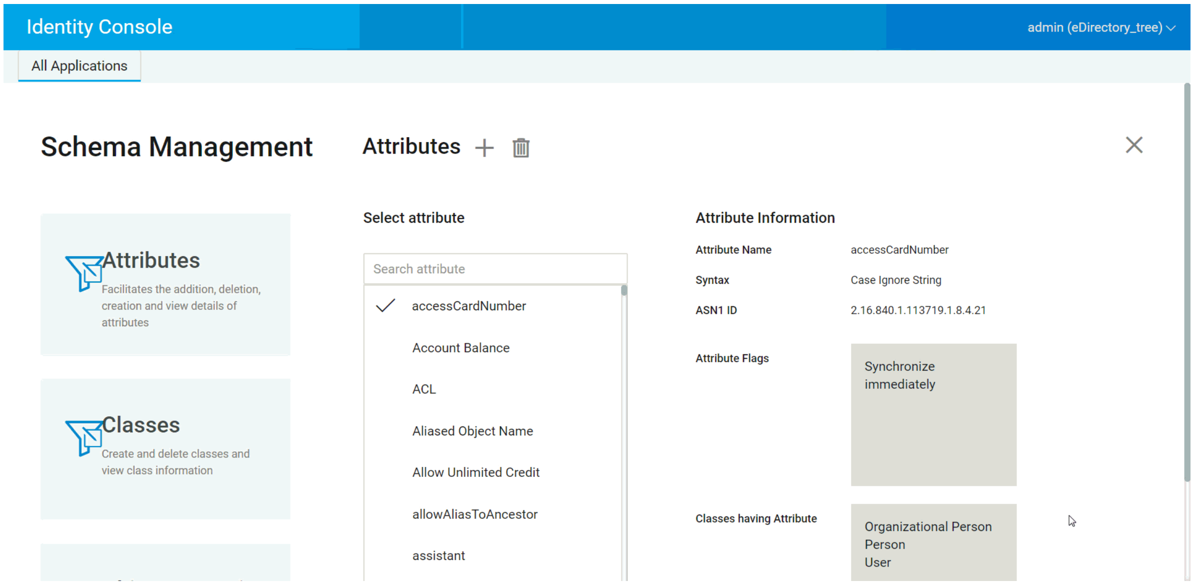
You can add optional attributes to existing classes if your organization's information needs change or if you are preparing to merge trees. To add an attribute to an existing class:

NOTE: Mandatory attributes can be defined only while creating a class. A mandatory attribute is one that must be completed when an object is being created.

---

1. Click the **Schema Management** option from the Identity Console landing page and select **Classes**.
2. Click any class listed under **Select class**.
3. The corresponding class information is displayed on the right side of the screen.
4. Click the + button next to the **Attributes** option and select the attributes you want to add and click **Add** > **Save**.

Figure 10-2 Assigning Attributes to a Class



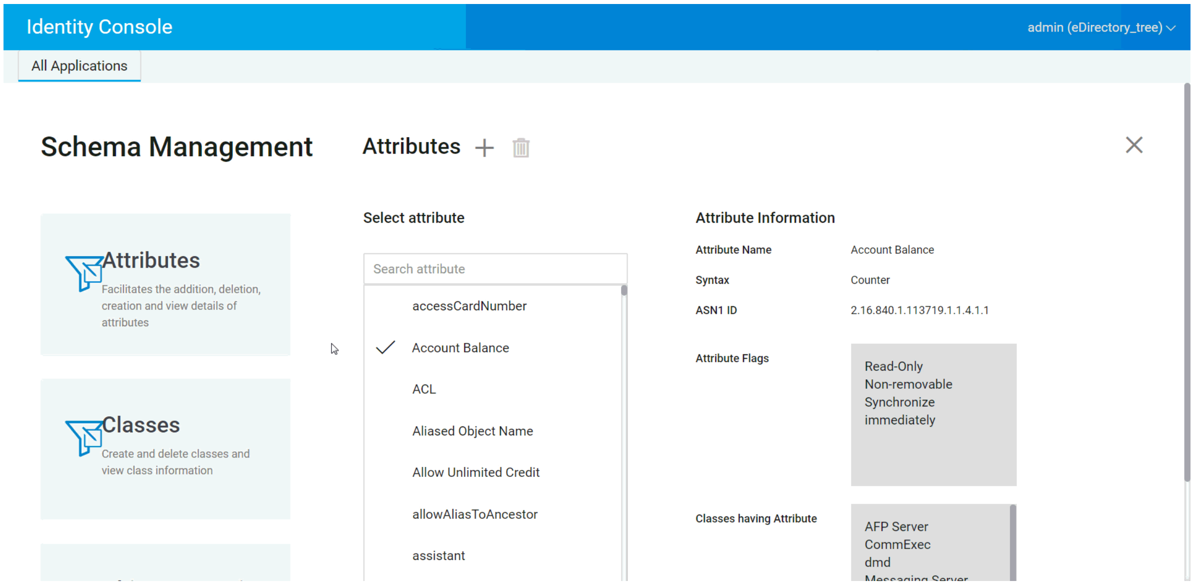
Attribute Name: accessCardNumber
Syntax: Case Ignore String
ASN1 ID: 2.16.840.1.113719.1.8.4.21
Attribute Flags: Synchronize immediately
Classes having Attribute: Organizational Person
Person
User

Viewing Attribute Information

You can view an attribute's structural details such as Syntax, flags and Classes that use the attribute. To see an attribute's information:

1. Click the **Schema Management** option from the Identity Console landing page and select **Attributes**.
2. Click any attribute listed under **Select attribute**.
3. The corresponding attribute information is displayed on the right side of the screen.

Figure 10-3 Viewing Attribute Information



Attribute Information

Attribute Name Account Balance

Syntax Counter

ASN1 ID 2.16.840.1.113719.1.1.4.1.1

Attribute Flags
Read-Only
Non-removable
Synchronize immediately

Classes having Attribute
AFP Server
CommExec
dmd

Deleting an Attribute

You can delete unused attributes that are not part of the base schema of your eDirectory tree. This might be useful after merging two directory trees, or if an attribute has become obsolete over time. To delete an attribute:

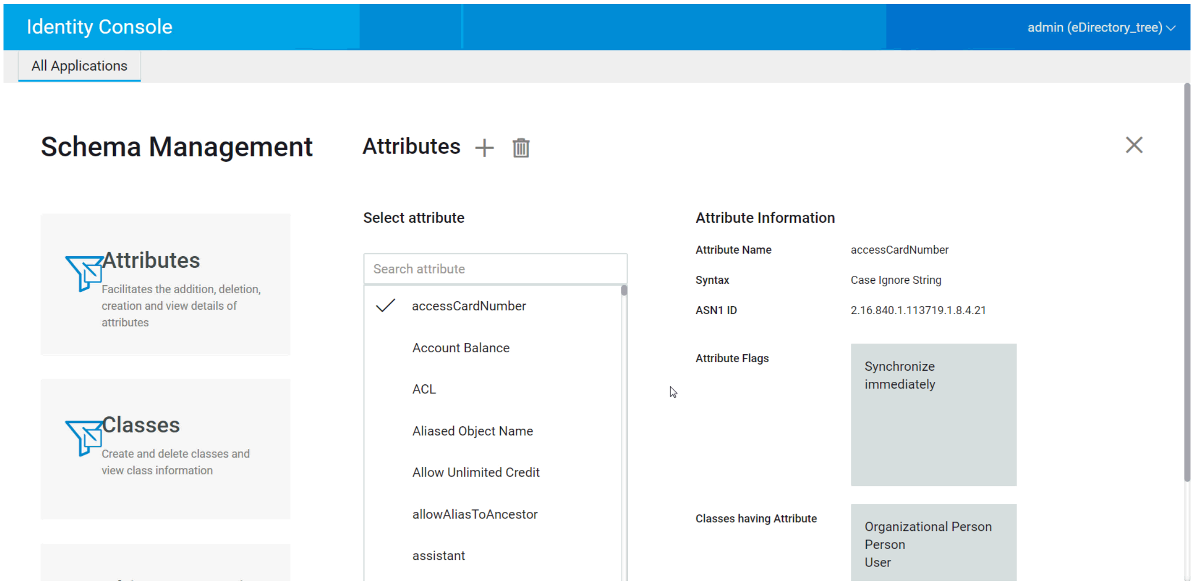
1. Click the **Schema Management** option from the Identity Console landing page and select **Attributes**.
2. Select the attribute you want to delete under the **Select attribute** list and click the 🗑 icon.

   NOTE: The 🗑 icon will be enabled only when you select an attribute that can be deleted.

   ---

3. Click **OK** to confirm the deletion.

Figure 10-4 *Deleting an Attribute*



Attribute Information

Attribute Name: accessCardNumber
Syntax: Case Ignore String
ASN1 ID: 2.16.840.1.113719.1.8.4.21
Attribute Flags: Synchronize immediately
Classes having Attribute: Organizational Person
Person
User

Deleting a Class

You can delete unused classes that are not part of the base schema of your eDirectory tree. Identity Console prevents you from deleting classes that are currently being used in locally replicated partitions. To delete a class:

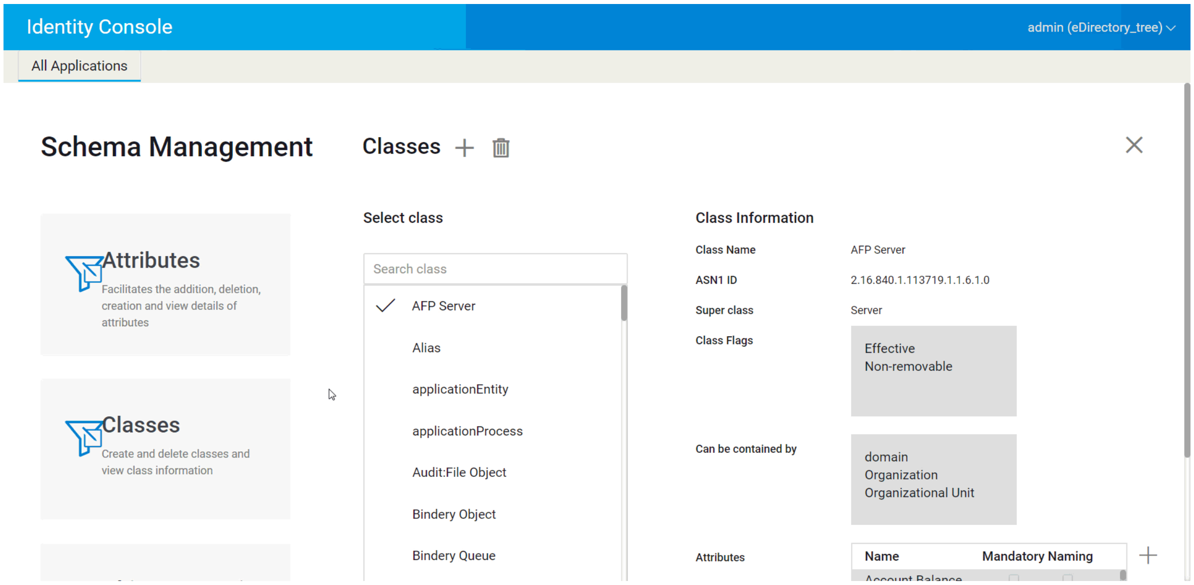
1. Click the **Schema Management** option from the Identity Console landing page and select **Classes**.
2. Select the class you want to delete under the **Select class** list and click the 🗑 icon.

NOTE: The 🗑 icon will be enabled only when you select a class that can be deleted.

---

3. Click **OK** to confirm the deletion.

Figure 10-5 Deleting a Class



Class Name: AFP Server
ASN1 ID: 2.16.840.1.113719.1.1.6.1.0
Super class: Server
Class Flags: Effective, Non-removable
Can be contained by: domain, Organization, Organizational Unit

Extending an Object

Perform the following steps to extend an object:

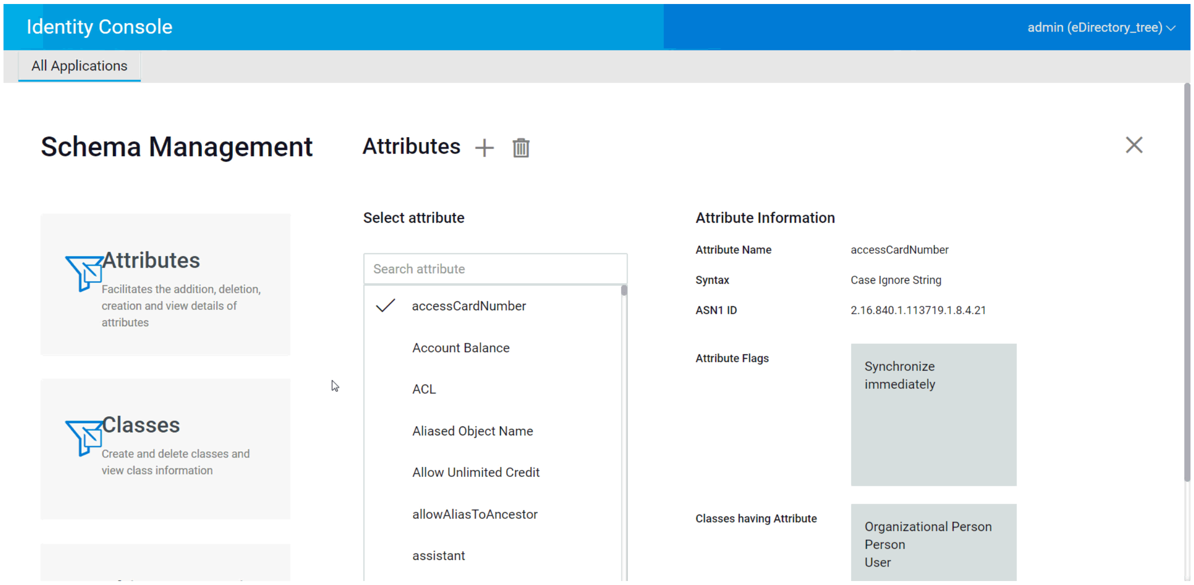
1. Click the **Schema Management** option from the Identity Console landing page and select **Object Extension**.
2. Specify the object name or use the object selector to select the object to be extended, click the 🔍 .icon.
3. Click the + icon and select the auxiliary class, then click **OK**.

NOTE: If any mandatory attribute is attached to the selected auxiliary class, then you will be prompted to enter the required values in the **Mandatory Attributes** pop-up window.

---

4. A confirmation message appears stating that the auxiliary class has been added to the object.
5. To remove an existing auxiliary class from the object, select the class and click the 🗑 icon.

Figure 10-6 *Extending an Object*



Attribute Information

Attribute Name: accessCardNumber

Syntax: Case Ignore String

ASN1 ID: 2.16.840.1.113719.1.8.4.21

Attribute Flags: Synchronize immediately

Classes having Attribute: Organizational Person
Person
User

11

Managing Audit Events

This chapter explains how to manage various audit events using Identity Console. Using this feature, you can enable or disable audit events for your NCP server.

Configuring CEF Audit Events

1. Log in to Identity Console using your username and password.
2. Select **Auditing**.
3. Select the NCP Server you want to monitor, and then click **OK**.

   NOTE: After you enable CEF events for any NCP server for the first time, few events will be selected by default.

4. Configure the CEF audit events:
   - **Events Configuration:** Enable or disable the following events based on the audit required for your environment:

NOTE: Individual event categories under the events configuration section will be collapsed by default. You can expand each category to select individual events.

Options	Description
Security Events	Select the security events for which you want to log events. You can log events to add or delete member, to detect intruder, to change password and to authenticate users etc.
Object Events	Select the object events for which you want to log events. You can log events to create delete, rename, move and search objects.
Attribute Events	Select the attribute events for which you want to log events. You can log events to read and delete attributes and to add, delete and compare attribute value.
LDAP Events	Select the LDAP events for which you want to log events.

- **Advanced Settings:** Using the advance settings, You can perform the following actions.
  - **Global:** You can select or clear the global settings for duplicate entries.
    - **Do Not Send Replicated Events:** Select this option to stop receiving duplicate events due to replication from other servers.
  - **Log Event's Values:** The events are logged into a text file. Event values with more than 768 bytes in size are considered "large values." You can log events of any size.
    - **Log Large Values:** Select this option to log events that are more than 768 bytes in size.
    - **Log Attributes Values:** Select this option to display the attribute values. This is applicable to **Add Value** and **Delete Value** events only.
    - **Log Encrypted Attribute Values:** Select this option to display the encrypted attribute values. This is applicable to **Add Value** and **Delete Value** events only.

  NOTE: If the event size is more than 768 byte size, the event value is truncated and saved to the log file.

Understanding the CEF Event Types

You can configure CEF to log events in the following categories:

- Security
- Objects
- Attributes
- LDAP

You can audit the following default set of event types:

Category	Event Type
Security	◆ ACL Changed ◆ Add Member ◆ Delete Member ◆ Intruder Detected ◆ Login Disabled ◆ Login Enabled ◆ Login ◆ Change Security Equals ◆ Audit Config ◆ Change Password ◆ Account Unlock ◆ Logout ◆ Connection ◆ Impersonate ◆ Authenticate ◆ Verify Password ◆ Change Login Config ◆ Query Credentials
Objects	◆ Create Object ◆ Delete Object ◆ Rename Object ◆ Move Object ◆ DSA Read ◆ Search
Attributes	◆ Read Attribute ◆ Delete Attribute ◆ Add Value ◆ Delete Value ◆ Compare Attribute Value

Category	Event Type
LDAP	- LDAP Bind - LDAP Bind Response - LDAP Unbind - LDAP Connection - LDAP Search - LDAP Search Response - LDAP Search Entry Response - LDAP Add - LDAP Add Response - LDAP Compare - LDAP Compare Response - LDAP Modify - LDAP Modify Response - LDAP Delete - LDAP Delete Response - LDAP Modify DN - LDAP Modify DN Response - LDAP Abandon - LDAP Extended Operation - LDAP System Extended Operation - LDAP Extended Operation Response - Modify LDAP Server Configuration - Unknown LDAP Operation - LDAP Password Modify

Configuring the CEF Audit Filtering

Using filters and event notifications, CEF is capable of reporting when a specific type of event occurs, or when it does not occur. You can also filter events for one or more specific object classes or attributes, depending on the event type. CEF evaluates all the generated events against the configured filters on the eDirectory server and logs only the events matching to those filters.

This section provides the information you need to configure your system filters and notifications.

- "Filtering eDirectory Events With Exclusion Filter" on page 67
- "Filtering CEF Object Events" on page 67
- "Filtering CEF Attribute Events" on page 68

Filtering eDirectory Events With Exclusion Filter

Click the **Exclusion Filter** link to configure filtering for those object classes and attributes for which you do not want an event to be generated. You can select object classes and attributes.

To configure filtering for unwanted eDirectory Events:

1. In Identity Console, select **Auditing** from the home page.
2. Select the NCP Server you want to monitor, and then click **OK**.
3. Now go to **Advanced Settings** and click **Exclusion Filter** under **Filters**.

   The CEF Exclusion Filtering window appears.
4. In the **Available Object Classes** list, select object classes for which you do not want to collect events, then click the right arrow to move them to the **Selected Object Classes** list.
5. In the **Available Attributes(s)** list, select any number of attributes. Select the attribute and click the right arrow to add the attribute to the selected list of attributes.
6. Click **Ok**.

Using the configured filter, CEF audit module stops generating events for all the selected object classes and attributes.

Filtering CEF Object Events

You can configure filtering for Objects to look for only a specific event or events. For example, if you want to be notified when someone creates a user account in eDirectory, you can create a filter selecting the User Object class to log events for creating a new user object.

To configure accounts filtering, click the Object Events link, select the class, and then click **OK** to exit the application.

To configure filters for Account Management events:

1. In Identity Console, select **Auditing** from the home page.
2. Select the NCP Server you want to monitor, and then click **OK**.
3. Now go to **Advanced Settings** and click **Object Events** under **Filters**.

   The CEF Object Filtering window appears.
4. In the **Available Object Classes** list, select any object class, then click the right arrow to move the object class to the **Selected Object Classes** list, and then click **OK**.

Using the configured filter, CEF audit module checks all generated events for the selected object classes and logs those events.

Filtering CEF Attribute Events

Click the **Attribute Events** link to configure filtering for the Attribute Events. For example, if you want to be notified when someone adds a new attribute value in eDirectory, you can create a filter to log events for adding a new value.

To configure filtering for Attribute Events:

1. In Identity Console, select **Auditing** from the home page.
2. Select the NCP Server you want to monitor, and then click **OK**.
3. Now go to **Advanced Settings** and click **Attribute Events** under **Filters**.

   The **Attributes Configuration Filtering** window appears.
4. In the **Available Object Classes** list, select object classes for which you want to collect events, then click the right arrow to move them to the **Selected Object Classes** list.
5. In the **Available Attributes(s)** list, select any number of attributes for the selected object classes. Select the attribute and click the right arrow to add the attribute to the selected list of attributes.

   NOTE: If you select an object class, then all the Attribute Events for all attributes on that object class are selected. In this case, you will get all the Attribute Events for the all attributes on the selected object classes.
6. Click **OK**.

With the filter configured, CEF audit module checks the generated events for all the selected object classes and attributes and logs those events.

12 Managing Encrypted Attributes

Identity Console is able to securely read the encrypted attributes from your eDirectory server. Using Identity Console, you can create, modify or delete several policies for these encrypted attributes.

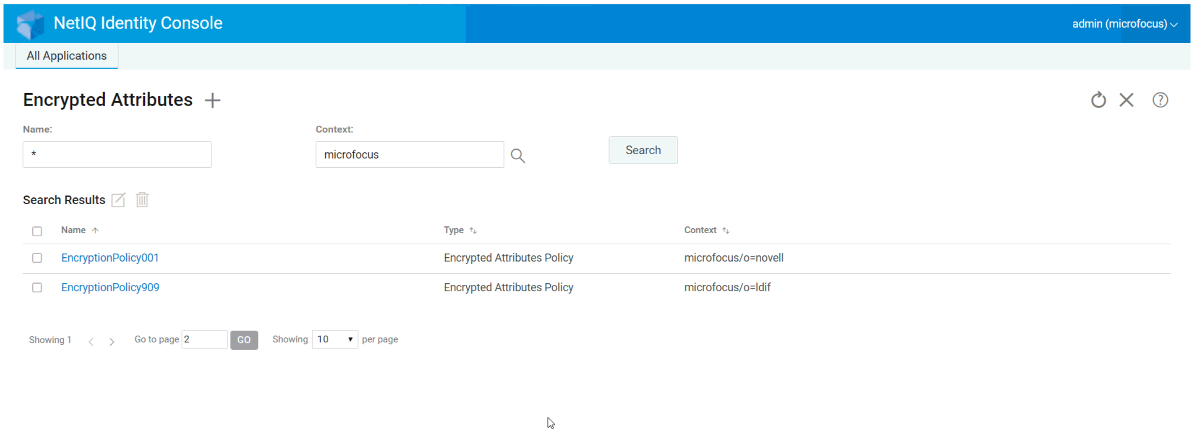
- "Creating a Policy for Encrypted Attributes" on page 69
- "Deleting an Encrypted Attributes Policy" on page 70
- "Modifying an Encrypted Attributes Policy" on page 70

Creating a Policy for Encrypted Attributes

To create a new attribute policy:

1. Click the **Encrypted Attributes** option from the Identity Console landing page.
2. Click the + icon.
3. In the Create Encrypted Attributes Policy page, enter the following details:
   - Specify the policy name
   - Enter or select the Context
   - Select the NCP Server
   - Select attributes
4. After specifying all the required details, click **Finish**.
5. A confirmation appears indicating the policy has been created.

Figure 12-1 *Creating an Encrypted Attributes Policy*



Name: *

Context: microfocus

☐	Name	Type	Context
☐	EncryptionPolicy001	Encrypted Attributes Policy	microfocus/o=novell
☐	EncryptionPolicy909	Encrypted Attributes Policy	microfocus/o=ldif

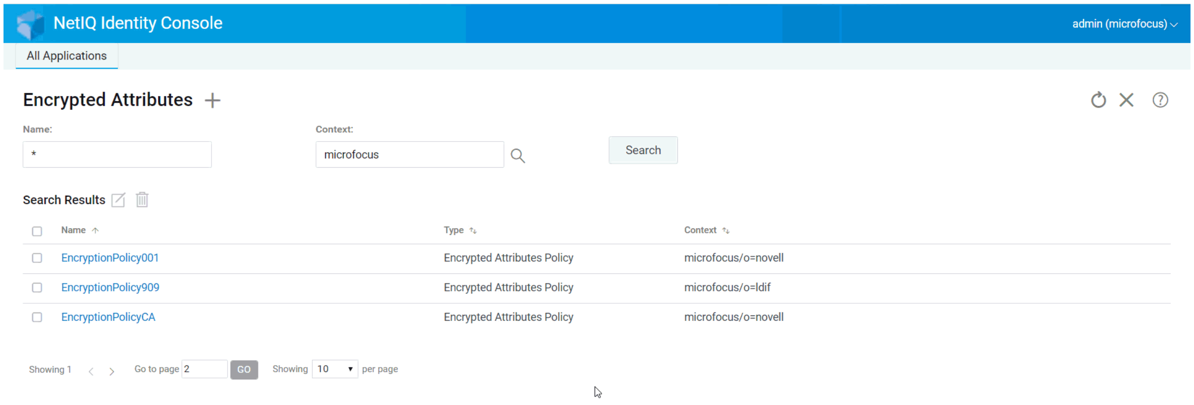
Showing 1 Go to page 2 Showing 10 per page

Deleting an Encrypted Attributes Policy

To delete an encrypted attributes policy:

1. Click the **Encrypted Attributes** option from the Identity Console landing page.
2. Specify the name and context of the attribute or use the search feature to find it, then click the Search button.
3. Select the attribute(s) from the list and click the 🗑 icon.
4. A confirmation appears indicating the policy has been deleted.

Figure 12-2 Deleting an Encrypted Attribute Policy



Name: *

Context: microfocus

Go to page 2

Showing 10 per page

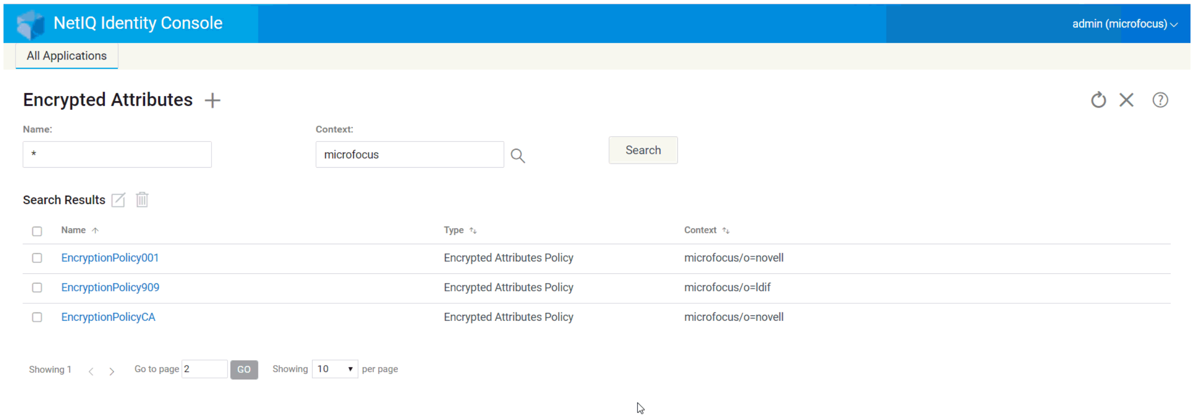
☐	Name	Type	Context
☐	EncryptionPolicy001	Encrypted Attributes Policy	microfocus/o=novell
☐	EncryptionPolicy909	Encrypted Attributes Policy	microfocus/o=ldif
☐	EncryptionPolicyCA	Encrypted Attributes Policy	microfocus/o=novell

Modifying an Encrypted Attributes Policy

To modify an encrypted attributes policy:

1. Click the **Encrypted Attributes** option from the Identity Console landing page.
2. Type the name and context of the object, then click the Search button.
3. Select the attribute from the objects list and click the ✎ icon.
4. Make your changes, then click the Save button.
5. A confirmation appears indicating the policy has been modified.

Figure 12-3 *Modifying an Encrypted Attributes Policy*



Name: *

Context: microfocus

☐	Name	Type	Context
☐	EncryptionPolicy001	Encrypted Attributes Policy	microfocus/o=novell
☐	EncryptionPolicy909	Encrypted Attributes Policy	microfocus/o=ldif
☐	EncryptionPolicyCA	Encrypted Attributes Policy	microfocus/o=novell

13 Managing Encrypted Replication

To enable encrypted replication, you need to configure a partition for encrypted replication. Configuration settings are stored in the partition Root object. You can only choose to enable encrypted replication at a partition level. When you enable encrypted replication at a partition level, replication between all the replicas hosting the partition is encrypted. For example, consider partition P1 has replicas R1, R2, R3, and R4. You can encrypt the replication between all the replicas.

- “Enabling Encrypted Replication for Partitions” on page 73

Enabling Encrypted Replication for Partitions

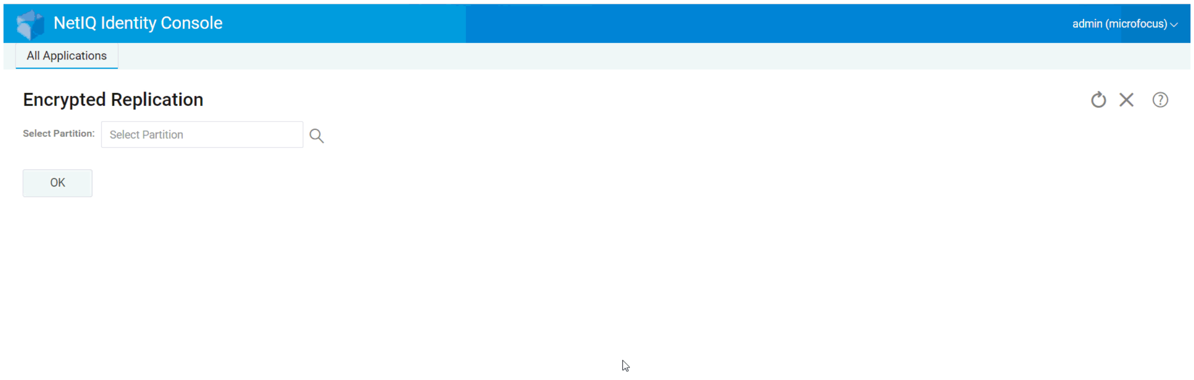
To enable encrypted replication for partitions:

NOTE: To enable a partition for encrypted replication, all the servers hosting the partition must be eDirectory 9.2 or later servers.

---

1. Click the **Encrypted Replication** option from the Identity Console landing page.
2. Specify or browse to the partition for which you want to enable encrypted replication.
3. Ensure to select the **Enable Encrypted replication** option. While disabling the encrypted replication for a partition, deselect this option.
4. Click **Finish**.
5. A confirmation appears indicating that encrypted replication has been enabled.

***Figure 13-1** Enabling Encrypted Replication for Partitions*



14

Managing Partitions and Replicas

Partition and replica operations let you manage eDirectory’s physical design and distribution across your directory servers.

Partitions create logical divisions of the eDirectory tree. For example, if you choose an Organizational Unit and create it as a new partition, you split the Organizational Unit and all of its subordinate objects from its parent partition. The Organizational Unit you choose becomes the root of a new partition. The replicas of the new partition exist on the same servers as the replicas of the parent, and objects in the new partition belong to the new partition’s root object.

The following tasks can be performed using the Partition module:

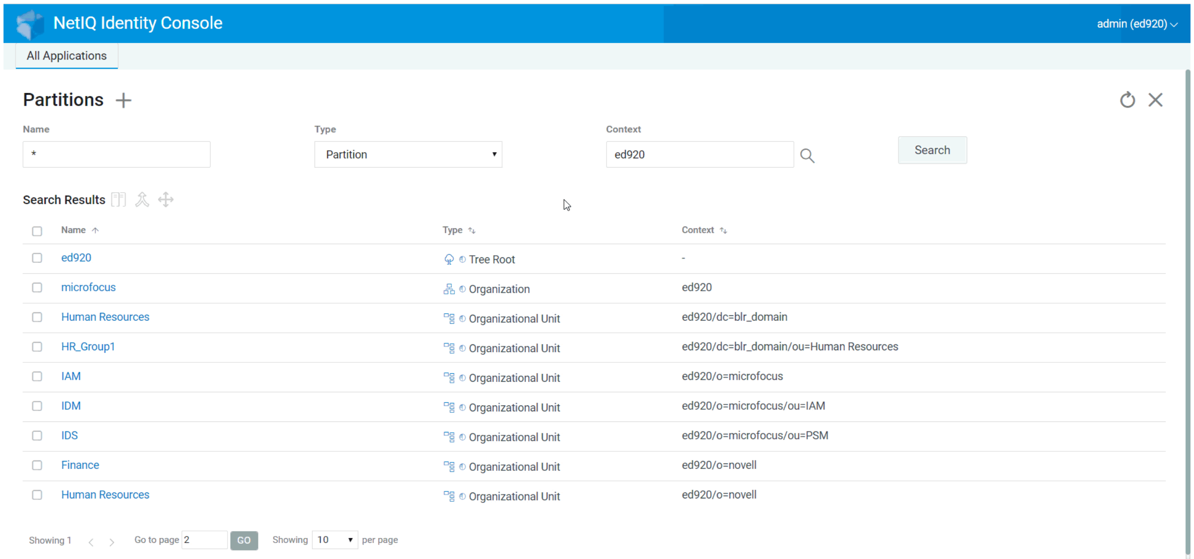
- “Creating Partition” on page 75
- “Merge Partitions” on page 76
- “Modifying Partitions” on page 77
- “Moving a Partition” on page 77

Creating Partition

To create a new partition:

1. Click the **Partition Management** option from the Identity Console landing page.
2. Click the + icon.
3. In the Create Partition page, specify the container to use as the root of the new partition, or use the Object Selector 🔍 icon to locate it, then click **Create**.
4. A confirmation appears indicating the partition has been created.

Figure 14-1 *Creating a New Partition*



Partitions +

Name: *
Type: Partition
Context: ed920
Search

Search Results

☐	Name	Type	Context
☐	ed920	Tree Root	-
☐	microfocus	Organization	ed920
☐	Human Resources	Organizational Unit	ed920/dc=blr_domain
☐	HR_Group1	Organizational Unit	ed920/dc=blr_domain/ou=Human Resources
☐	IAM	Organizational Unit	ed920/o=microfocus
☐	IDM	Organizational Unit	ed920/o=microfocus/ou=IAM
☐	IDS	Organizational Unit	ed920/o=microfocus/ou=PSM
☐	Finance	Organizational Unit	ed920/o=novell
☐	Human Resources	Organizational Unit	ed920/o=novell

Showing 1 < > Go to page 2 GO Showing 10 per page

Merge Partitions

To merge partitions with its parent partition:

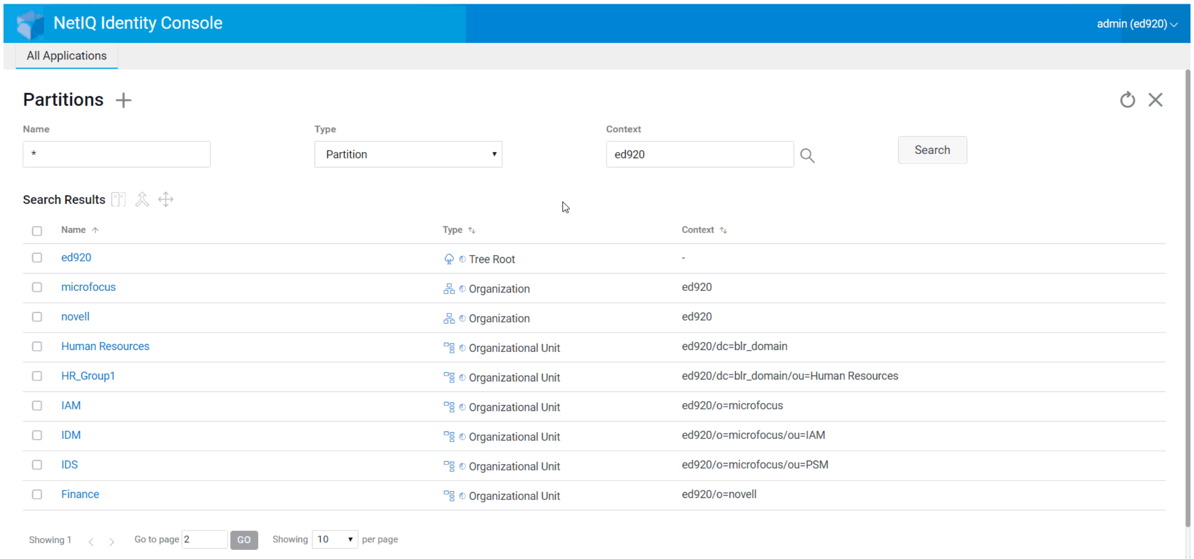
1 Click the **Partition Management** option from the Identity Console landing page.

2 Specify the name, type and context of the partition or use the search feature to find it, then click the Search button.

3 Select the partition from the search list and click on the icon and click **OK**.

4 A confirmation appears indicating the partition has been merged.

Figure 14-2 *Merging Partitions*



Partitions +

Name: *
Type: Partition
Context: ed920
Search

Search Results

☐	Name	Type	Context
☐	ed920	Tree Root	-
☐	microfocus	Organization	ed920
☐	novell	Organization	ed920
☐	Human Resources	Organizational Unit	ed920/dc=blr_domain
☐	HR_Group1	Organizational Unit	ed920/dc=blr_domain/ou=Human Resources
☐	IAM	Organizational Unit	ed920/o=microfocus
☐	IDM	Organizational Unit	ed920/o=microfocus/ou=IAM
☐	IDS	Organizational Unit	ed920/o=microfocus/ou=PSM
☐	Finance	Organizational Unit	ed920/o=novell

Showing 1 < > Go to page 2 GO Showing 10 per page

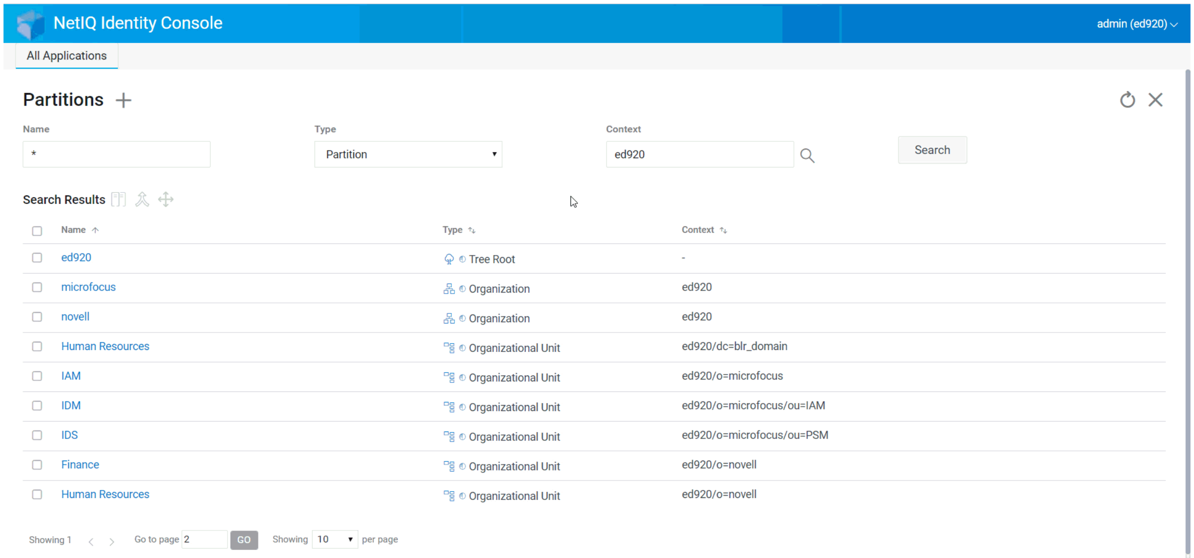
Modifying Partitions

To modify partitions:

1. Click the **Partition Management** option from the Identity Console landing page.
2. Type the name, type and context of the partition, then click the Search button.
3. Select the partition from the search list and click on the ◫ icon.
4. Click the **Edit** option under **Filter** to change Replica filters and its corresponding Classes and Attributes and click **OK**.

   In case you selected **Server** in the **Type** field, you will see the list of all the servers. Clicking on each server will display a list of all the partitions in the server.
5. A confirmation appears indicating the partition has been modified.

Figure 14-3 *Modifying Partitions*



Name: *

Type: Partition

Context: ed920

☐	Name	Type	Context
☐	ed920	Tree Root	-
☐	microfocus	Organization	ed920
☐	novell	Organization	ed920
☐	Human Resources	Organizational Unit	ed920/dc=blr_domain
☐	IAM	Organizational Unit	ed920/o=microfocus
☐	IDM	Organizational Unit	ed920/o=microfocus/ou=IAM
☐	IDS	Organizational Unit	ed920/o=microfocus/ou=PSM
☐	Finance	Organizational Unit	ed920/o=novell
☐	Human Resources	Organizational Unit	ed920/o=novell

Showing 1 Go to page 2 GO Showing 10 per page

Moving a Partition

Moving a partition lets you move a subtree in your directory tree. This is also known as a prune and graft operation. You can only move partitions that have no subordinate partitions. If subordinate partitions exist, you must first merge those partitions before performing the move operation.

When you move a partition, eDirectory changes all references to the partition Root object. Although the object's common name remains unchanged, the complete name of the container (and of all its subordinates) changes.

NOTE: When you move a partition, you must follow the eDirectory containment rules. For example, you cannot move an Organizational Unit directly under the root of the directory tree, because the root's containment rules permit only Locality, Country, or Organization objects, but not Organizational Unit objects.

To move a Partition:

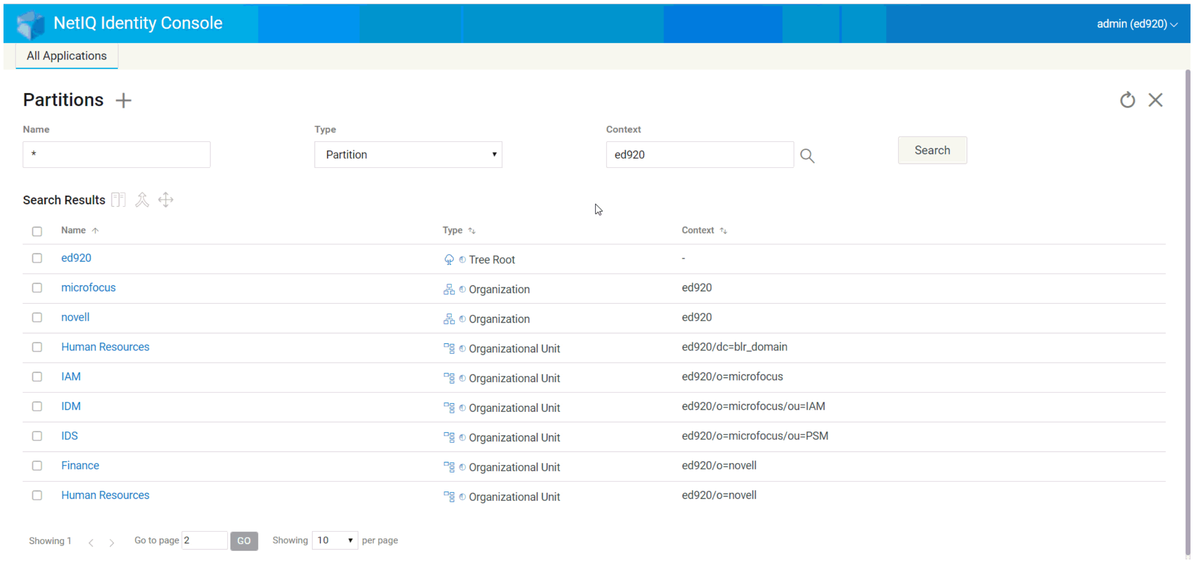
1. Click the **Partition Management** option from the Identity Console landing page.
2. Type the name, type and context of the partition, then click the Search button.
3. Select the partition from the search list and click the ✥ icon.
4. Select the destination container object into which you want to move the specified partition and click **OK**.

   NOTE: **The Create an alias in place of moved partition** creates a pointer to the partition's new location. This allows any operations that are dependent on the old location to continue uninterrupted until you can update those operations to reflect the new location. Users can continue to log in to the network and find objects in the original directory location.

   ---

5. A confirmation message appears indicating the move partition operation was successful.

Figure 14-4 Moving a Partition



Name: *

Type: Partition

Context: ed920

Search

☐	Name	Type	Context
☐	ed920	Tree Root	-
☐	microfocus	Organization	ed920
☐	novell	Organization	ed920
☐	Human Resources	Organizational Unit	ed920/dc=blr_domain
☐	IAM	Organizational Unit	ed920/o=microfocus
☐	IDM	Organizational Unit	ed920/o=microfocus/ou=IAM
☐	IDS	Organizational Unit	ed920/o=microfocus/ou=PSM
☐	Finance	Organizational Unit	ed920/o=novell
☐	Human Resources	Organizational Unit	ed920/o=novell

Showing 1 ‹ › Go to page 2 GO Showing 10 per page

15

Managing Indexes

Index Manager is an attribute of the Server object that lets you manage database indexes. These indexes are used by eDirectory to significantly improve query performance.

NetIQ eDirectory ships with a set of indexes that provide basic query functionality. These default indexes are for the following attributes.

The following tasks can be performed using the Index module:

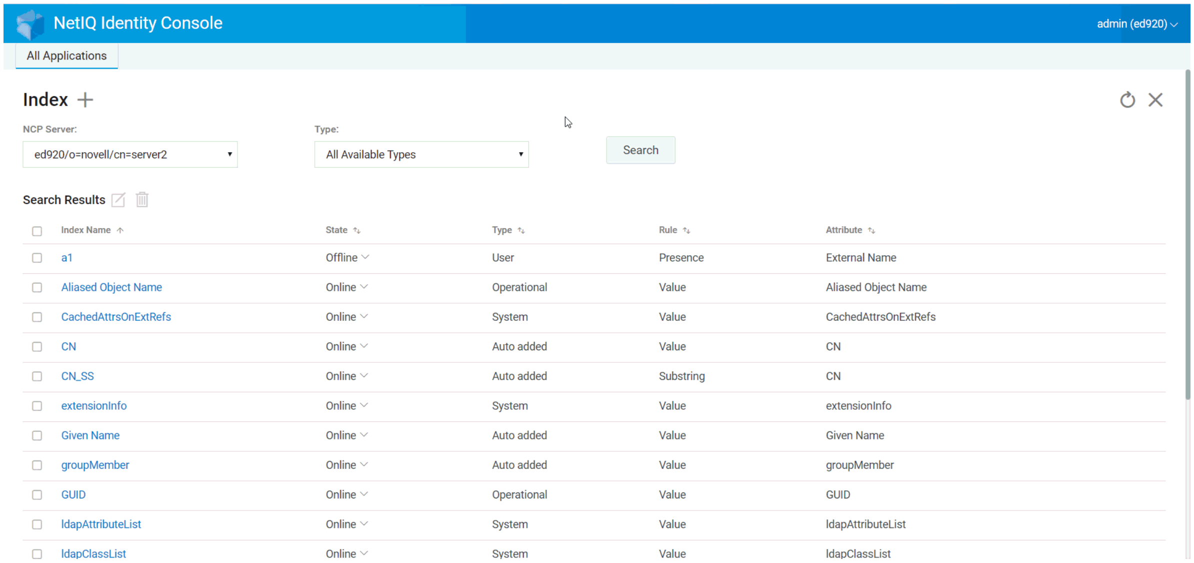
- "Creating Index" on page 79
- "Deleting an Index" on page 80
- "Copying an Index" on page 81
- "Changing State of an Index" on page 82

Creating Index

To create a new Index:

1. Click the **Index Management** option from the Identity Console landing page.
2. Click the + icon.
3. Enter the Index Name.
4. Select the server(s) from the list of available NCP servers.
5. Select the required attribute(s).
6. Select the index rule:
    - 6a **Substring:** This matches a subset of the attribute value string. For example, a query to find a LastName with "der" would return matches for Derington, Anderson, and Lauder. A substring index is the most resource-intensive index to create and maintain.
    - 6b **Presence:** This requires only the presence of an attribute rather than specific attribute values. A query to find all entries with a Login Script attribute would use a presence index.
    - 6c **Value:** This matches the entire value or the first part of the value of an attribute. For example, value matching could be used to find entries with a LastName that is equal to "Jensen" and entries with a LastName that begins with "Jen."
7. Click the Create button.
8. A confirmation appears indicating the index has been created.

Figure 15-1   Creating a New Index



NCP Server: ed920/o=novell/cn=server2

Type: All Available Types

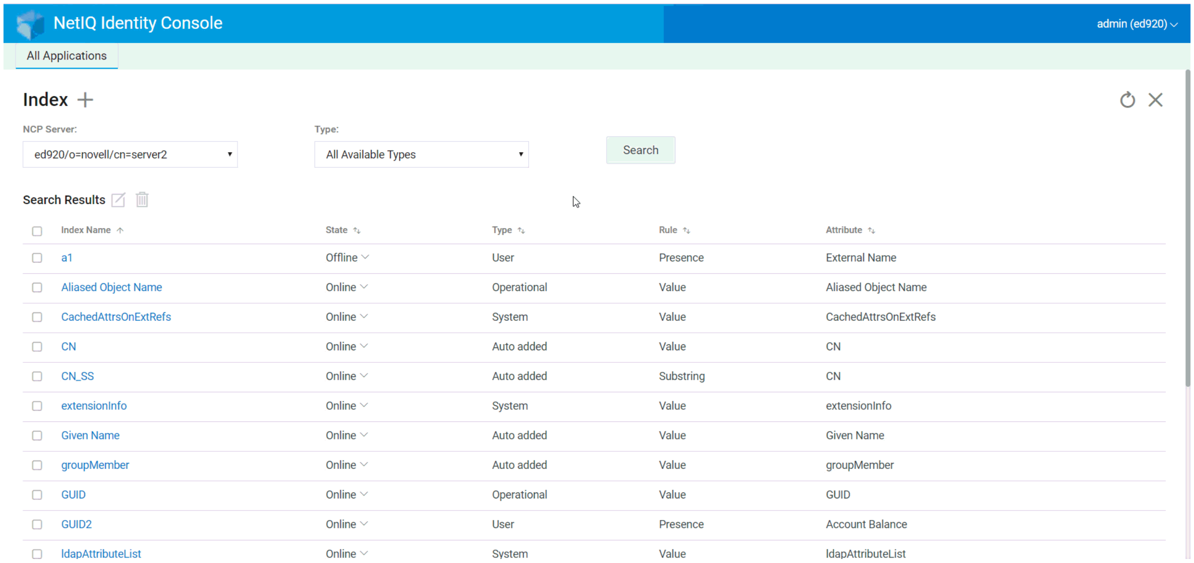
☐	Index Name	State	Type	Rule	Attribute
☐	a1	Offline	User	Presence	External Name
☐	Aliased Object Name	Online	Operational	Value	Aliased Object Name
☐	CachedAttrsOnExtRefs	Online	System	Value	CachedAttrsOnExtRefs
☐	CN	Online	Auto added	Value	CN
☐	CN_SS	Online	Auto added	Substring	CN
☐	extensionInfo	Online	System	Value	extensionInfo
☐	Given Name	Online	Auto added	Value	Given Name
☐	groupMember	Online	Auto added	Value	groupMember
☐	GUID	Online	Operational	Value	GUID
☐	ldapAttributeList	Online	System	Value	ldapAttributeList
☐	ldapClassList	Online	System	Value	ldapClassList

Deleting an Index

To delete an Index:

1. Click the **Index Management** option from the Identity Console landing page.
2. Select the NCP server and type of the Index, then click the Search button.
3. Select the Index from the search list and click the 🗑 icon.
4. A confirmation appears indicating the Index has been deleted.

Figure 15-2   Deleting an Index



NCP Server: ed920/o=novell/cn=server2

Type: All Available Types

☐	Index Name	State	Type	Rule	Attribute
☐	a1	Offline	User	Presence	External Name
☐	Aliased Object Name	Online	Operational	Value	Aliased Object Name
☐	CachedAttrsOnExtRefs	Online	System	Value	CachedAttrsOnExtRefs
☐	CN	Online	Auto added	Value	CN
☐	CN_SS	Online	Auto added	Substring	CN
☐	extensionInfo	Online	System	Value	extensionInfo
☐	Given Name	Online	Auto added	Value	Given Name
☐	groupMember	Online	Auto added	Value	groupMember
☐	GUID	Online	Operational	Value	GUID
☐	GUID2	Online	User	Presence	Account Balance
☐	ldapAttributeList	Online	System	Value	ldapAttributeList

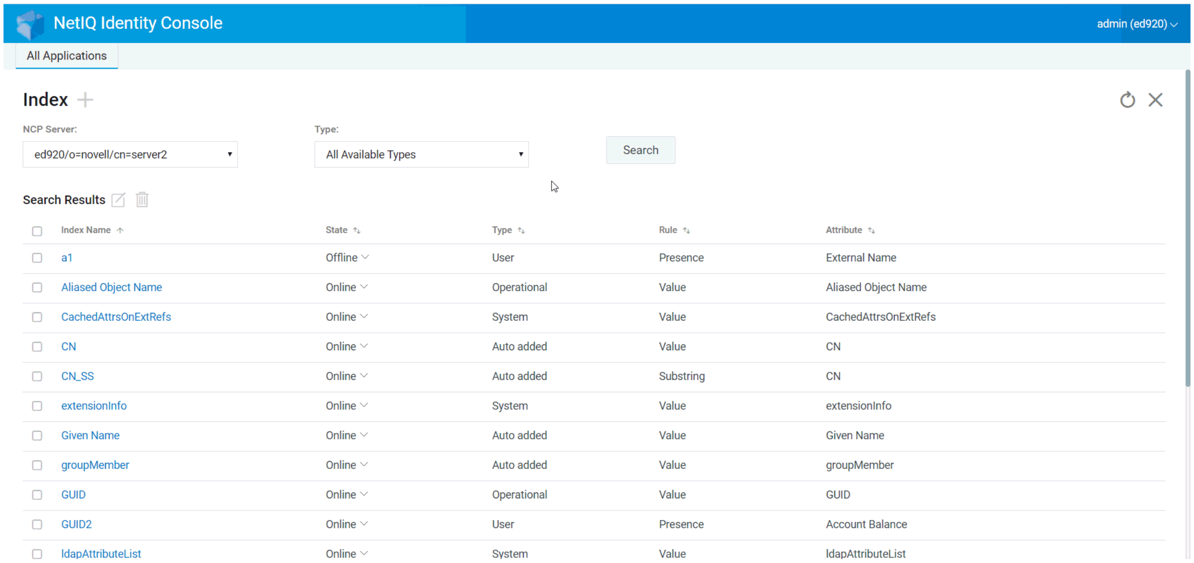
Copying an Index

If you've found a particular index to be useful on one server and you see the need for this index on another server, you can copy the index definition from one server to another. In reviewing predicate data, you might also find just the opposite case: an index that was meeting a need for several servers is no longer useful on one of these servers. In that case, you could delete the index from the single server that isn't benefiting from the index.

To copy an Index:

1. Click the **Index Management** option from the Identity Console landing page.
2. Select the NCP server and type of the Index, then click the Search button.
3. Select the Index from the search list and click on the ✎ icon.
4. Select the desired NCP server(s) where you want to copy the Index and click the Save button.
5. A confirmation appears indicating the Index has been modified.

Figure 15-3 Copying an Index



NCP Server: ed920/o=novell/cn=server2

Type: All Available Types

Search Results

☐	Index Name	State	Type	Rule	Attribute
☐	a1	Offline	User	Presence	External Name
☐	Aliased Object Name	Online	Operational	Value	Aliased Object Name
☐	CachedAttrsOnExtRefs	Online	System	Value	CachedAttrsOnExtRefs
☐	CN	Online	Auto added	Value	CN
☐	CN_SS	Online	Auto added	Substring	CN
☐	extensionInfo	Online	System	Value	extensionInfo
☐	Given Name	Online	Auto added	Value	Given Name
☐	groupMember	Online	Auto added	Value	groupMember
☐	GUID	Online	Operational	Value	GUID
☐	GUID2	Online	User	Presence	Account Balance
☐	ldapAttributeList	Online	System	Value	ldapAttributeList

Changing State of an Index

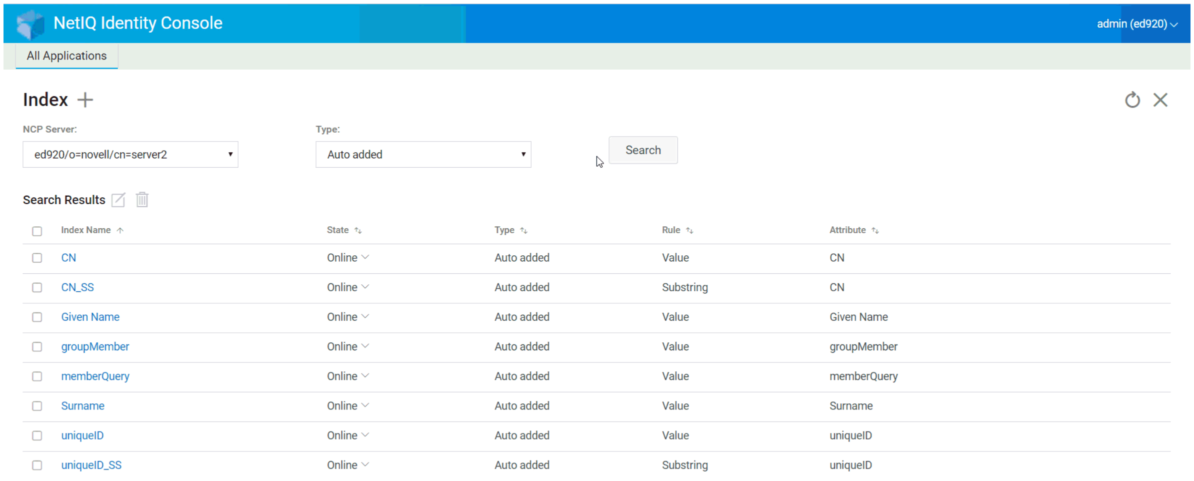
During peak times you might want to tune performance by temporarily taking indexes offline. For example, to achieve additional bulk-load speed, you might want to suspend all of the user-defined indexes. Because each object addition or modification requires updating defined indexes, having all indexes active might slow down bulk-loading of data. After the bulk-load is completed, the indexes can be brought online again.

To make an Index offline:

1. Click the **Index Management** option from the Identity Console landing page.
2. Select the NCP server and type of the Index, then click the Search button.
3. Click the drop-down list for **State** from the list of indexes. An index can have the following states:
   - **Online:** Currently running
   - **Offline:** Suspended. The index can be started again.

NOTE: The state of System and Operational type Indexes can not be changed. Such Indexes cannot be deleted as well.

Figure 15-4 Taking an Index Offline



NCP Server: ed920/o=novell/cn=server2

Type: Auto added

Search Results

☐	Index Name	State	Type	Rule	Attribute
☐	CN	Online	Auto added	Value	CN
☐	CN_SS	Online	Auto added	Substring	CN
☐	Given Name	Online	Auto added	Value	Given Name
☐	groupMember	Online	Auto added	Value	groupMember
☐	memberQuery	Online	Auto added	Value	memberQuery
☐	Surname	Online	Auto added	Value	Surname
☐	uniqueID	Online	Auto added	Value	uniqueID
☐	uniqueID_SS	Online	Auto added	Substring	uniqueID

16 Configuring LDAP Objects

An eDirectory installation creates an LDAP server object and an LDAP Group object. The default configuration for LDAP Services is located in the directory on these two objects. You can modify the default configuration by using the LDAP Management task in Identity Console.

The LDAP server object represents server-specific configuration data. However, the LDAP Group object contains configuration information that can be conveniently shared among multiple LDAP servers. This object provides common configuration data and represents a group of LDAP servers. The servers have common data.

You can associate multiple LDAP server objects with one LDAP Group object. All the associated LDAP servers then get their server-specific configuration from their LDAP server object but get common or shared information from the LDAP Group object.

The following tasks can be performed using the LDAP module:

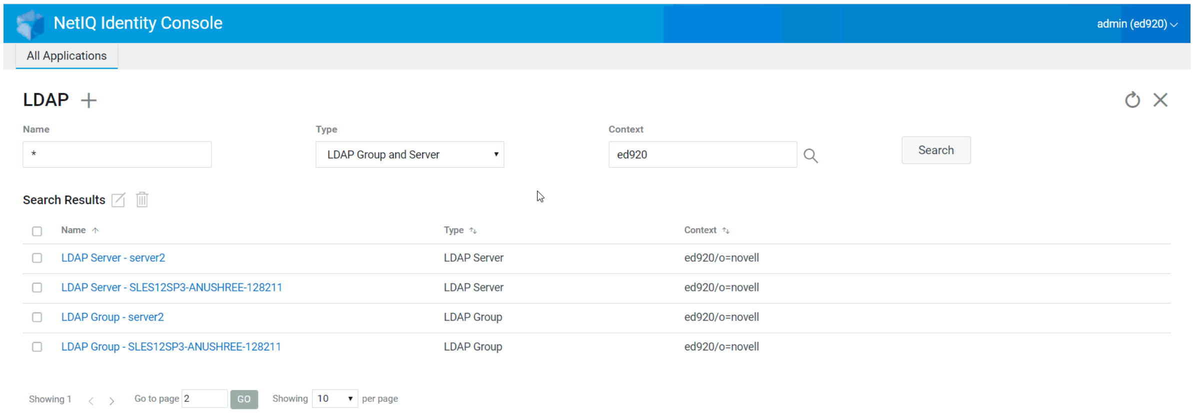
- "Creating LDAP Objects" on page 83
- "Deleting LDAP Objects" on page 84
- "Modifying LDAP Objects" on page 85

Creating LDAP Objects

To create a new LDAP object:

1. Click the **LDAP Configuration** option from the Identity Console landing page.
2. Click the + icon.
3. In the Create LDAP Object page, specify the name, type and context, or use the Search Context 🔍 icon to locate it, then click **Create**.
4. A confirmation appears indicating the LDAP object has been created.

Figure 16-1 Creating a New LDAP Object



Name: *
Type: LDAP Group and Server
Context: ed920

Search Results

☐	Name	Type	Context
☐	LDAP Server - server2	LDAP Server	ed920/o=novell
☐	LDAP Server - SLES12SP3-ANUSHREE-128211	LDAP Server	ed920/o=novell
☐	LDAP Group - server2	LDAP Group	ed920/o=novell
☐	LDAP Group - SLES12SP3-ANUSHREE-128211	LDAP Group	ed920/o=novell

Showing 1 Go to page 2 GO Showing 10 per page

Deleting LDAP Objects

To delete LDAP objects:

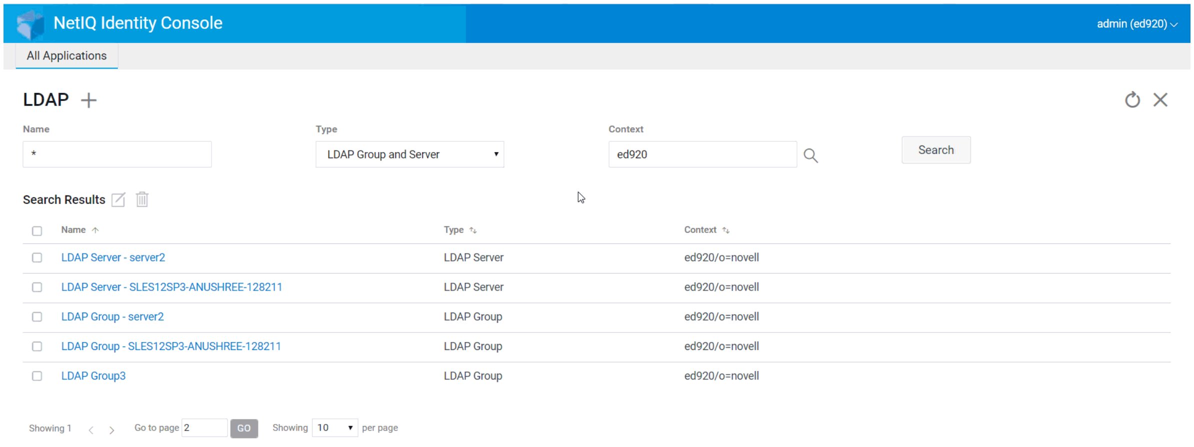
1 Click the **LDAP Configuration** option from the Identity Console landing page.

2 Specify the name, type and context of the LDAP object, then click the Search button.

3 Select the LDAP object(s) from the search list and click the 🗑 icon.

4 A confirmation appears indicating the LDAP object(s) has been deleted.

Figure 16-2 Deleting LDAP Objects



Name: *
Type: LDAP Group and Server
Context: ed920

Search Results

☐	Name	Type	Context
☐	LDAP Server - server2	LDAP Server	ed920/o=novell
☐	LDAP Server - SLES12SP3-ANUSHREE-128211	LDAP Server	ed920/o=novell
☐	LDAP Group - server2	LDAP Group	ed920/o=novell
☐	LDAP Group - SLES12SP3-ANUSHREE-128211	LDAP Group	ed920/o=novell
☐	LDAP Group3	LDAP Group	ed920/o=novell

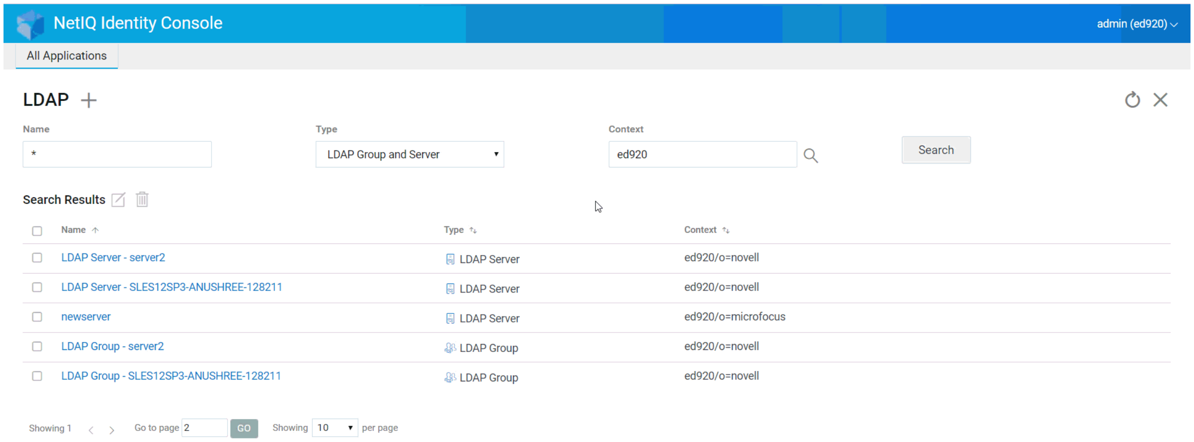
Showing 1 Go to page 2 GO Showing 10 per page

Modifying LDAP Objects

To modify LDAP objects:

1. Click the **LDAP Configuration** option from the Identity Console landing page.
2. Type the name, type and context of the LDAP object, then click the Search button.
3. Select the LDAP object from the search list and click the ✎ icon.
4. Modify the attributes and information for the specific LDAP object as required and click the Save button. For more information about the attributes for LDAP objects, see Configuring LDAP Server and LDAP Group Objects on Linux in the *NetIQ eDirectory Administration Guide*.
5. A confirmation appears indicating the LDAP object has been modified.

Figure 16-3 *Modifying LDAP objects*



Name: *

Type: LDAP Group and Server

Context: ed920

☐	Name	Type	Context
☐	LDAP Server - server2	LDAP Server	ed920/o=novell
☐	LDAP Server - SLES12SP3-ANUSHREE-128211	LDAP Server	ed920/o=novell
☐	newserver	LDAP Server	ed920/o=microfocus
☐	LDAP Group - server2	LDAP Group	ed920/o=novell
☐	LDAP Group - SLES12SP3-ANUSHREE-128211	LDAP Group	ed920/o=novell

Showing 1 ‹ › Go to page 2 GO Showing 10 per page

17 Managing Certificates

NetIQ Certificate Server is automatically installed when you install eDirectory. Certificate Server provides public key cryptography services that are natively integrated into eDirectory and that allow you to mint, issue, and manage both user and server certificates. These services allow you to protect confidential data transmissions over public communications channels such as the Internet.

NOTE: If you want to use the Certificate Management module with Identity Console, you must upgrade your eDirectory server to 9.2.4 HF2.

Identity Console provides the following certificate management tasks:

- "Managing Certificate Authority" on page 87
- "Managing Server Certificates" on page 91
- "Managing User Certificates" on page 94
- "Managing Trusted Root and Containers" on page 96
- "Creating Default Server Certificate Objects" on page 98
- "Issuing a Public Key Certificate" on page 100
- "Managing SAS Service Object" on page 103

Managing Certificate Authority

By default, the NetIQ Certificate Server installation process creates the Organizational Certificate Authority (CA) for you. You are prompted to specify an Organizational CA name. When you click Finish, the Organizational CA is created with the default parameters and placed in the Security container.

If you want more control over the creation of the Organizational CA, you can create the Organizational CA manually by using Identity Console portal. Also, if you delete the Organizational CA, you need to re-create it.

Using the Certificate Authority Module, you can perform the following tasks:

- "Creating an Organizational CA Certificates" on page 88
- "Backing Up Organizational CA Certificates" on page 88
- "Restoring an Organizational CA" on page 89
- "Validating the Organizational CA's Certificates" on page 89
- "Replacing the Organizational CA's Certificates" on page 90
- "Revoking the Organizational CA's Certificates" on page 90

Creating an Organizational CA Certificates

To create an Organizational CA object, perform the following steps:

1. Click **Certificate Management** > **CA Management** options from the Identity Console landing page.
2. If no Organizational Certificate Authority object exists, this opens the Create an Organizational Certificate Authority Object dialog box and the corresponding wizard that creates the object. Follow the prompts to create the object.

   NOTE: Ensure that the CRL file path which is specified here, is in respect with the eDirectory installation path.

3. After you have finished creating the Certificate Authority, we recommend that you make a backup of the CA’s public/private key pair and store this in a safe and secure place. For more information, see “Backing Up Organizational CA Certificates” on page 88.

Backing Up Organizational CA Certificates

We recommend that you back up your Organizational CA's private key and certificates in case the Organizational CA's host server has an unrecoverable failure. If a failure should occur, you can use the backup file to restore your Organizational CA to any server in the tree.

NOTE: The ability to back up an Organizational CA is available only for Organizational CAs created with Certificate Server version 9.0 at a minimum. In previous versions of Certificate Server, the Organizational CA's private key was created in a way that made exporting it impossible.

The backup file contains the CA's private key, self-signed certificate, public key certificate, and several other certificates necessary for it to operate. This information is stored in PKCS #12 format (also known as PFX).

The Organizational CA should be backed up when it is working properly.

To back up the Organizational CA, perform the following steps:

1. Click **Certificate Management** > **CA Management** options from the Identity Console landing page.
2. Click **Certificates** tab.
3. Select either the **Self Signed Certificate** or the **Public Key Certificate**. Both certificates are written to the file during the backup operation. We recommend that you select the Self Signed Certificate for RSA and ECDSA certificates separately.
4. Click the 📤 icon.
5. Choose to export the private key, specify a password with 6 or more alphanumeric characters to use in encrypting the PFX file and select PKCS12 as export format, then click **OK**.
6. The encrypted backup file is written to the location specified. It is now ready to be stored in a secure location for emergency use.

Restoring an Organizational CA

If the Organizational CA object has been deleted or corrupted, or if the Organizational CA’s host server has suffered an unrecoverable failure, the Organizational CA can be restored to full operation through using a backup file created as described in “Backing Up Organizational CA Certificates” on page 88.

To restore the Organizational CA, perform the following steps:

1. Click **Certificate Management** > **CA Management** options from the Identity Console landing page.
2. Click the ↑↓ at the top of the screen (next to **Certificate Authority Management**) to delete the existing Organizational CA.
3. You will now be prompted to configure a new Organizational CA. This opens the Create an Organizational Certificate Authority Object dialog box and the corresponding wizard that creates the object.
4. In the creation dialog box, specify the server that should host the Organizational CA and the name of the Organizational CA object.
5. Select **Import**.
6. Select both RSA and ECDSA certificates. The Certificate Server requires that both certificates have the same subject name. However, the Certificate Server does not support importing external self-signed CA certificates. However, it allows you to import subordinate CA certificates.
7. In the subsequent screens, browse and select the name of the file for RSA and ECDSA.
8. Enter the password used to encrypt the file when the backup was made and click **OK**.
9. The Organizational CA’s private key and certificates have now been restored and the CA is fully functional. The file can now be stored again for future use.

Validating the Organizational CA's Certificates

If you suspect a problem with a certificate or think that it might no longer be valid, you can easily validate the certificate by using Identity Console. Any certificate in the eDirectory tree can be validated, including certificates issued by external CAs.

The certificate validation process includes several checks of the data in the certificate as well as the data in the certificate chain. A certificate chain is composed of a root CA certificate and, optionally, the certificates of one or more intermediate CAs.

To validate a certificate:

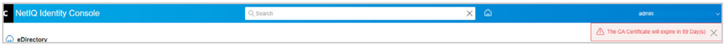
1. Click **Certificate Management** > **CA Management** options from the Identity Console landing page.
2. Click **Certificates** tab.
3. Select either the **Self Signed Certificate** or the **Public Key Certificate**.
4. Click the ✓ to validate the selected CA certificates.

Replacing the Organizational CA’s Certificates

If the certificates become corrupt or invalid for some reason, or if you just want to replace the existing certificates, perform the following steps:

1. Click **Certificate Management** > **CA Management** options from the Identity Console landing page.
2. Click **Certificates** tab.
3. Select either the **Self Signed Certificate** or the **Public Key Certificate**.
4. Click the ↑↓ to replace the selected CA certificate.
5. Import a CA certificate in `.pfx` or `.p12` format and specify a password to encrypt the private key.
6. Click **OK**.

NOTE: Identity Console starts alerting you of the CA certificate expiry 60 days prior to the expiry due date. This message gets displayed once you login to Identity Console.



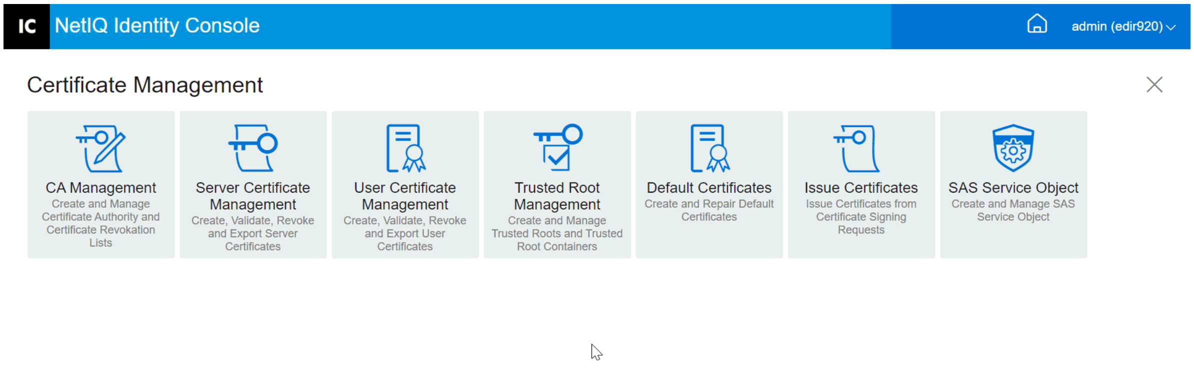
The CA Certificate will expire in 59 Day(s)

Revoking the Organizational CA’s Certificates

To revoke a certificate:

1. Click **Certificate Management** > **CA Management** options from the Identity Console landing page.
2. Click **Certificates** tab.
3. Select either the **Self Signed Certificate** or the **Public Key Certificate**.
4. Click the ⊘ icon.
5. Read and understand the risk involved with revoking server certificates.
6. Select a valid reason for revocation from the drop-down list, select the invalidity date and specify any other comment.
7. Click **OK** to finish the revocation.

Figure 17-1 Managing Certificate Authority


IC NetIQ Identity Console
admin (edir920)
Certificate Management
CA Management
Create and Manage Certificate Authority and Certificate Revokation Lists
Server Certificate Management
Create, Validate, Revoke and Export Server Certificates
User Certificate Management
Create, Validate, Revoke and Export User Certificates
Trusted Root Management
Create and Manage Trusted Roots and Trusted Root Containers
Default Certificates
Create and Repair Default Certificates
Issue Certificates
Issue Certificates from Certificate Signing Requests
SAS Service Object
Create and Manage SAS Service Object

Managing Server Certificates

Using the Server Certificate Management module, the administrator can perform the following tasks:

- "Creating Server Certificate Objects" on page 91
- "Exporting Server Certificate Objects" on page 92
- "Validating Server Certificate Objects" on page 92
- "Replacing a Server Certificate Object" on page 92
- "Revoking Server Certificate Objects" on page 93
- "Deleting Server Certificate Objects" on page 93

Creating Server Certificate Objects

To create a server certificate object, perform the following steps:

1 Click **Certificate Management** > **Server Certificate Management** options from the Identity Console landing page.

2 Click the + icon.

3 In the **Create Server Certificate** page, specify a **Nickename**, server and select anyone of the following options:

   - **Standard (Default Parameters):** Allows you to create a default server certificate object of type RSA or ECDSA.
   - **Custom (User Specified Parameters):** Allows you to specify the custom parameters for the server certificate object.
   - **Import (Allows to Import a PKCS12 File):** Allows you to import a `PKCS12` file in `.pfx` or `.p12` format.

4 After specifying the parameters, click **Next** to review the summary of the certificate.

5 In the **Summary** screen, click **OK** to create a server certificate object.

Exporting Server Certificate Objects

To export server certificate objects, perform the following steps:

1 Click **Certificate Management** > **Server Certificate Management** options from the Identity Console landing page.

2 Select the appropriate server from the drop-down list.

3 Select the appropriate server certificate from the list and click the 📄 icon.

4 In the next screen, select check box for **Export Private key** and specify a password to protect the private key. Confirm the password and select the export format.

NOTE: Server certificates can be exported in `PKCS12` format only.

5 Click **OK** to export the server certificate object.

Validating Server Certificate Objects

To validate a server certificate object, perform the following steps:

1 Click **Certificate Management** > **Server Certificate Management** options from the Identity Console landing page.

2 Select the appropriate server from the drop-down list.

3 Select the appropriate server certificate from the list and click the ✓ icon.

4 A confirmation appears indicating a successful validation of the server certificate object.

Replacing a Server Certificate Object

If the server certificates become corrupt or invalid for some reason, or if you just want to replace the existing default certificates, perform the following steps:

1 Click **Certificate Management** > **Server Certificate Management** options from the Identity Console landing page.

2 Select the appropriate server from the drop-down list.

3 Select the appropriate server certificate from the list and click the ⇅ icon.

4 Read and understand the risk involved with replacing server certificates and click **OK**.

5 In the next screen, browse and select the new server certificate in `.pfx` or `.p12` format and specify a password.

6 Click **OK** to replace the server certificate.

Revoking Server Certificate Objects

To revoke a server certificate object, perform the following steps:

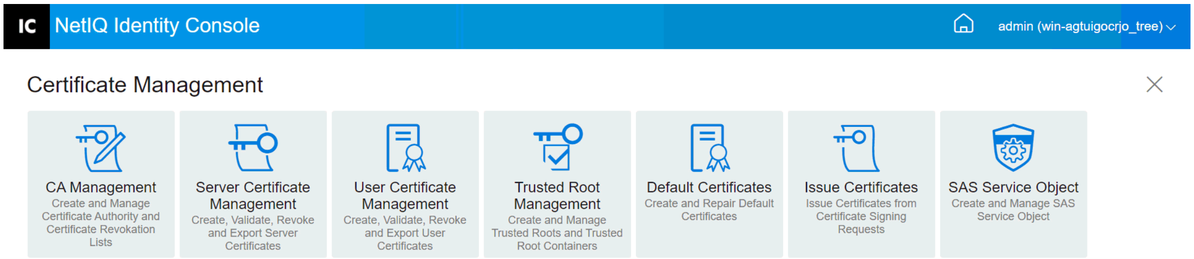
1. Click **Certificate Management** > **Server Certificate Management** options from the Identity Console landing page.
2. Select the appropriate server from the drop-down list.
3. Select the appropriate server certificate from the list and click the ⊘ icon.
4. Read and understand the risk involved with revoking server certificates and click **OK**.
5. In the next screen, select a valid reason for revocation from the drop-down list, select the invalidity date and specify any other comment.
6. Click **OK** to finish the revocation.

Deleting Server Certificate Objects

To remove server certificate objects, perform the following steps:

1. Click **Certificate Management** > **Server Certificate Management** options from the Identity Console landing page.
2. Select the appropriate server from the drop-down list.
3. Select the appropriate server certificate from the list and click the 🗑 icon.
4. In the next screen, click **OK**.
5. A confirmation appears indicating a successful deletion of the server certificate object.

Figure 17-2 *Managing Server Certificates*


IC
NetIQ Identity Console
admin (win-agtuigocrjo_tree)
Certificate Management
CA Management
Create and Manage Certificate Authority and Certificate Revokation Lists
Server Certificate Management
Create, Validate, Revoke and Export Server Certificates
User Certificate Management
Create, Validate, Revoke and Export User Certificates
Trusted Root Management
Create and Manage Trusted Roots and Trusted Root Containers
Default Certificates
Create and Repair Default Certificates
Issue Certificates
Issue Certificates from Certificate Signing Requests
SAS Service Object
Create and Manage SAS Service Object

Managing User Certificates

Using the User Certificate Management module, you can perform the following task:

- "Creating User Certificate Objects" on page 94
- "Exporting User Certificate Objects" on page 94
- "Validating User Certificate Objects" on page 95
- "Revoking User Certificate Objects" on page 95
- "Deleting User Certificate Objects" on page 95

Creating User Certificate Objects

To create a user certificate object, perform the following steps:

1. Click **Certificate Management** > **User Certificate Management** options from the Identity Console landing page.
2. Click the + icon.
3. In the **Create User Certificate** page, specify a **Nickename**, server and select anyone of the following options:
    - **Standard (Default Parameters):** Allows you to create a default user certificate object of type RSA or ECDSA.
    - **Custom (User Specified Parameters):** Allows you to specify the custom parameters for the user certificate object.
    - **Import:** Allows you to import a certificate file in `CERT` or `PKCS12` format.
4. After specifying the parameters, click **Next** to review the summary of the certificate.
5. In the **Summary** screen, click **OK** to create a user certificate object.

Exporting User Certificate Objects

To export user certificate objects, perform the following steps:

1. Click **Certificate Management** > **User Certificate Management** options from the Identity Console landing page.
2. Select the appropriate server from the drop-down list.
3. Select the appropriate user certificate from the list and click the 📤 icon.
4. In the next screen, select check box for **Export Private key** and specify a password to protect the private key. Confirm the password and select the export format.

    NOTE: User certificates can be exported in `PKCS12` format only.

5. Click **OK** to export the user certificate object.

Validating User Certificate Objects

To validate a user certificate object, perform the following steps:

1. Click **Certificate Management** > **User Certificate Management** options from the Identity Console landing page.
2. Select the appropriate server from the drop-down list.
3. Select the appropriate user certificate from the list and click the ✓ icon.
4. A confirmation appears indicating a successful validation of the user certificate object.

Revoking User Certificate Objects

To revoke a user certificate object, perform the following steps:

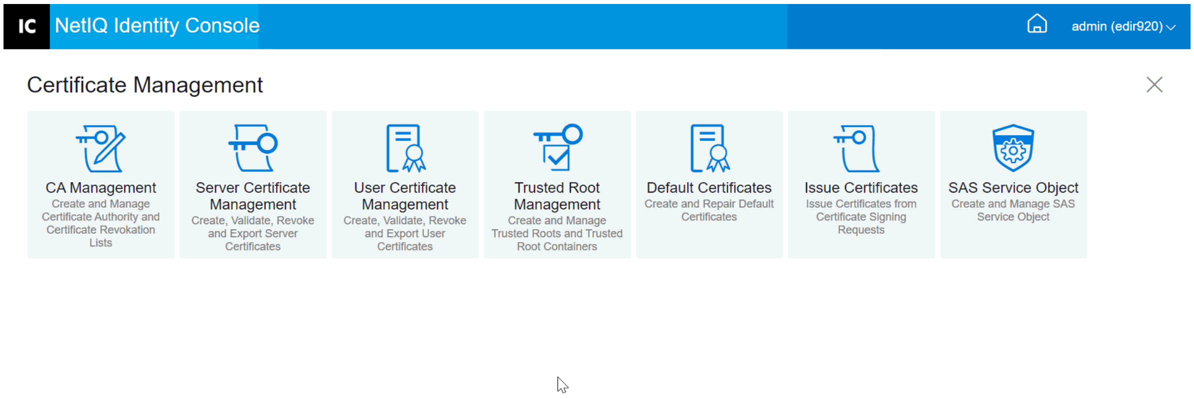
1. Click **Certificate Management** > **User Certificate Management** options from the Identity Console landing page.
2. Select the appropriate server from the drop-down list.
3. Select the appropriate user certificate from the list and click the ⊘ icon.
4. Read and understand the risk involved with revoking user certificates.
5. Select a valid reason for revocation from the drop-down list, select the invalidity date and specify any other comment.
6. Click **OK** to finish the revocation.

Deleting User Certificate Objects

To remove user certificate objects, perform the following steps:

1. Click **Certificate Management** > **User Certificate Management** options from the Identity Console landing page.
2. Select the appropriate server from the drop-down list.
3. Select the appropriate user certificate from the list and click the 🗑 icon.
4. In the next screen, click **OK**.
5. A confirmation appears indicating a successful deletion of the user certificate object.

Figure 17-3 Managing User Certificates


IC
NetIQ Identity Console
admin (edir920)
Certificate Management
CA Management
Create and Manage Certificate Authority and Certificate Revokation Lists
Server Certificate Management
Create, Validate, Revoke and Export Server Certificates
User Certificate Management
Create, Validate, Revoke and Export User Certificates
Trusted Root Management
Create and Manage Trusted Roots and Trusted Root Containers
Default Certificates
Create and Repair Default Certificates
Issue Certificates
Issue Certificates from Certificate Signing Requests
SAS Service Object
Create and Manage SAS Service Object

Managing Trusted Root and Containers

A trusted root provides the basis for trust in public key cryptography. Trusted roots are used to validate certificates signed by other CAs. Trusted roots enable security for SSL, secure e-mail, and certificate-based authentication.

Using the Trusted Root Management module, you can perform the following tasks:

- "Creating a Trusted Root Container" on page 96
- "Creating a Trusted Root Certificate Object" on page 97
- "Exporting Trusted Root Certificate Objects" on page 97
- "Validating Trusted Root Certificate Objects" on page 97
- "Deleting Trusted Root Certificate Objects" on page 98
- "Deleting Trusted Root Containers" on page 98

Creating a Trusted Root Container

To create a trusted root container, perform the following tasks:

1. Click **Certificate Management** > **Trusted Root Management** options from the Identity Console landing page. The **Trusted Root Container** check box will be selected by default.
2. Click the + icon to create a new trusted root container.
3. Specify a name for the trusted root container.
4. Use the object selector to browse for the appropriate container.
5. Click the **OK** button.
6. A confirmation appears indicating that the trusted root container has been created successfully.

Creating a Trusted Root Certificate Object

To create a trusted root object, perform the following steps:

1. Click **Certificate Management** > **Trusted Root Management** options from the Identity Console landing page. The **Trusted Root Container** check box will be selected by default. Select the **Trusted Root** check box.
2. Click the + icon to create a new trusted root object.
3. Specify a name for the trusted root object.
4. Select the appropriate trusted root container from the drop-down list.
5. Browse and select the appropriate certificate file in `.der` or `.b64` format.

   NOTE: Any type of certificate can be stored in a Trusted Root object (CA certificates, intermediate CA certificates, or user certificates).

   ---

6. Click the **OK** button.
7. A confirmation appears indicating that the trusted root object has been created successfully.

Exporting Trusted Root Certificate Objects

To export trusted root certificate objects, perform the following steps:

1. Click **Certificate Management** > **Trusted Root Management** options from the Identity Console landing page. The **Trusted Root Container** check box will be selected by default. Select the **Trusted Root** check box.
2. Select the appropriate trusted root certificate from the list and click the icon.
3. In the next screen, select check box for **Export Private key** and specify a password to protect the private key. Confirm the password and select the export format.

   NOTE: Trusted root certificates can be exported in `DER` or in `BASE64` formats only.

   ---

4. Click **OK** to export the trusted root certificate object.

Validating Trusted Root Certificate Objects

To validate trusted root certificate objects, perform the following steps:

1. Click **Certificate Management** > **Trusted Root Management** options from the Identity Console landing page. The **Trusted Root Container** check box will be selected by default. Select the **Trusted Root** check box.
2. Select the appropriate trusted root certificate from the list and click the ✓ icon.
3. A confirmation appears indicating a successful validation of the trusted root certificate object.

Deleting Trusted Root Certificate Objects

To remove trusted root certificate objects, perform the following steps:

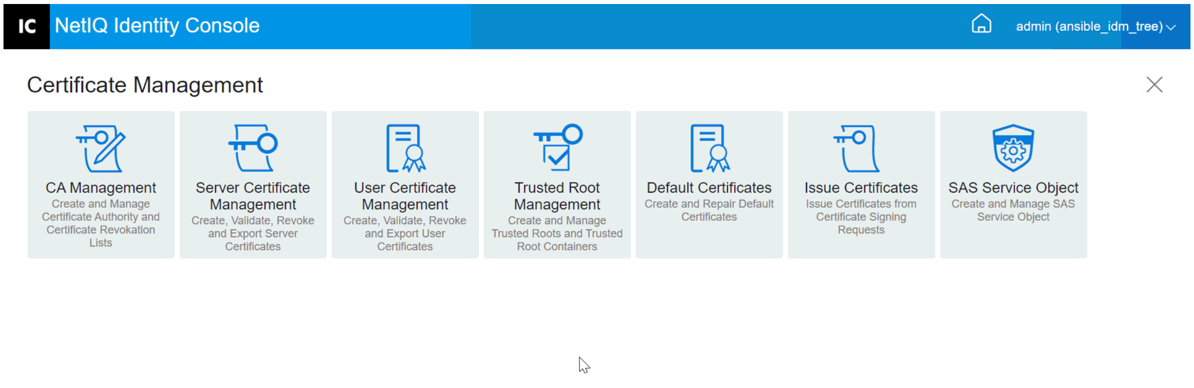
1. Click **Certificate Management** > **Trusted Root Management** options from the Identity Console landing page. The **Trusted Root Container** check box will be selected by default. Select the **Trusted Root** check box.
2. Select the appropriate trusted root certificate from the list and click the 🗑 icon.
3. Click **OK** on the warning screen.
4. A confirmation appears indicating a successful removal of the trusted root certificate object.

Deleting Trusted Root Containers

To remove a trusted root container, perform the following steps:

1. Click **Certificate Management** > **Trusted Root Management** options from the Identity Console landing page. The **Trusted Root Container** check box will be selected by default.
2. Select the appropriate trusted root container from the list and click the 🗑 icon.
3. Click **OK** on the warning screen.
4. A confirmation appears indicating a successful removal of the trusted root container.

Figure 17-4 *Managing Trusted Root Containers*


IC
NetIQ Identity Console
admin (ansible_idm_tree)
Certificate Management
CA Management
Create and Manage Certificate Authority and Certificate Revokation Lists
Server Certificate Management
Create, Validate, Revoke and Export Server Certificates
User Certificate Management
Create, Validate, Revoke and Export User Certificates
Trusted Root Management
Create and Manage Trusted Roots and Trusted Root Containers
Default Certificates
Create and Repair Default Certificates
Issue Certificates
Issue Certificates from Certificate Signing Requests
SAS Service Object
Create and Manage SAS Service Object

Creating Default Server Certificate Objects

The Certificate Server installation creates default Server Certificate objects.

- SSL CertificateDNS - *server_name*

- A certificate for each IP address configured on the server (IPAG*xxx.xxx.xxx.xxx* - *server_name*)
- A certificate for each DNS name configured on the server (DNSAG*www.example.com* - *server_name*)

NOTE: eDirectory does not automatically create SSL CertificateIP. SSL Certificate DNS contains all the IPs listed in the Subject Alternative Name. When you attempt to create or repair the default certificates using Identity Console, the SSL CertificateIP certificate is not created or repaired by default. However, the plug-in interface provides a check box that you can select to override the default behavior and force the creation/repair of the SSL CertificateIP certificate.

eDirectory 9.0 and above automatically creates ECDSA certificates if Organization CA has a ECDSA certificate.

If these certificates become corrupt or invalid for some reason, or if you just want to replace the existing default certificates, you can use the Create Default Server Certificates Wizard, as described in the following procedure:

1. Click **Certificate Management** > **Default Certificates** options from the Identity Console landing page.
2. Select the server or servers that you want to create default certificates for, then

   click **Next**.
3. Select Yes if you want to overwrite the existing default server certificates or select No if you want

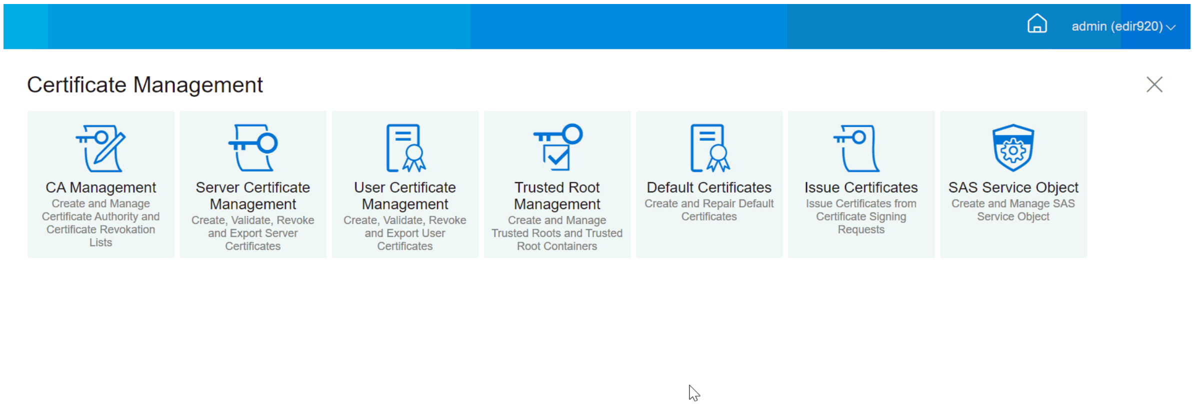
   to overwrite the existing default server certificates only if they are invalid.
4. (Single Server only) If you want to use the existing DNS address, select that option. If you want

   to use a different DNS address, select that option and specify the new DNS address.
5. (Single Server only) If you want to use the existing default IP address, select that option. If you

   want to use a different IP address, select that option and specify the new IP address.
6. Click **Next**.
7. Review the summary page, then click **Finish**.

If you want more control over the creation of the Server Certificate object, you can create the Server Certificate object manually. For more information, see "Creating Server Certificate Objects" on page 91.

Figure 17-5 *Creating Default Server Certificate Objects*


admin (edir920)
Certificate Management
CA Management
Create and Manage Certificate Authority and Certificate Revokation Lists
Server Certificate Management
Create, Validate, Revoke and Export Server Certificates
User Certificate Management
Create, Validate, Revoke and Export User Certificates
Trusted Root Management
Create and Manage Trusted Roots and Trusted Root Containers
Default Certificates
Create and Repair Default Certificates
Issue Certificates
Issue Certificates from Certificate Signing Requests
SAS Service Object
Create and Manage SAS Service Object

Issuing a Public Key Certificate

Your Organizational CA works the same way as an external CA. That means, it has the ability to issue certificates from certificate signing requests (CSRs). You can issue certificates using your Organizational CA when a user sends a CSR to you for signing. The user requesting the certificate can then take the issued certificate and import it directly into the cryptography-enabled application.

This task allows you to generate certificates for cryptography-enabled applications that do not recognize Server Certificate objects.

To issue a certificate, perform the following steps:

1. Click Certificate Management > Issue Certificates options from the Identity Console landing page.
2. Browse and select a CSR file.
3. Select the appropriate Key Type and the corresponding Key Usage under Key Usage Specifications. These options allow you to select a key type. Each key type has predefined key usage values associated with it:
   - 3a **Unspecified:** This option is selected by default does not activate any key usage in the certificate.
   - 3b **Certificate Authority:** This option activates the Certificate signing and CRL signing key usages.
   - 3c **Encryption:** This option activates the Key Encipherment key usage.
   - 3d **Signature:** This option activates the Digital Signature key usage.
   - 3e **SSL or TSL:** This option configures the key so that it can be used in SSL or TLS transactions.
   - 3f **Custom:** This option lets you select any or all of the key usage options manually.
   - 3g **Set the Key Usage Extension to Critical:** With any key type except Unspecified selected, you can mark the key usage extension as critical. Any extension that is critical must be understood by the receiving software before the certificate can be used for any purpose.

Therefore, marking an extension as critical does pose some risk, because not all applications can use the certificate. However, for well known extensions such as key usage, the risk is minimal. In general, if key usage is specified, the extension should be marked critical.

4 You can choose to encode an **Extended Key Usage** extension in the certificate. To activate this feature, select **Enable Extended Key Usage**:

- **4a** **Server:** This option activates the Server Authentication extended key usage.
- **4b** **User:** This option activates the User Authentication and E-mail Protection extended key usages.
- **4c** **Custom:** This option lets you select any or all Extended Key Usages.
- **4d** **Any:** Lets the key be used for any extended key usage.
- **4e** **Set the Extended Key Usage Extension to Critical:** Any extension that is critical must be understood by the receiving software before the certificate can be used for any purpose. Therefore, marking an extension as critical does pose some risk, because not all applications can use the certificate. As many applications do not understand the Extended Key Usage Extension, marking this extension as critical poses significant risk of the certificate not being accepted by a given application; therefore, it should only be set to critical when necessary.

5 Select the appropriate **Basic Constraints**:

- **5a** **Certificate Type:**
  - **5a1** **Unspecified:** Select this option if you do not want to add a basic constraint extension to the certificate.
  - **5a2** **Certificate Authority:** Select this option to add a Certificate Authority basic constraint extension to the certificate. If the certificate is for a Certificate Authority, you must select this option.
  - **5a3** **End Entity:** Select this option to add a basic constraint extension to the certificate that specifies this is an End Entity (that is not a Certificate Authority) certificate. Note: If a certificate is of type End Entity, the path length should be set to Unspecified.
- **5b** **Path Length:**
  - **5b1** **Unspecified:** Select this option if you don't want to specify how many levels of subordinate CAs can be created under this CA.

    NOTE: If a certificate is of type End Entity, the path length should only be set to Unspecified.

  - **5b2** **Specific:** Select this option if you want to specify how many levels of subordinate CAs can be created under this CA. Click the Up and Down-arrows to specify the path length.

> **NOTE:** If the certificate being created is a subordinate CA, the path length must be consistent with the superior CA. For example, if the superior CA has a path length of 3, the subordinate's path length must be 2 or less. If the superior CA has an unspecified path length, the subordinate may also have an unspecified path length or any specific path length desired.

5c **Set Basic Constraints Extension to Critical:** In general, the Basic Constraints Extension must be set to critical for CA certificates. Any extension that is critical must be understood by the receiving software before the certificate can be used for any purpose. Therefore, marking an extension as critical does pose some risk, because not all applications can use the certificate. However, for well known extensions such as Basic Constraints, the risk is minimal.

6 Specify the following certificate parameters:

6a **Subject Name:** Displays the fully typed name of your eDirectory tree.

6b **Subject Name:** Displays the fully typed name of your eDirectory tree.

6c **Validity Period:** Use the drop-down list to specify a period over which the certificate is to be valid. The range is from 6 months to the maximum, the year 2036 (a time limitation based on a 32-bit time value). If you select the Specify Dates option, you can edit the Effective Date and the Expiration Date fields to create a custom validity period. The maximum date selected must fall within the validity date of the CA.

6c1 **Effective Date:** Lets you display or edit the time and date when the certificate becomes valid.

6c2 **Expiration Date:** Lets you display or edit the time and date when the certificate becomes invalid.

6d **Custom Extensions:** Enables Certificate Server to support any standard or custom extensions that you want to include when creating a certificate. Extensions must have been previously created and stored in a file (one extension per file). Any extension must be ASN.1 encoded as defined in IETF RFC 2459/3280 section 4.2.

If you want to include one or more custom extensions in the certificate you are creating, click New and then browse for a file containing the custom extension and add it to the certificate. Multiple extensions can be added by repeating this process.

To delete a custom extentions file, select it and then click the 🗑 icon.

7 Select the appropriate certificate format from the following options:

7a **File in Binary DER Format:** This option lets you save or export a certificate to a file displayed in the Filename field. By default, the certificate file is exported with a `.DER` extension at the root of drive C: of a Windows-based Identity Console workstation and at your home directory of a Linux-based Identity Console workstation.

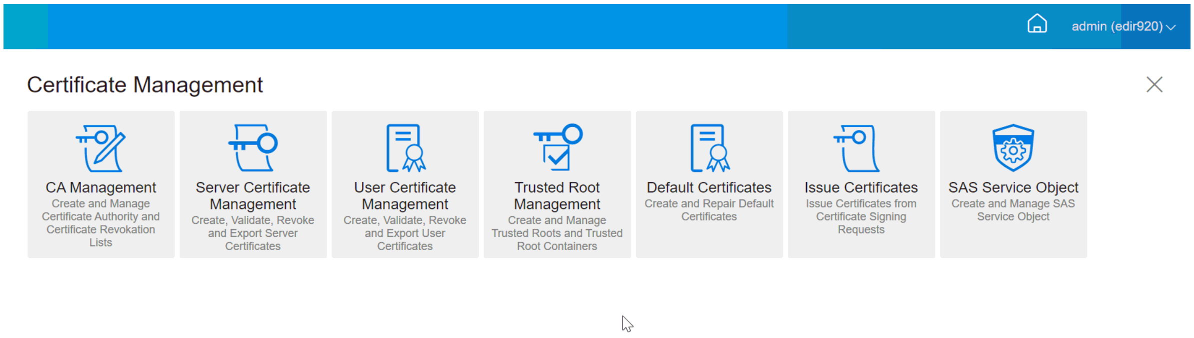
7b **File in Base64 Format:** This option lets you save a CSR or export a certificate to a file displayed in the Filename field. By default, the certificate and CSR files are exported with a .B64 extension at the root of drive C: of a Windows-based Identity Console workstation and at your home directory of a Linux-based Identity Console workstation.

7c **File in CER Format:** This option lets you save a CSR or export a certificate to a file displayed in the Filename field. By default, the certificate and CSR files are exported with a .CER extension at the root of drive C: of a Windows-based Identity Console workstation and at your home directory of a Linux-based Identity Console workstation.

8 Review the Summary of the certificate in the next screen and click **OK**.

9 A confirmation appears indicating that the certificate has been issued successfully.

Figure 17-6 *Issuing a Public Key Certificate*


admin (edir920)
Certificate Management
CA Management
Create and Manage Certificate Authority and Certificate Revokation Lists
Server Certificate Management
Create, Validate, Revoke and Export Server Certificates
User Certificate Management
Create, Validate, Revoke and Export User Certificates
Trusted Root Management
Create and Manage Trusted Roots and Trusted Root Containers
Default Certificates
Create and Repair Default Certificates
Issue Certificates
Issue Certificates from Certificate Signing Requests
SAS Service Object
Create and Manage SAS Service Object

Managing SAS Service Object

The SAS service object facilitates communication between a server and its server certificates. If you remove a server from an eDirectory tree, you also need to delete the SAS service object associated with that server. If you want to put the server back into the tree, you must create the SAS service object to go with that server. If you do not, you cannot create new server certificates.

The SAS service object is automatically created as part of the server health check. You should not need to create it manually.

You can create a new SAS service object only if there is not a properly named SAS service object in the same container as the server object. For example, for a server named WAKE, you will have a SAS service object named SAS Service - WAKE. The utility adds the DS pointers from the Server object to the SAS object, and from the SAS object to the Server object, as well as set up the correct ACL entries on the SAS service object.

If a SAS service object already exists with the proper name, you cannot create a new one. The old SAS service object’s DS pointers might be wrong or missing, or the ACLs might not be correct. In this case, you can delete the corrupt SAS service object and use Identity Console portal to create a new one.

Creating or Deleting an SAS Service Object

To create or delete an SAS service object, perform the following steps:

1 Click **Certificate Management** > **SAS Service Object** options from the Identity Console landing page.

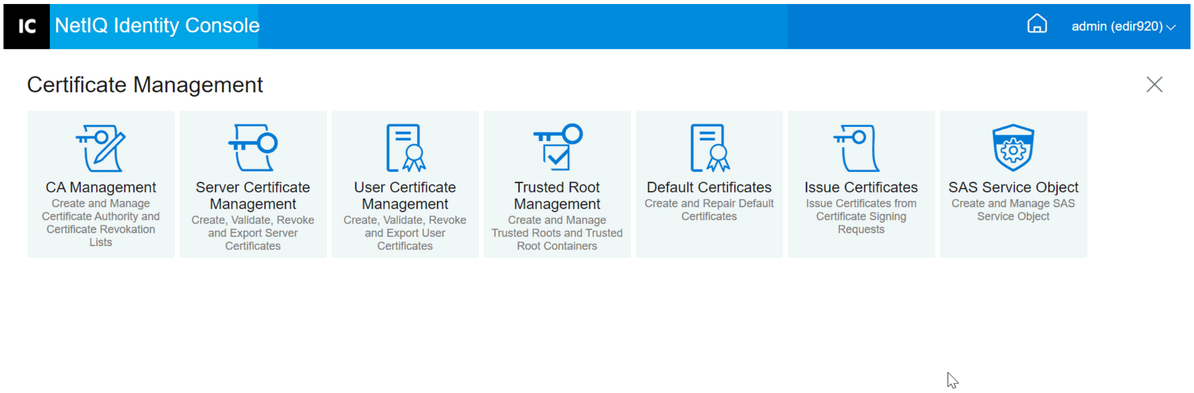
2 If there is no SAS Service Object created for an existing server, then click the + icon to create a new one.

3 A confirmation message appears indicating an SAS Service Object has been created successfully.

4 To remove an SAS Service Object, click the 🗑 icon.

5 Click **OK** in the confirmation screen to remove an SAS Service Object successfully.

Figure 17-7 *Managing SAS Service Objects*


IC
NetIQ Identity Console
admin (edir920)
Certificate Management
CA Management
Create and Manage Certificate Authority and Certificate Revokation Lists
Server Certificate Management
Create, Validate, Revoke and Export Server Certificates
User Certificate Management
Create, Validate, Revoke and Export User Certificates
Trusted Root Management
Create and Manage Trusted Roots and Trusted Root Containers
Default Certificates
Create and Repair Default Certificates
Issue Certificates
Issue Certificates from Certificate Signing Requests
SAS Service Object
Create and Manage SAS Service Object

18 Managing Authentication Framework

Using the Authentication module, you can perform the following tasks:

- “Managing Login and Post-Login Methods and Sequences” on page 105
- “Managing Password Policies” on page 111
- “Managing Challenge Sets” on page 117

Managing Login and Post-Login Methods and Sequences

NMAS includes support for a number of login and post-login methods from NetIQ and from third-party authentication developers. Some methods require additional hardware and software. Make sure that you have all of the necessary hardware and software for the methods you will use.

This section describes how to install, set up, and configure login and post-login methods and sequences for NMAS.

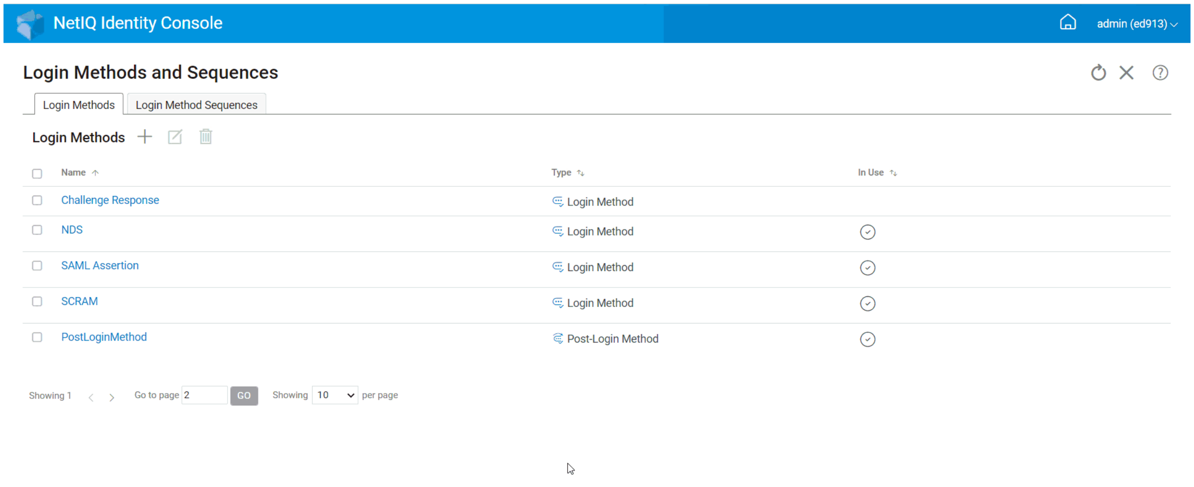
- “Installing a Login or Post-Login Method” on page 105
- “Updating an Existing Login or Post-Login Method” on page 106
- “Uninstalling Login or Post-Login Method(s)” on page 107
- “Creating a New Login Method Sequence” on page 107
- “Modifying a Login Method Sequence” on page 108
- “Authorizing or De-Authorizing a Login Method Sequence” on page 109
- “Setting a Default Login Method Sequence” on page 110
- “Deleting Login Method Sequence(s)” on page 111

Installing a Login or Post-Login Method

To install a login method, perform the following tasks:

1. Click **Authentication Management** > **Login Methods and Sequences** options from the Identity Console landing page.
2. Click the + icon to install a new login method.
3. Browse and select the login method (.zip) file you want to install, then click **Next**.
4. Follow the installation wizard to complete the login method installation process.

Figure 18-1 Installing a New Login Method



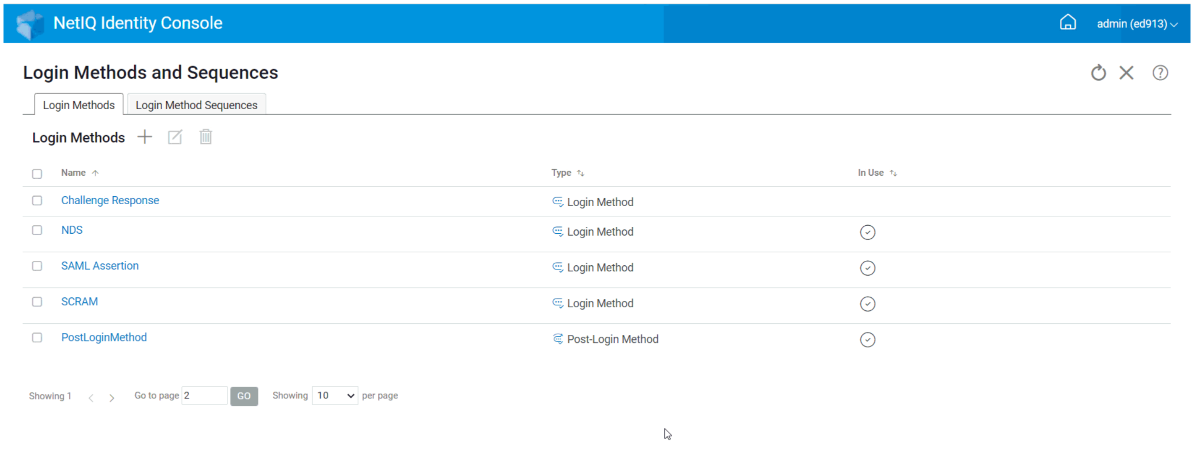
☐	Name	Type	In Use
☐	Challenge Response	Login Method	
☐	NDS	Login Method	✓
☐	SAML Assertion	Login Method	✓
☐	SCRAM	Login Method	✓
☐	PostLoginMethod	Post-Login Method	✓

Updating an Existing Login or Post-Login Method

To update an existing login method, perform the following steps:

1. Click **Authentication Management** > **Login Methods and Sequences** options from the Identity Console landing page.
2. Select the login method that you want to update from the list and click the ✎ icon.
3. Browse and select the login method (.zip) file you want to update, then click **Next**.
4. Follow the update wizard to complete updating the login method.

Figure 18-2 Updating an Existing Login Method



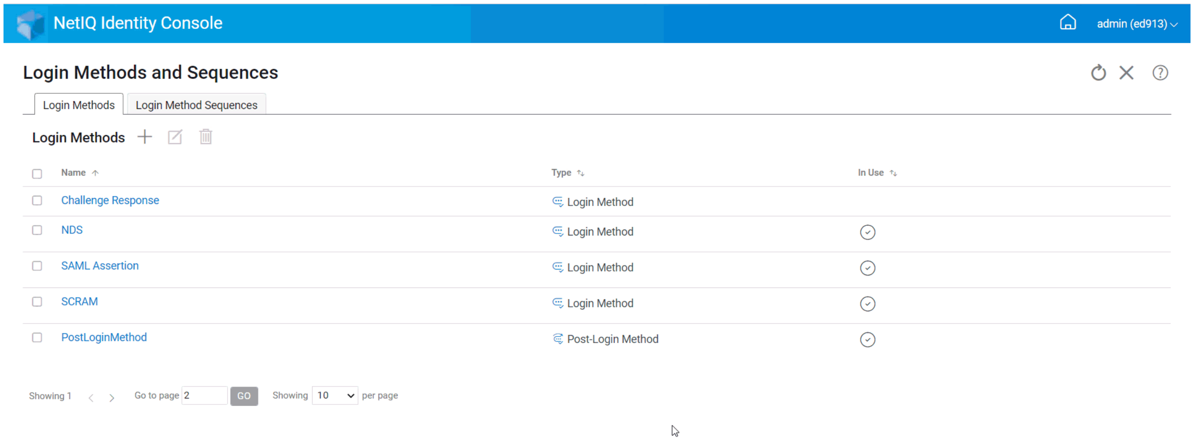
☐	Name	Type	In Use
☐	Challenge Response	Login Method	
☐	NDS	Login Method	✓
☐	SAML Assertion	Login Method	✓
☐	SCRAM	Login Method	✓
☐	PostLoginMethod	Post-Login Method	✓

Uninstalling Login or Post-Login Method(s)

To uninstall a login or post-login method(s), perform the following steps:

1. Click **Authentication Management** > **Login Methods and Sequences** options from the Identity Console landing page.
2. Select the login method(s) that you want to uninstall from the list and click the 🗑 icon.
3. In the next screen, click **OK**.
4. A confirmation message appears indicating that the login method(s) has been uninstalled.

Figure 18-3 *Uninstalling a Login Method*



☐	Name	Type	In Use
☐	Challenge Response	Login Method	
☐	NDS	Login Method	✓
☐	SAML Assertion	Login Method	✓
☐	SCRAM	Login Method	✓
☐	PostLoginMethod	Post-Login Method	✓

Creating a New Login Method Sequence

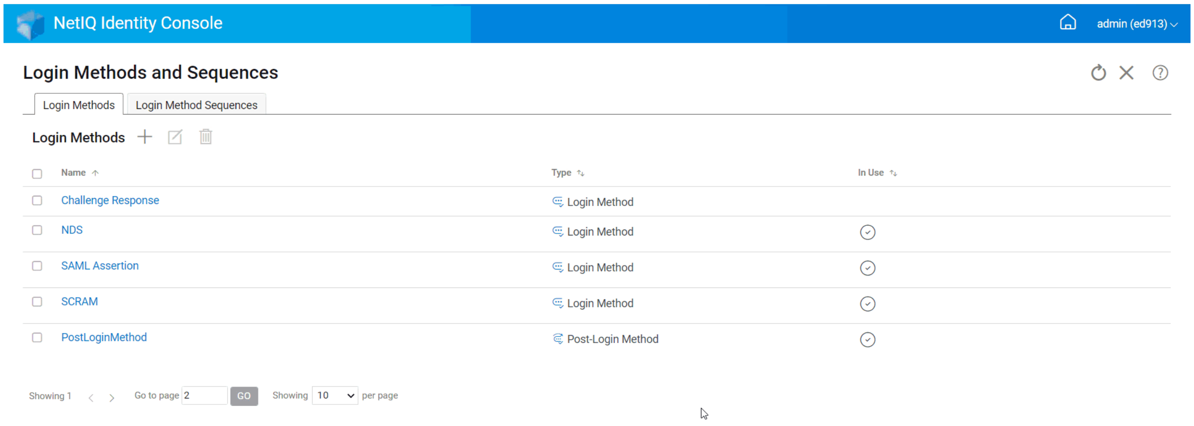
Once you have various login methods created for your environment, you can decide on which order these methods should be used. To create a new login method sequence, perform the following steps:

1. Click **Authentication Management** > **Login Methods and Sequences** options from the Identity Console landing page.
2. Select the **Login Method Sequences** tab.
3. Click the + icon to create a new login method sequence.
4. Specify a **name** and select the **Sequence type**.
5. Select the required login and post-login methods from the available login and post-login methods list.

NOTE: You can decide the order of the login methods by clicking on the up and down arrow visible on the login method objects.

6. Click on the **Create** button.
7. A confirmation message appears indicating a new login method sequence has been created successfully.

Figure 18-4 *Creating a Login Method Sequence*



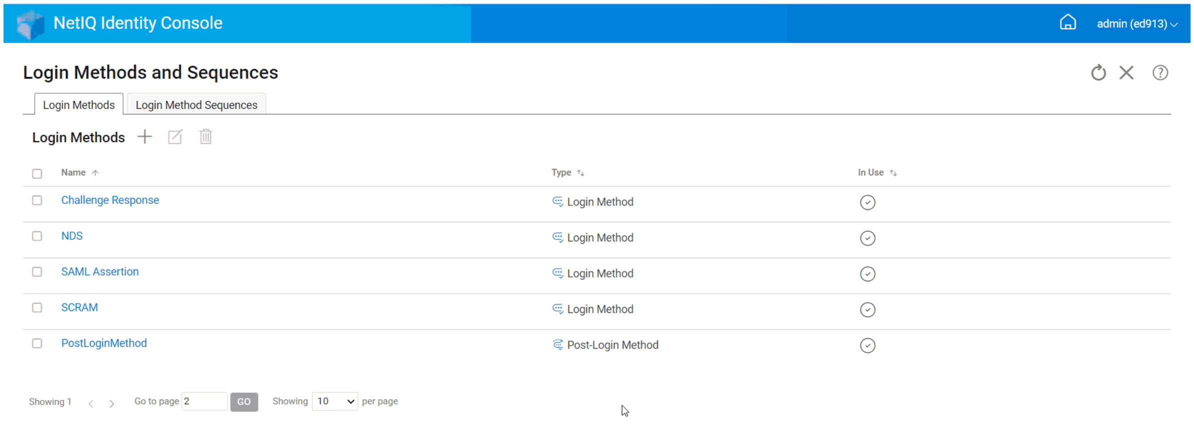
☐	Name	Type	In Use
☐	Challenge Response	Login Method	
☐	NDS	Login Method	✓
☐	SAML Assertion	Login Method	✓
☐	SCRAM	Login Method	✓
☐	PostLoginMethod	Post-Login Method	✓

Modifying a Login Method Sequence

To modify an existing login method sequence, perform the following steps:

1. Click **Authentication Management** > **Login Methods and Sequences** options from the Identity Console landing page.
2. Select the **Login Method Sequences** tab.
3. Click the ✎ icon to modify an existing login method sequence.
4. Make necessary changes in the **Modify Login Method Sequence** page and click **Save**.
5. A confirmation message appears indicating that the login method sequence has been modified successfully.

Figure 18-5 *Modifying a Login Method Sequence*



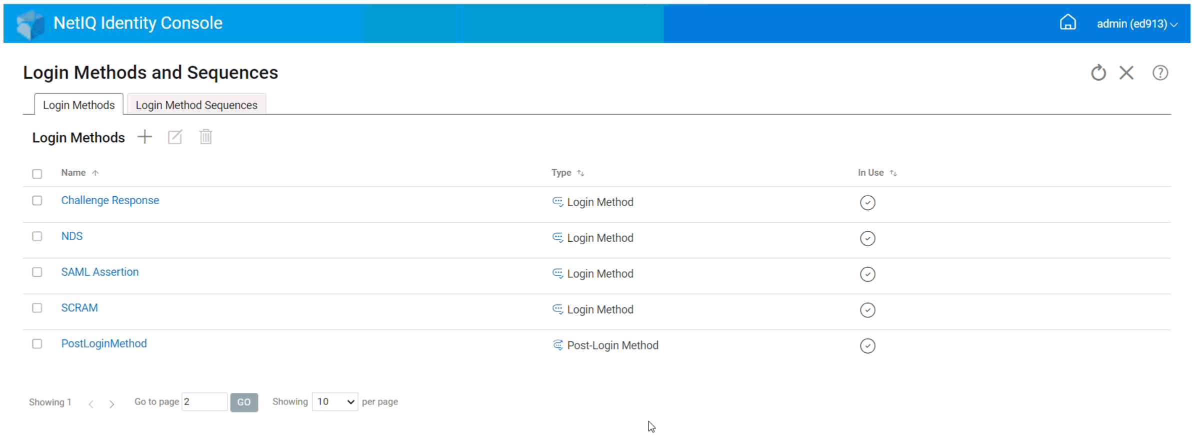
☐	Name	Type	In Use
☐	Challenge Response	Login Method	✓
☐	NDS	Login Method	✓
☐	SAML Assertion	Login Method	✓
☐	SCRAM	Login Method	✓
☐	PostLoginMethod	Post-Login Method	✓

Authorizing or De-Authorizing a Login Method Sequence

A login method sequence should be authorized and set to default in order to associate them with users, containers and partitions. To authorize a login method sequence, perform the following steps:

1. Click **Authentication Management** > **Login Methods and Sequences** options from the Identity Console landing page.
2. Select the **Login Method Sequences** tab.
3. Select the appropriate login method sequence from the list and click the ✓ icon.
4. To de-authorize a login method sequence, select the login method sequence and click the ⊗ icon.
5. Alternatively, you can also authorize or de-authorize a login method sequence from the drop-down menu under the **Authorized** column in the Login Method Sequences list.

Figure 18-6 Authorizing or De-Authorizing a Login Method Sequence



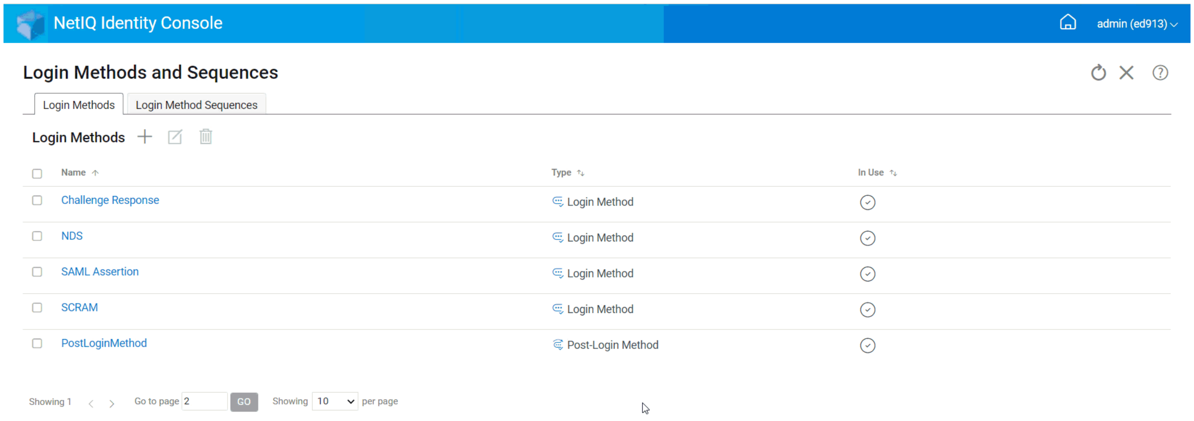
☐	Name	Type	In Use
☐	Challenge Response	Login Method	✓
☐	NDS	Login Method	✓
☐	SAML Assertion	Login Method	✓
☐	SCRAM	Login Method	✓
☐	PostLoginMethod	Post-Login Method	✓

Setting a Default Login Method Sequence

To set a default login sequence so that users are not required to specify a login sequence when logging in:

1. Click **Authentication Management** > **Login Methods and Sequences** options from the Identity Console landing page.
2. Select the **Login Method Sequences** tab.
3. Enable ✕ icon to set an authorized login method sequence to default.

Figure 18-7 Setting a Default Login Method Sequence



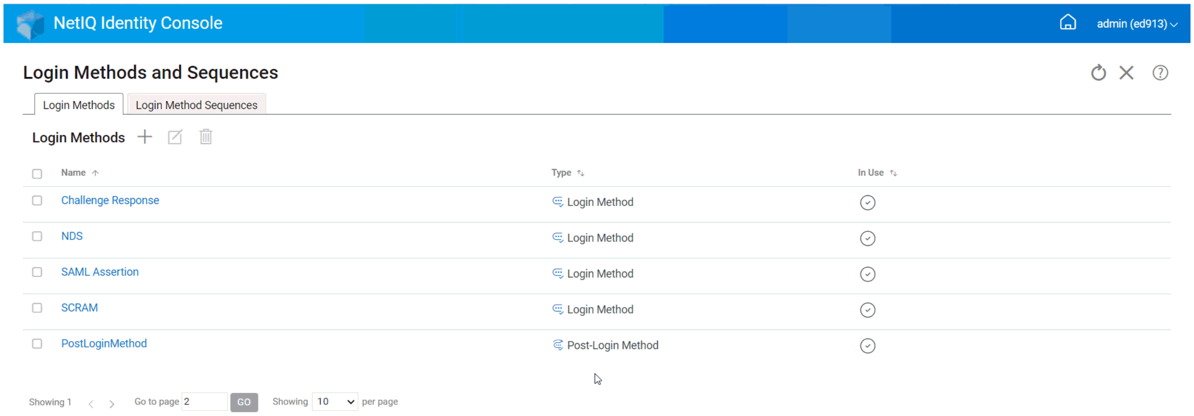
☐	Name	Type	In Use
☐	Challenge Response	Login Method	✓
☐	NDS	Login Method	✓
☐	SAML Assertion	Login Method	✓
☐	SCRAM	Login Method	✓
☐	PostLoginMethod	Post-Login Method	✓

Deleting Login Method Sequence(s)

To delete a login method sequence:

1. Click **Authentication Management** > **Login Methods and Sequences** options from the Identity Console landing page.
2. Select the **Login Method Sequences** tab.
3. Select the appropriate login method sequence from the list and click the 🗑 icon.
4. Click **OK** in the next confirmation screen.

Figure 18-8 *Deleting a Login Method Sequence*



☐	Name	Type	In Use
☐	Challenge Response	Login Method	✓
☐	NDS	Login Method	✓
☐	SAML Assertion	Login Method	✓
☐	SCRAM	Login Method	✓
☐	PostLoginMethod	Post-Login Method	✓

Managing Password Policies

A password policy is a collection of administrator-defined rules that specify the criteria for creating and replacing end-user passwords. NMAS enables you to enforce password policies that you assign to users in eDirectory.

Password policies can also include Forgotten Password Self-Service features, to reduce help desk calls for forgotten passwords. Another self-service feature is Reset Password Self-Service, which lets users change their passwords while viewing the rules the administrator has specified in the password policy. Users access these features through the Identity Manager User Application or Identity Console.

Using the Password Policies module, you can perform the following tasks:

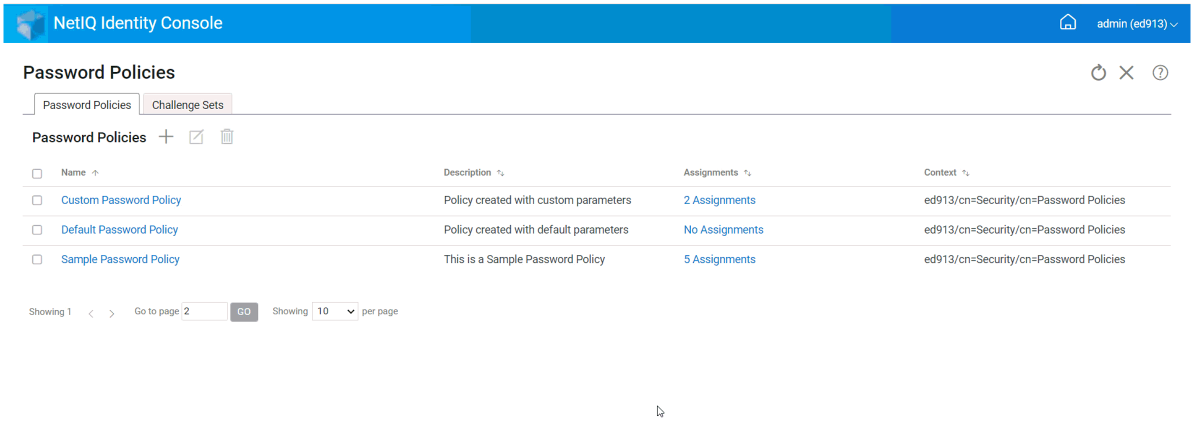
- "Creating a Password Policy with Default Settings" on page 112
- "Creating a Password Policy with Custom Settings" on page 112
- "Modifying a Password Policy" on page 115
- "Deleting Password Policies" on page 116

Creating a Password Policy with Default Settings

To create a new password policy, perform the following steps:

1. Click **Authentication Management** > **Password Policies** options from the Identity Console landing page.
2. Click the + icon to create a new password policy.
3. Specify the name, context, description and a password change message in the next screen.
4. If you want to create a password policy with the default settings, check the box for **Create a new Password Policy based on default settings** and click on **Next** to view the **Summary** page.
5. Verify the details in **Summary** page and click **Create**.
6. A confirmation message appears indicating that the Password Policy has been created successfully.

Figure 18-9 *Creating a Password Policy with Default Settings*



☐	Name	Description	Assignments	Context
☐	Custom Password Policy	Policy created with custom parameters	2 Assignments	ed913/cn=Security/cn=Password Policies
☐	Default Password Policy	Policy created with default parameters	No Assignments	ed913/cn=Security/cn=Password Policies
☐	Sample Password Policy	This is a Sample Password Policy	5 Assignments	ed913/cn=Security/cn=Password Policies

Creating a Password Policy with Custom Settings

To create a Password Policy with custom settings, perform the following steps:

1. Click **Authentication Management** > **Password Policies** options from the Identity Console landing page.
2. Click the + icon to create a new password policy.
3. Specify the name, context, description and a password change message in the next screen.
4. If you want to create a password policy with the custom settings, click **Next**.

5 Perform the following actions in the Configuration page:

5a **Enable Universal Password:** Enabling Universal Password for a policy enables you to use options in the Password Policies feature. However, before you can enable Universal Password for a policy, you must meet the prerequisites for Universal Password in your environment.

5b **Enable the Advanced Password Rules:** This option enables the password rules found in Advanced Password Rules. These rules help you secure your environment by giving you control over criteria, such as the lifetime of a password and content of a password such as combination of letters, numbers, uppercase or lowercase letters, and special characters. You can exclude passwords that you don't feel are secure, such as your company name.

5c **Password Synchronization:** These options determine how Universal Password is synchronized within eDirectory with other types of Identity Vault passwords. The Password Synchronization contains the following options:

5c1 **Remove NDS password when setting password:** If this option is selected, the NDS password will be disabled when the Universal Password is set. Users will be unable to use older methods or utilities that log in directly with the NDS password instead of communicating with NMAS. If this option is set, the next option Synchronize NDS password when setting password will be disabled by default.

5c2 **Synchronize NDS password when setting password:** If you select this option, setting the Universal Password in applications such as the Identity Console also changes the NDS password.

5c3 **Synchronize Simple Password when setting password:** This option provides the compatibility with NetIQ and third-party clients using Simple Password and user provisioning.

5c4 **Synchronize Distribution Password when setting password:** This option determines whether the metadirectory engine can retrieve or set a user's Universal Password in eDirectory.

5d **Universal Password Retrieval:** The following options are available:

5d1 **Allow user to retrieve password:** Allows user agent to retrieve password. This option determines whether the Forgotten Password Self-Service feature can retrieve a password on behalf of a user, so that the password can be e-mailed to the user. If you don't select this option, the corresponding feature is dimmed on the Forgotten Password tab in the password policy.

5d2 **Allow admin to retrieve password:** Select that box if you have a particular service that needs it. Identity Manager does not have a need for administrators to retrieve passwords. However, some third-party services might take advantage of this option.

5d3 **Allow the following to retrieve password:** Select the appropriate user who is supposed to retrieve password by clicking the + icon.

5e **Authentication:**

5e1 **Verify whether existing passwords comply with the password policy (Verification occurs on login):** This option is useful if you are deploying a new password policy or changing the Advanced Password Rules for an existing policy, and you want to make sure that existing passwords comply with the new or changed rules.

If you select this option, when users log in, their existing passwords are analyzed to make sure that they comply with the Advanced Password Rules in the new or changed password policy. If an existing password does not comply, the user is required to change it.

Once done, click **Next**.

6 **Advanced Password Rules** help you secure your environment by giving you control over password details such as lifetime of password, the frequency of changing the password and What a password contains.

Special characters are the characters that are not numbers (0-9) and are not alphabetic characters.

Perform the following actions in the Advanced Password Rules page:

6a You can manage password syntax settings using the Microsoft Complexity Policy (pre-Microsoft Windows Server 2008), Microsoft Server 2008 Password Policy, or Novell syntax.

6b Specify the required options for Change Password, Password Lifetime, Password Length and Composition, and Password Exclusion in the wizard and click **Next**.

7 You can reduce help desk costs by enabling **Forgotten Password** self-service for users who forget a password. These self-service features are available to users through the Identity Console portal. perform the following actions in the Forgotten Password page:

NOTE: If you enable Forgotten Password, you must also specify whether a Challenge Set is required to help the user log in.

7a **Challenge Sets:** If you use Challenge Sets, users are unable to use Forgotten Password self-service until they answer the Challenge Set questions. To make sure that users are prompted to enter this information through the Identity Console portal, select the **Require Challenge Set** option.

7b **Action:** The available options under this tab enable your user to reset password using Challenge Sets and Universal Password, to enable the current password or the password hint to be sent via email and to display the password hint option.

7c **Authenticate:** Select **Force user to configure Challenge Questions and/or Hint upon authentication** box to ensure that users are prompted to specify the Challenge Sets or Password hint.

Once done, click **Next**.

8 A policy is not in effect until you assign it to one or more objects. We recommend that you assign policies as high in the tree as possible, to simplify administration. A Password Policy can be assigned to the following objects:

8a **Login Policy object:** We recommend that you create a default password policy for all users in the tree and assign to Login Policy object which is located in the Security container.

8b **A container that is a partition root:** If you assign a policy to a container that is the root of a partition, all users in that partition, including users in sub-containers, inherit the policy assignment.

8c **A container that is not a partition root:** If you assign a policy to a container that is not the root of a partition, only users held in that specific container inherit the policy assignment. Users that are held in sub-containers do not inherit the policy.

To apply the policy to all users below a container that is not a partition root, assign the policy to each sub-container individually.

8d **A user:** You can assign a policy to one or more users.

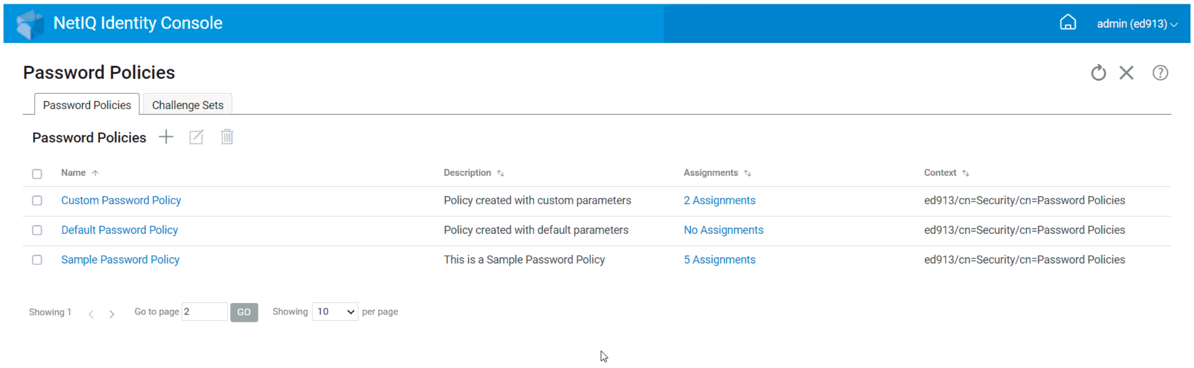
To assign a policy, click on the + icon. Then browse and select the appropriate object to assign a password policy.

In case you want remove a policy association, select the policy from the list and click on the 🗑 icon.

9 Verify the details in **Summary** page and click **Create**.

10 A confirmation message appears indicating that the Password Policy has been created successfully.

Figure 18-10 *Creating a Password Policy with Custom Settings*



☐	Name	Description	Assignments	Context
☐	Custom Password Policy	Policy created with custom parameters	2 Assignments	ed913/cn=Security/cn=Password Policies
☐	Default Password Policy	Policy created with default parameters	No Assignments	ed913/cn=Security/cn=Password Policies
☐	Sample Password Policy	This is a Sample Password Policy	5 Assignments	ed913/cn=Security/cn=Password Policies

Modifying a Password Policy

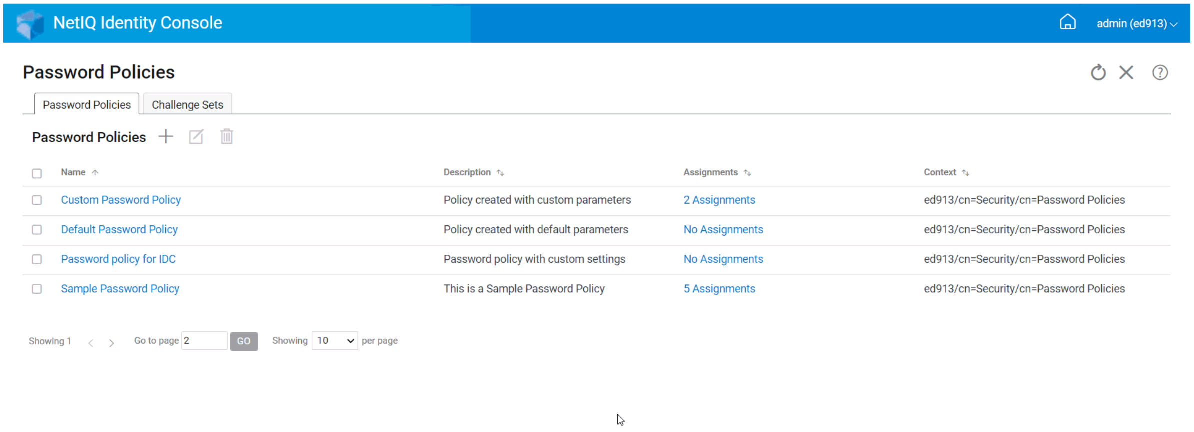
To modify an existing password policy, perform the following steps:

1 Click **Authentication Management** > **Password Policies** options from the Identity Console landing page.

2 Select the appropriate Password Policy from the list and click the ✎ icon.

3 Make necessary changes in the **Modify Password Policy** page and click **Save**.

Figure 18-11 Modifying a Password Policy



NetIQ Identity Console

admin (ed913)

Password Policies

Password Policies | Challenge Sets

Password Policies

☐	Name	Description	Assignments	Context
☐	Custom Password Policy	Policy created with custom parameters	2 Assignments	ed913/cn=Security/cn=Password Policies
☐	Default Password Policy	Policy created with default parameters	No Assignments	ed913/cn=Security/cn=Password Policies
☐	Password policy for IDC	Password policy with custom settings	No Assignments	ed913/cn=Security/cn=Password Policies
☐	Sample Password Policy	This is a Sample Password Policy	5 Assignments	ed913/cn=Security/cn=Password Policies

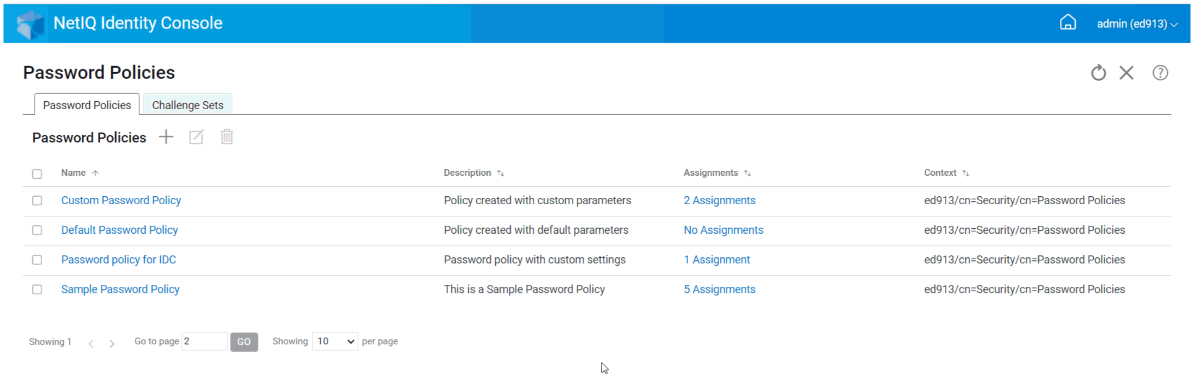
Showing 1 < > Go to page 2 GO Showing 10 per page

Deleting Password Policies

To delete password policies, perform the following steps:

1. Click **Authentication Management** > **Password Policies** options from the Identity Console landing page.
2. Select the appropriate Password Policies from the list and click the 🗑 icon.
3. In the next warning screen, click **OK**.
4. A confirmation message appears indicating that the password policies have been deleted.

Figure 18-12 Deleting a Password Policy



NetIQ Identity Console

admin (ed913)

Password Policies

Password Policies | Challenge Sets

Password Policies

☐	Name	Description	Assignments	Context
☐	Custom Password Policy	Policy created with custom parameters	2 Assignments	ed913/cn=Security/cn=Password Policies
☐	Default Password Policy	Policy created with default parameters	No Assignments	ed913/cn=Security/cn=Password Policies
☐	Password policy for IDC	Password policy with custom settings	1 Assignment	ed913/cn=Security/cn=Password Policies
☐	Sample Password Policy	This is a Sample Password Policy	5 Assignments	ed913/cn=Security/cn=Password Policies

Showing 1 < > Go to page 2 GO Showing 10 per page

Managing Challenge Sets

A Challenge Set is one or more questions that a user answers to validate their identity. A Challenge Set is part of Password Self-Service.

When a user has a problem remembering or using their password, they can use Password Self-service instead of calling the Help Desk. A Challenge Set enables a user to validate identity, and then receive a hint or password in an e-mail, or reset a password using a Web browser.

You can allow users to create and answer their own questions, or require users to answer questions that you create.

The Challenge Sets page lets you search for existing challenge sets; create a new challenge set; and edit existing challenge sets.

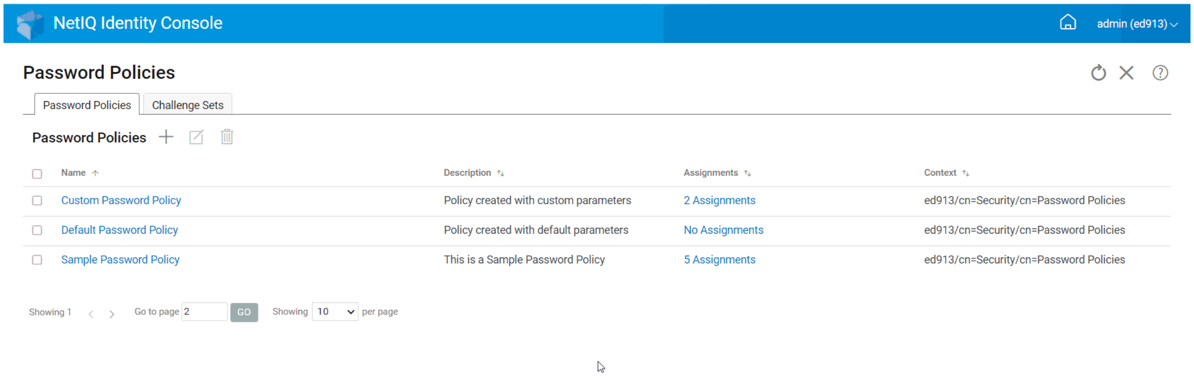
- "Creating a New Challenge Set" on page 117
- "Modifying a Challenge Set" on page 118
- "Deleting Challenge Set(s)" on page 119

Creating a New Challenge Set

To create a new Challenge Set, perform the following steps:

1. Click **Authentication Management** > **Password Policies** > **Challenge Sets** from the Identity Console landing page.
2. Click the + icon to create a new challenge set.
3. Specify a name for the Challenge Set object, and select the container or sub-container where the Challenge Set should be created.
4. Create a new set of questions to be asked for retrieving the user's password. You can also select from the existing set of random questions.
5. Set the number of questions to be asked and click **Create**.
6. A confirmation message appears indicating that the Challenge Set has been created successfully.

Figure 18-13 Creating a Challenge Set



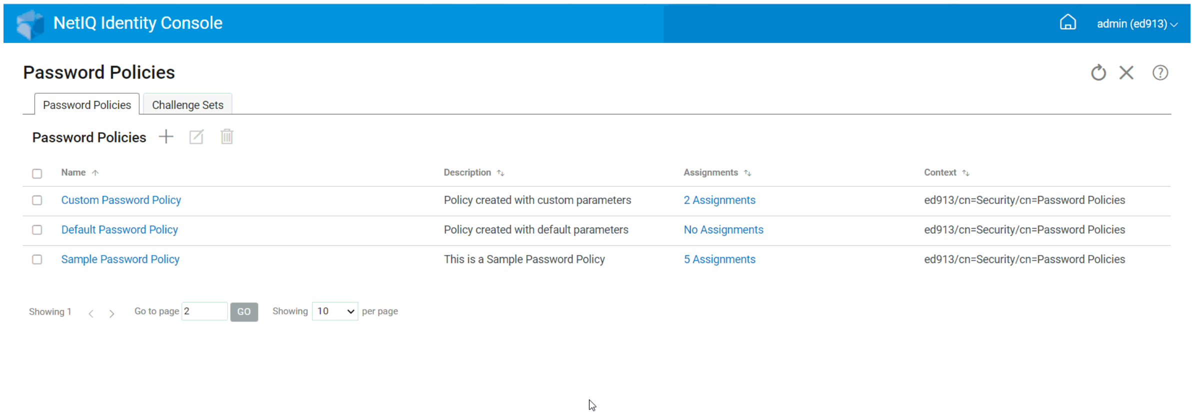
☐	Name	Description	Assignments	Context
☐	Custom Password Policy	Policy created with custom parameters	2 Assignments	ed913/cn=Security/cn=Password Policies
☐	Default Password Policy	Policy created with default parameters	No Assignments	ed913/cn=Security/cn=Password Policies
☐	Sample Password Policy	This is a Sample Password Policy	5 Assignments	ed913/cn=Security/cn=Password Policies

Modifying a Challenge Set

To modify an existing Challenge Set, perform the following steps:

1. Click **Authentication Management** > **Password Policies** > **Challenge Sets** from the Identity Console landing page.
2. Select the appropriate Challenge Set from the list and click the ✎ icon.
3. Make necessary changes in the Modify Challenge Set page and click **Save**.
4. A confirmation message appears indicating that the Challenge Set has been modified successfully.

Figure 18-14 Modifying a Challenge Set



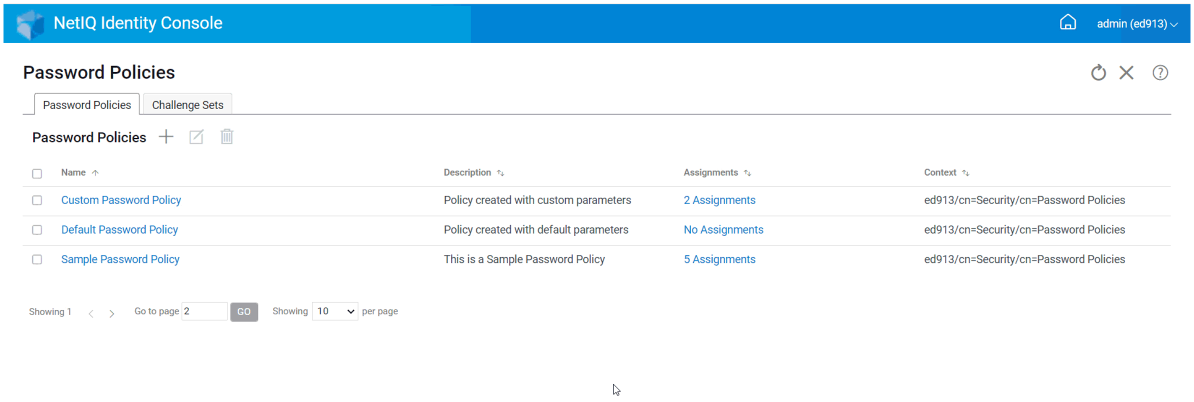
☐	Name	Description	Assignments	Context
☐	Custom Password Policy	Policy created with custom parameters	2 Assignments	ed913/cn=Security/cn=Password Policies
☐	Default Password Policy	Policy created with default parameters	No Assignments	ed913/cn=Security/cn=Password Policies
☐	Sample Password Policy	This is a Sample Password Policy	5 Assignments	ed913/cn=Security/cn=Password Policies

Deleting Challenge Set(s)

To delete Challenge Set(s), perform the following steps:

1. Click **Authentication Management** > **Password Policies** > **Challenge Sets** from the Identity Console landing page.
2. Select the required Challenge Set from the list and click the 🗑 icon.
3. Click **OK** on the confirmation screen.
4. A confirmation message appears indicating that the Challenge Set has been deleted successfully.

Figure 18-15 *Deleting a Challenge Set*



☐	Name	Description	Assignments	Context
☐	Custom Password Policy	Policy created with custom parameters	2 Assignments	ed913/cn=Security/cn=Password Policies
☐	Default Password Policy	Policy created with default parameters	No Assignments	ed913/cn=Security/cn=Password Policies
☐	Sample Password Policy	This is a Sample Password Policy	5 Assignments	ed913/cn=Security/cn=Password Policies

19 Managing SNMP Group Objects

The Simple Network Management Protocol (SNMP) is the standard operations and maintenance protocol for the Internet for exchanging management information between the management console applications and managed devices.

Using the SNMP module, you can perform the following tasks:

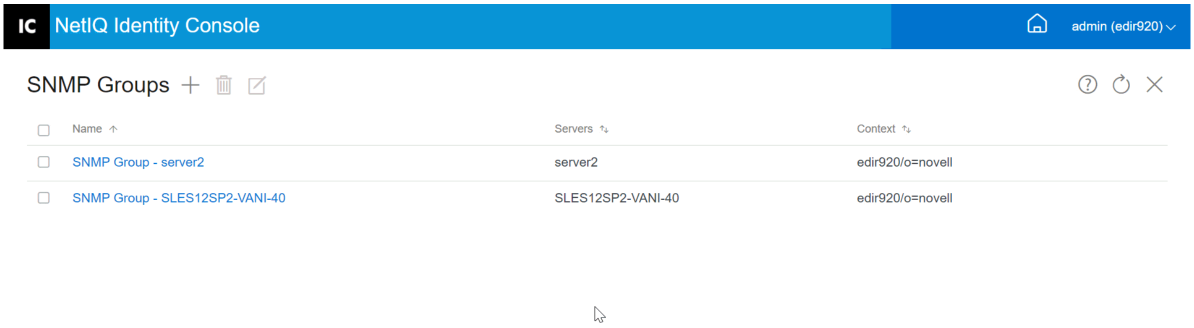
- "Creating SNMP Group Objects" on page 121
- "Modifying SNMP Group Objects" on page 122
- "Deleting SNMP Group Objects" on page 122

Creating SNMP Group Objects

To create SNMP group objects, perform the following steps:

1. Click the **SNMP** module from the Identity Console landing page.
2. Click the + icon to create a new SNMP group object.
3. Specify the name and select the context to create a new SNMP group object.
4. Click the **Create** button.
5. A message appears on your screen confirming that the SNMP group object has been created successfully.

Figure 19-1 *Creating SNMP Group Objects*



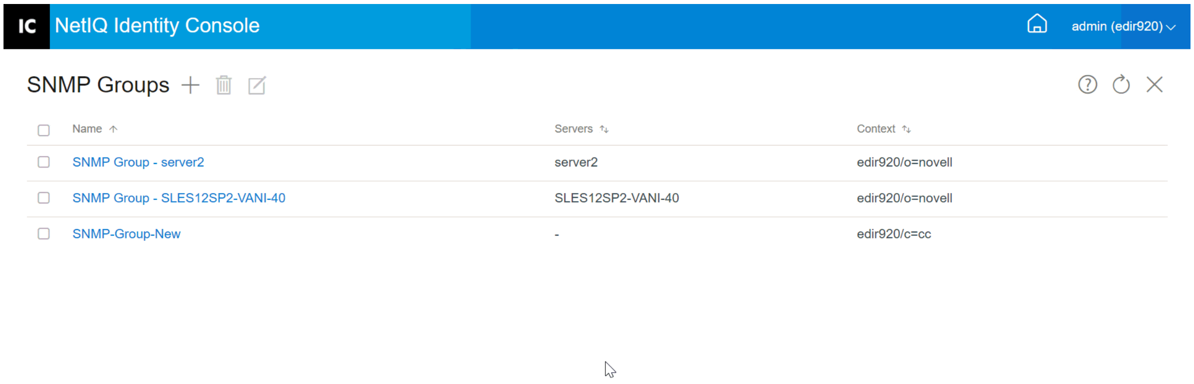
☐	Name	Servers	Context
☐	SNMP Group - server2	server2	edir920/o=novell
☐	SNMP Group - SLES12SP2-VANI-40	SLES12SP2-VANI-40	edir920/o=novell

Modifying SNMP Group Objects

To modify SNMP group objects, perform the following steps:

1. Click the **SNMP** module from the Identity Console landing page.
2. Select the SNMP group object that you want to modify and click the ✎ icon.
3. Modify the configurable parameters in the **General**/**Traps** page.
4. Once done, click the **Save** button.
5. A message appears on your screen confirming that the SNMP group object has been modified successfully.

Figure 19-2 Modifying SNMP Group Objects



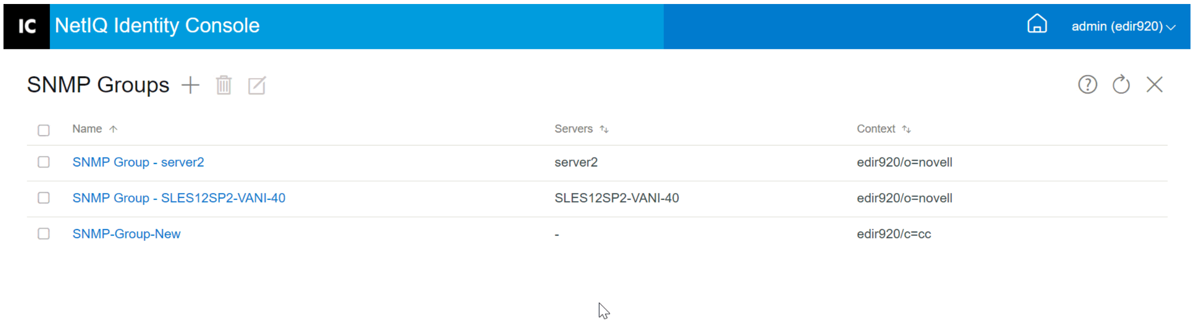
☐	Name	Servers	Context
☐	SNMP Group - server2	server2	edir920/o=novell
☐	SNMP Group - SLES12SP2-VANI-40	SLES12SP2-VANI-40	edir920/o=novell
☐	SNMP-Group-New	-	edir920/c=cc

Deleting SNMP Group Objects

To delete SNMP group objects, perform the following steps:

1. Click the **SNMP** module from the Identity Console landing page.
2. Select the SNMP group object that you want to modify and click the 🗑 icon.
3. Click **OK** in the next screen.
4. A message appears on your screen confirming that the SNMP group object has been deleted successfully.

Figure 19-3 Deleting SNMP Group Objects



☐	Name	Servers	Context
☐	SNMP Group - server2	server2	edir920/o=novell
☐	SNMP Group - SLES12SP2-VANI-40	SLES12SP2-VANI-40	edir920/o=novell
☐	SNMP-Group-New	-	edir920/c=cc

20 Managing the Enhanced Background Authentication

To access eDirectory from the EBA plug-in of Identity Console, you must have an EBA enabled server in your tree with a valid eba.p12 file. For more information on how to enabled EBA on your eDirectory tree, see Enabling EBA on an eDirectory Tree in the *NetIQ eDirectory Administration Guide*.

NOTE: If you want to use the EBA module with Identity Console, you must upgrade your eDirectory server to 9.2.4 HF2.

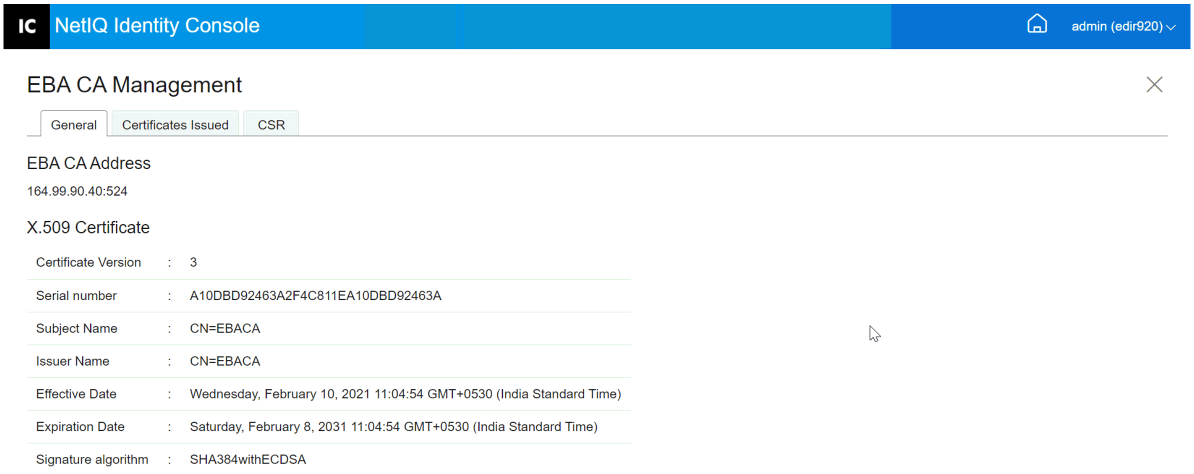
To open the EBA CA management page, log in to the Identity Console portal and click the **EBA** module.

The EBA CA management page includes the following tabs to manage different aspects of EBA CA:

- **General:** Displays the IP address of EBA CA and its certificate.
- **Certificates Issued:** Displays the NCP CA certificates along with their IP address and port.

  To revoke a certificate, select the certificate and click ⊘. Use this option only in extreme situations, because the server owning the NCP CA certificate will become non-functional when you revoke its certificate. Usually, revoking the certificate becomes necessary when a server is compromised.
- **CSR:** Lists the pending certificate signing requests for administrator approval. To approve a certificate signing request, select the certificate from the list and click **Approve**.

__Figure 20-1__ Managing Enhanced Background Authentication



EBA CA Address

164.99.90.40:524

X.509 Certificate

Certificate Version : 3
Serial number : A10DBD92463A2F4C811EA10DBD92463A
Subject Name : CN=EBACA
Issuer Name : CN=EBACA
Effective Date : Wednesday, February 10, 2021 11:04:54 GMT+0530 (India Standard Time)
Expiration Date : Saturday, February 8, 2031 11:04:54 GMT+0530 (India Standard Time)
Signature algorithm : SHA384withECDSA

21 Configuring and Customizing Identity Console

This section describes how to navigate through Identity Console web interface.

Contextless Login

The Contextless Login feature of Identity Console allows the users to login with only a user name and a password, without having to know or understand their entire user object context. For example, `admin.support`. If there are multiple users with the same user name in the tree, the Contextless Login tries to login using the first user account that it finds with the supplied password. In this case the user should provide the full context when logging in.

Administrators have the right to move the User objects or change the organization's name but this does not restrict the users from logging in.

Service Account: For using the Contextless Login, you need to provide the credentials for Service Account which should have the following rights on tree root object:

- Read on the `CN` attribute.
- Browse on [Entry Rights].

To take advantage of Contextless Login for a given tree, based on your environment, you have to enable the Contextless Login feature. The following procedure explains how to enable the Contextless login:

Enabling the Contextless Login for Standalone

To run the login script you must have administrator credentials or read permissions for CN attribute on the tree. The following procedure explains how to enable Contextless Login for Standalone.

1. Navigate to the folder where the build is extracted.
2. Run the contextless login script, for example: `./contextless-login`, and enter the following information of a service identity account:
   - Server IP Address: IP Address/DNS of eDirectory server.
   - User DN: User DN for authentication.
   - Password: Password for authentication

   Example:

   ```
   ./contextless-login -h < Tree Server IP/DNS> -a < cn=User,
   o=organization > -w < Password >.
   ```

   NOTE: When a password has special characters, it must be enclosed within single quotation marks. Example: 'Nvll13#-Th1$1$L0ng'

A message appears as `'Contextless login configured`'.

Enabling the Contextless Login for Docker

To enable the Contextless Login for Docker, run the command:

```
docker exec -it <identityconsole container name> /opt/novell/eDirAPI/sbin/
contextless-login -h < Tree Server IP/DNS> -a <User DN> -w <User Password>
```

For example:

```
docker exec -it idconsolecontainer-1 /opt/novell/eDirAPI/sbin/contextless-
login -h edirserver.novell.com -a cn=admin,o=novell -w novell
```

NOTE: When a password has special characters, it must be enclosed within single quotation marks. Example: 'Nvll13#-Th1$1$L0ng'

Enabling the Contextless Login for Workstation

At present the Contextless Login do not support Workstation.

IMPORTANT: If the password of the Service Account is modified or expired you need to re-run the Contextless Login script with the new credentials.

Customizing the Home Screen

Latest version of the Identity Console comes with customized branding where you can customize the header of the Identity Console application from home screen. The header, the company’s name, the colors, and the logo or favicon, can be customized directly from home screen itself.

The following procedure explain how to customize the home screen.

1. On the home screen > Your ID drop-down menu at top right > System Preferences.
2. On the Custom Branding page modify the **Header Title** and colors as per requirement.
3. (Optional) Upload a Logo.
4. Click **Save.**

Header Title: Allows you to change to your organization’s name. The organization name that you enter here will appear on the title bar of the web browser in place of the default text **Identity Console**.

Header Title Color: Allows you to set the color in which your organization’s name will be displayed on the title bar.

Header Left Color: Allows you to set the color of the left panel on the title bar.

Header Right Color: Allows you to set the color of the right panel on the title bar.

Logo Size: The image file size is recommended to be 50 x 50 pixel.

Configuring a Whitelist of Target URLs

A security practice such as IP whitelisting in networking and computer systems is useful in controlling access to applications or services based on the IP addresses of devices or networks. It is a way to allow access to only a specific list of approved URLs, effectively creating a whitelist of trusted entities that are allowed to communicate with the Identity Console. Any incoming connection attempts from URLs not on the whitelist of Identity Console are typically blocked. This allows redirection only to the configured URLs. For example, when an authentication request is not targeted to the whitelisted URLs, the Identity Console rejects the request. Also, you cannot configure External Applications. See: Managing External Applications.

The following procedure explains how to configure a whitelist of trusted URLs in the Identity Console.

1. On the Identity Console home screen > Your ID drop-down menu at top right > System Preferences.
2. On the System Preferences screen click **URL Filter**.
3. Click **Add URL** +.
4. Add the URL. For example, `https://11.11.11.111:7000/xyz.com` > click Add.
5. Click **Save**.

   The **URL List Modified Successfully** message appears.
6. Click **OK**.

NOTE:
- If the URL list is empty, the Identity Console will not allow to launch External Applications. The error message appears as **URL Mismatch. Please Configure the URL from System Preferences**.
- At least one RAC collection is required to manage External application.

Configuring Browser Refresh

While working on the Identity Console application, the session is logged out if you click the refresh button on the browser. The latest Identity Console application gives an option to the user to decide whether the session needs to be logged out or not when refresh button is pressed. The following procedure explains how to change the server settings to enable Identity console to store session:

1. Login to the Identity Console server with Administrator credentials.
2. Run the following command while logged in as root or root-equivalent user:

   ```
   cd /usr/bin
   ```

3. Run the following command:

   ```
   ./identityconsole enablerefresh
   ```

   A warning message appears: `enabling refresh will lead to storing the session in Identity console.`

   ```
   Do you want to store the session in Identity console [y/n]
   ```

4. Press **Y**, and enter.

   The message appear as `Enabling Identity console to store session, Session store Enabled!.`

To disable Identity console from storing the session, run the following command:

```
./identityconsole disablerefresh
```

Contextual Search

Contextual Search provides you an introductory layout for the search functionality. Here you can enter keyword and the search field determines information source to search and displays matching results. Using Contextual Search option, you can look for a resource and access it with ease across any page of the Identity Console application.

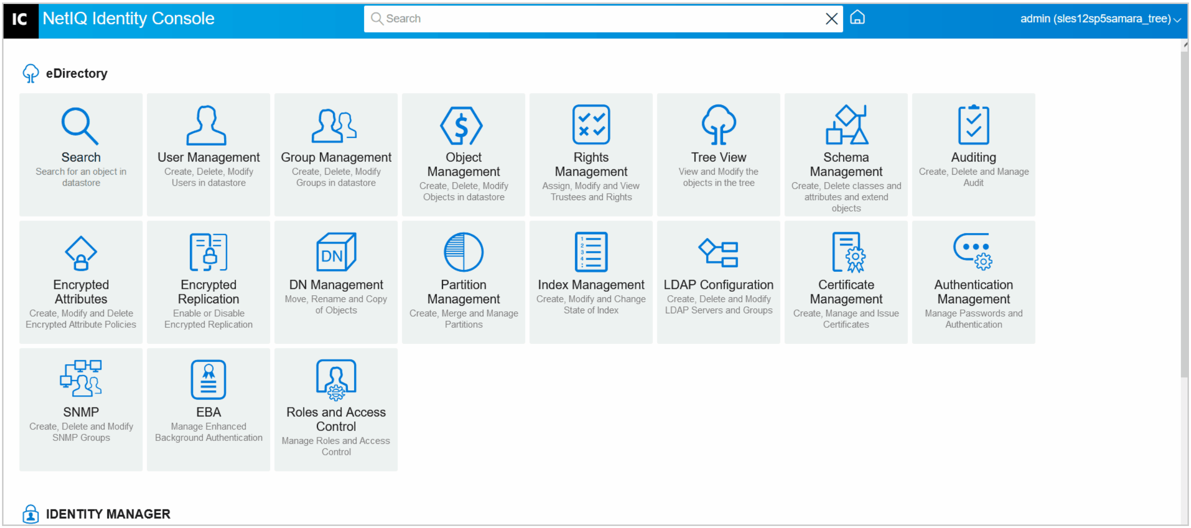
Scope of the Contextual Search is limited to the following objects:

- Tiles.
- Drivers.
- Driver Sets.
- Jobs.
- Email Templates.
- Driver Policies.

- ECMAScript.
- eDirectory Resources.

When you click Contextual Search field, it will show the list of features that are available on that particular page. The following graphic explains how the Contextual Search works for a user and for an Identity Manager tile.

Figure 21-1 *Searching a Tile or User*


IC
NetIQ Identity Console
Search
admin (sles12sp5samara_tree)
eDirectory
Search
Search for an object in datastore
User Management
Create, Delete, Modify Users in datastore
Group Management
Create, Delete, Modify Groups in datastore
Object Management
Create, Delete, Modify Objects in datastore
Rights Management
Assign, Modify and View Trustees and Rights
Tree View
View and Modify the objects in the tree
Schema Management
Create, Delete classes and attributes and extend objects
Auditing
Create, Delete and Manage Audit
Encrypted Attributes
Create, Modify and Delete Encrypted Attribute Policies
Encrypted Replication
Enable or Disable Encrypted Replication
DN Management
Move, Rename and Copy of Objects
Partition Management
Create, Merge and Manage Partitions
Index Management
Create, Modify and Change State of Index
LDAP Configuration
Create, Delete and Modify LDAP Servers and Groups
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
Roles and Access Control
Manage Roles and Access Control
IDENTITY MANAGER

Configuring Session-timeout for Identity Console

The session-timeout value represents the amount of time users can leave a page unattended in their web browser. The application will logout when the set time is complete.

NOTE: Session-timeout by default set at 15 minutes, the user can change the value as per their requirement.

To set the session-timeout, perform the following actions:

1. Login in to the Identity Console application server.
2. Navigate to the `/etc/opt/novell/eDirAPI/conf/` location.
3. Open the `edirapi.conf` file in a text editor and add the property `SessionIdleTimeout` with appropriate value.
4. Save the file and restart Identity Console.

II

Managing Identity Manager Using Identity Console

This section describes various tasks that you can perform to manage your Identity Manager server(s) using the Identity Console portal.

22 Managing Drivers and Driver Sets

A driver set is a container that holds Identity Manager drivers. Only one driver set can be active on a server at a time. As a result, all active drivers must be grouped into the same driver set. Driver Set can be created using Designer tool. For more information, see Configuring Driver Sets in the *NetIQ Designer for Identity Manager Administration Guide*.

- "Adding or Deleting Servers" on page 135
- "Activating Driver Sets Using Product Activation Key" on page 136
- "Viewing Activation Information of Driver Sets" on page 137
- "Starting and Stopping Drivers" on page 137
- "Searching for Drivers" on page 138
- "Filtering the Drivers and Driver Sets" on page 139
- "Deleting the Driver Set" on page 140
- "Driver Actions" on page 140

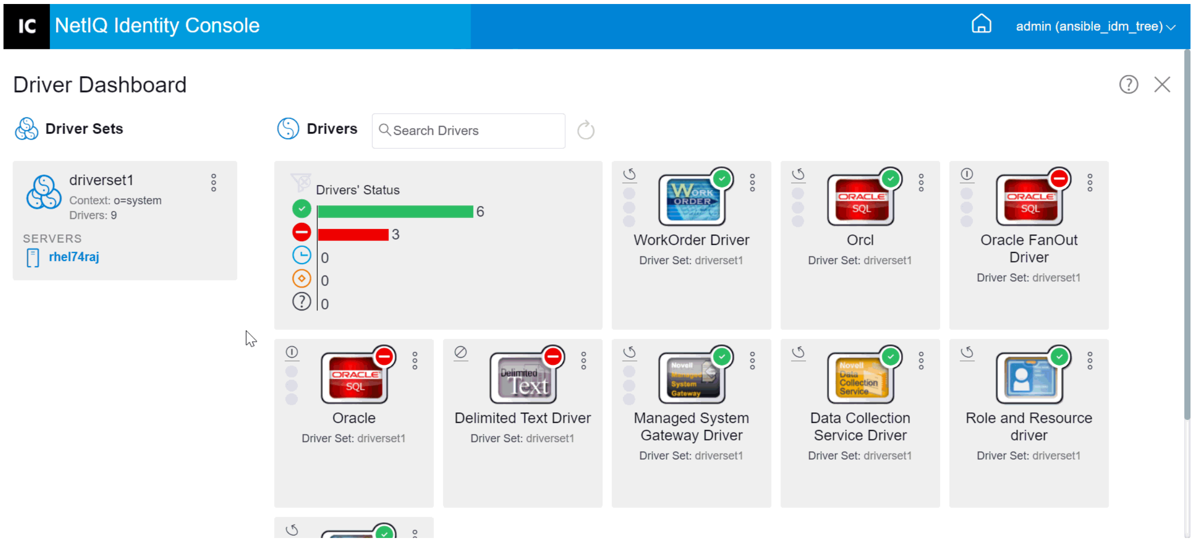
Adding or Deleting Servers

A driver set can be associated to one or multiple servers at a time. However, based on your requirement, you can associate a different driver set object to the available server.

To add a new server, click the ⋮ icon on the specific driver set object > select **Add Servers** and select the appropriate server from the context browser.

To delete an existing server, select the **Remove Server** option.

Figure 22-1 *Adding Server to Driver Set*



Activating Driver Sets Using Product Activation Key

Before using any driver set and the drivers residing inside the driver set, you must activate it using the activation code received in your email id. After purchasing a license, you will receive your activation key from NetIQ. Perform the following steps to activate the driver set using your activation key:

1 Click the **IDM Administration** tab from the Identity Console home screen.

2 Click Actions icon ⋮ on the specific driver set box that you want to activate and click **Activation Installation**.

On applying Activation, each driverset tab in IDM Administration tile displays the activation information for all servers associated with that driverset. This info helps to identify when the activation will expiry.

3 If you have the activation file downloaded on your computer, then select the check box for **Select a file containing credentials**.

4 Browse and select the activation file and click on **Submit**.

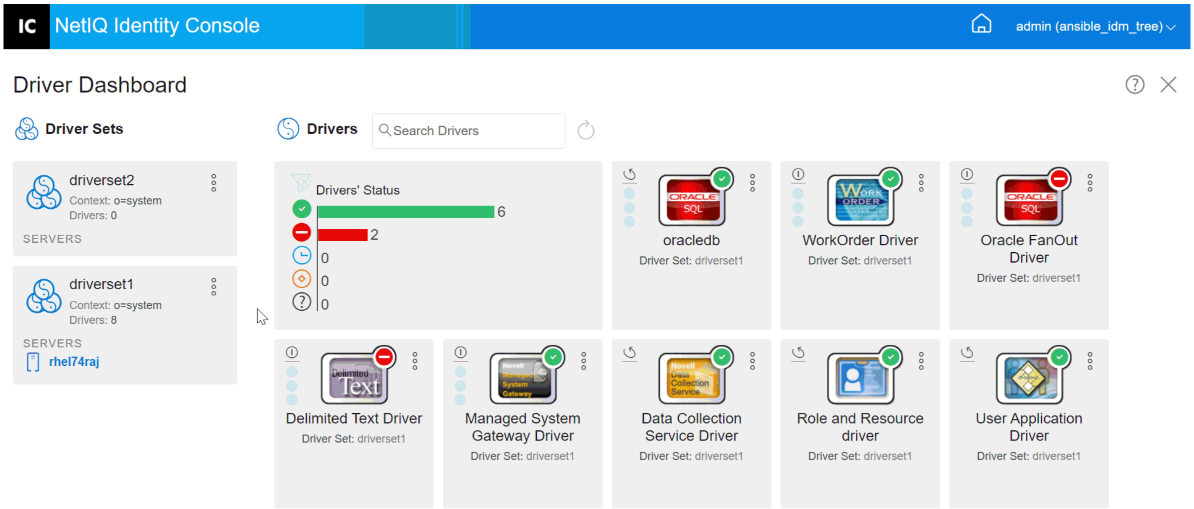
5 Alternatively, you can activate the driver set using the content of the activation file. Select the check box for **Enter the credentials**.

5a Open the Product Activation Credential file, then copy the contents of the Product Activation Credential to your clipboard.

5b If you chose to copy the contents, do not include any extra lines or spaces. You should begin copying from the first dash (-) of the credential (----BEGIN PRODUCT ACTIVATION CREDENTIAL) through the last dash (-) of the credential (END PRODUCT ACTIVATION CREDENTIAL-----) and click **Finish**.

6 A confirmation message appears indicating that the driver set has been activated successfully.

Figure 22-2 *Activating Driver Sets*

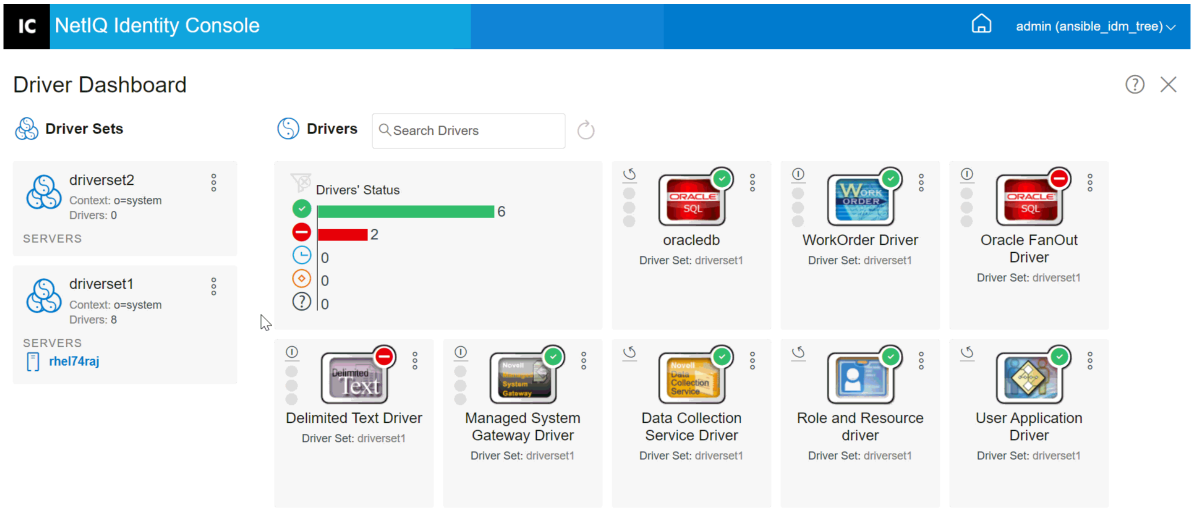


Viewing Activation Information of Driver Sets

After activating the driver set, you must verify that the driver set has been activated successfully. To verify, perform the following steps:

1. Click the **IDM Administration** tab from the Identity Console home screen.
2. Click Actions icon ⋮ on the specific driver set object for which you want to verify the activation info and click on **Activation Info**.
3. The activation related information window pops-up on your computer. You can verify the activation details of the specific driver set on this page.

Figure 22-3 *Viewing Activation Information of Driver Sets*

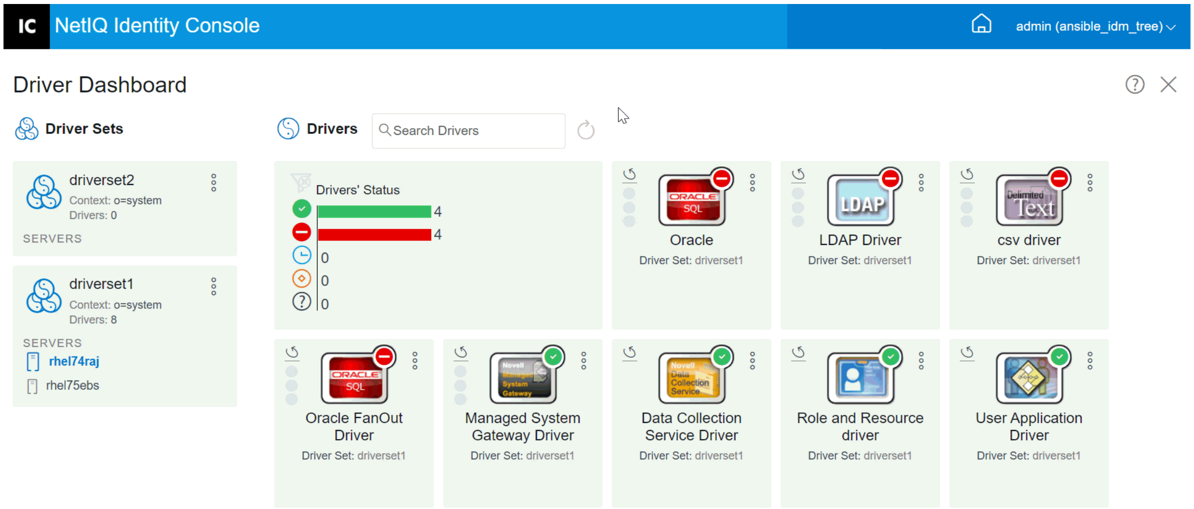


Starting and Stopping Drivers

When a driver is created, it is stopped by default. To make the driver work, you must start the driver. Identity Manager is an event-driven system, so after the driver is started, it remains idle until an event occurs. Perform the following steps to start/stop the driver(s).

1. Click the **IDM Administration** tab from the Identity Console home screen.
2. Click the specific driver set object on the right hand side of your computer screen to display all the drivers associated to it.
3. Click the Actions icon ⋮ on the specific driver and select **Start Driver**.
4. To stop a driver object, click the Actions icon ⋮ on the specific driver and select **Stop Driver**.
5. (Optional) Alternatively, you can start or stop all the drivers simultaneously residing in the same driver set object. Click the Actions icon ⋮ on the driver set object and select **Start All Drivers** or **Stop All Drivers**.

Figure 22-4 Starting and Stopping Drivers

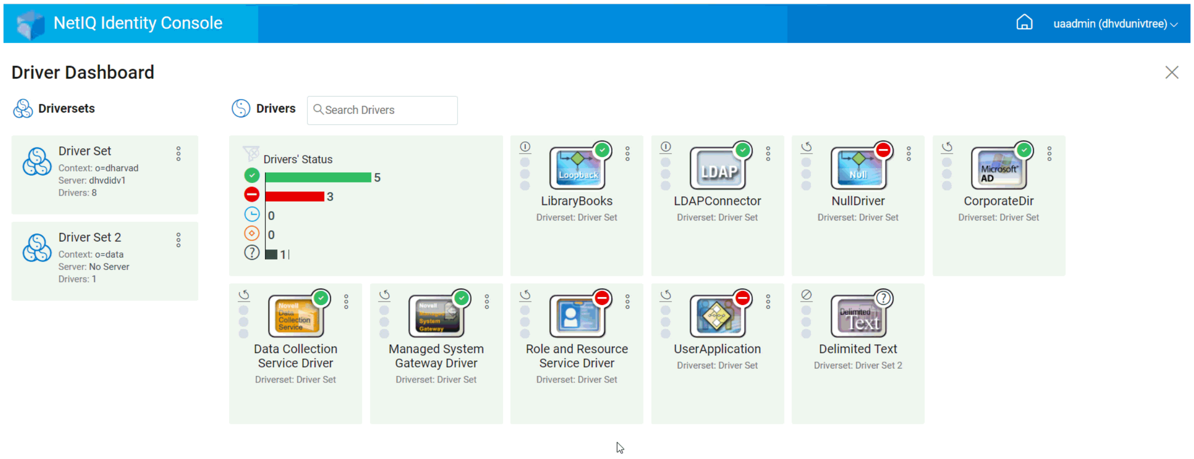


Searching for Drivers

Identity Console provides the option to search for a specific driver in your server. To search for a driver, perform the following steps:

1. Click the **IDM Administration** tab from the Identity Console home screen.
2. Specify the name of the driver in the **Search** box. The specific driver object will appear on your computer screen. You can also refresh the list of the drivers by clicking the ⟳ icon.

Figure 22-5 Searching for Drivers



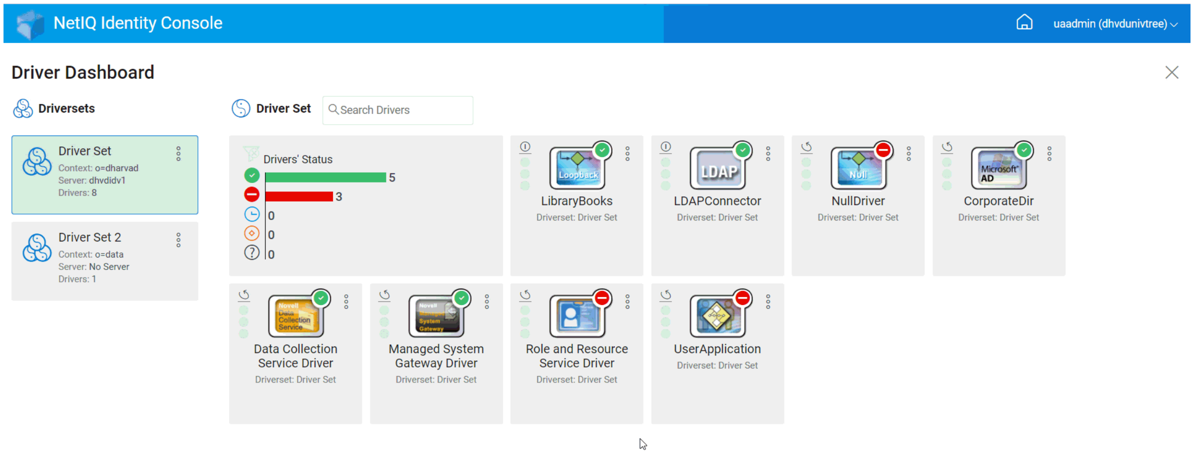
Filtering the Drivers and Driver Sets

The drivers can be filtered based on their status from the **IDM Administration** page. To filter drivers:

1. Click the **IDM Administration** tab from the Identity Console home screen.
2. Click the following icons on the **Drivers' Status** tile to filter out drivers based on their status:
   - Click ✓ icon to filter all the running drivers in your server.
   - Click ⛔ icon to filter all the stopped drivers in your server.
   - Click 🕒 icon to filter all those drivers which are starting up.
   - Click ◈ icon to filter all those drivers which are stopping.
   - Click ⓘ icon to filter out those drivers which do not have a status associated to them. When a driver set does not have a server associated to it, the drivers residing in that driver set will display **Unknown** status.

   To clear any filter that has been applied for the drivers, click ⊗ icon visible on the **Drivers' Status** tile.
3. The driver sets can also be filtered using the Identity Console portal. By default, Identity Console portal will display all the drivers associated to all the driver sets in your server. If you want to view drivers under a specific driver set, you must select that appropriate driver set from the list of driver sets on the left hand side of the Identity Console portal. To clear the driver set selection, click on the selected driver set once again.

Figure 22-6 *Filtering Drivers and Driver Sets*



Deleting the Driver Set

To delete a driver set, perform the following steps:

1. Click the **IDM Administration** tab from the Identity Console home screen.
2. Click the actions button ⋮ on the appropriate driver set that you want to delete.
3. Select **Delete**.

Driver Actions

The following actions are supported by clicking the actions icon ⋮ on the individual driver’s tile:

- **Start Driver**: To start a driver
- **Stop Driver**: To stop a driver
- **Restart Driver**: To restart a stopped driver
- **Delete Driver**: To delete a driver
- **Statistics**: To view the driver’s performance statistics
- **Copy Data**: To copy the driver’s data from one server to another server. This option is only available for multi-server environment.

23 Managing Driver Set Properties

This section provides information about the properties that are common to all driver sets. This includes all properties (Named Password, Log Level, Driver set inspector and so forth).

This section is divided into the following categories:

Configuring Driver Sets

To modify the Driver Set's configuration, perform the following steps:

1. Click on **IDM Administration** > **Click on the context menu (three dots) of the appropriate Driver Set** > **Driver Set Properties**.
2. By default, the **Driver Set Configuration** page appears. The Driver Set Configuration options are divided into the following categories:

Named Password

Identity Manager allows you to securely store multiple passwords for a driver set. This functionality is referred to as named passwords. Each different password is accessed by a key, or name.

You can add named passwords to a driver set or to individual drivers. Named passwords for a driver set are available to all drivers in the set.

To use a named password in a driver policy, you refer to it by the name of the password, instead of using the actual password, and the Identity Manager engine sends the password to the driver. The method described in this section for storing and retrieving named passwords can be used with any driver without making changes to the driver shim.

Named Password can be accessed by selecting **IDM Administration** > **Click the context menu (three dots) of the appropriate Driver Set** > **Driver Set Properties** > **Named Password** under **Driver Set Configuration**.

To add a new named password, click the + icon. To remove an existing named password, select the appropriate password and click the 🗑 icon.

Global Configuration Values

Displays an ordered list of Global Configuration objects. The objects contain extension GCV definitions for the driver that Identity Manager loads when the driver starts. You can add or remove the Global Configuration objects, and you can change the order in which the objects are executed.

Click the ⭳ icon to save the GCVs. To refresh the list of GCVs, click the ↻ icon.

Configuring the Java Environment Parameters

To configure Java Environment Parameters, perform the following steps:

1. In Identity Console, select **IDM Administration** > **Click the context menu (three dots) of the appropriate Driver Set** > **Driver Set Properties**.
2. Click **Java Environment Parameters** under **Driver Set Configuration** to display the property page that contains the Java environment parameters.
3. Modify the following settings as desired:

   Classpath Additions: Specify additional paths for the JVM to search for package (`.jar`) and class (`.class`) files. Using this parameter is the same as using the `java -classpath` command. When entering multiple class paths, separate them with a semicolon (;) for a Windows JVM and a colon (:) for a UNIX or Linux JVM.

   JVM Options: Specify additional options to use with the JVM. Refer to your JVM documentation for valid options.

   `DHOST_JVM_OPTIONS` is the corresponding environment variable. It specifies the arguments for JVM 1.2. For example:

   ```
   -Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
   ```

   Each option string is separated by whitespace. If an option string contains whitespace, then it must be enclosed in double quotes.

   The driver set attribute option has precedence over the `DHOST_JVM_OPTIONS` environment variable. This environment variable is tacked on to the end of driver set attribute option.

   Initial Heap Size: Specify the initial (minimum) heap size available to the JVM. Increasing the initial heap size can improve startup time and throughput performance. Use a numeric value followed by G, M, or K. If no letter size is specified, the size defaults to bytes. Using this parameter is the same as using the `java -Xms` command.

   `DHOST_JVM_INITIAL_HEAP` is the corresponding environment variable. It specifies the initial JVM heap size in decimal number of bytes. It has precedence over the driver set attribute option.

   Refer to your JVM documentation for information about the JVM's default initial heap size.

   Maximum Heap Size: Specify the maximum heap size available to the JVM. Use a numeric value followed by G, M, or K. If no letter size is specified, the size defaults to bytes. Using this parameter is the same as using the `java -Xmx` command.

`DHOST_JVM_MAX_HEAP` is the corresponding environment variable. It specifies the maximum JVM heap size in decimal number of bytes. It has precedence over the driver set attribute option.

Refer to your JVM documentation for information about the JVM's default maximum heap size.

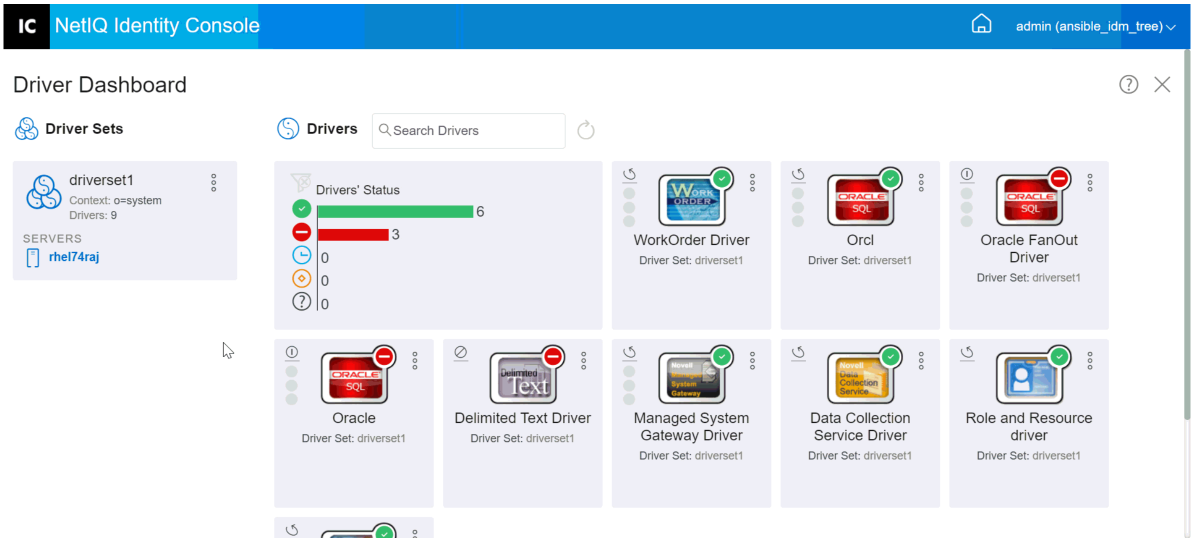
4. Click to save your changes.
5. Restart Identity Vault to apply the changes.

Managing Valued Attribute List

To add attributes to the valued attribute list for a specific Driver Set, perform the following steps:

1. In Identity Console, select the **Object Management** module.
2. Select **DirXML-DriverSet** type from the drop-down list and click the Search button.
3. Click the appropriate driver set from the search list.
4. To add unvalued attribute(s) to the valued list of attributes, click the + icon next to the **Valued Attributes** and select the appropriate unvalued attributes from the list.
5. Once done, click **OK**.

Figure 23-1 Managing Driver Set Configuration Parameters



Managing Jobs for Driver Sets

Identity Console enables you to schedule events using the Jobs option for all the driver residing in the respective driver set.

The Job Scheduler page contains the job's name, whether the job is enabled or disabled, when it is scheduled to run, and the job description. Click the job name to bring up the Jobs page. Click the enable/disable icon under the Enabled column to enable or disable the job. Click the job's description to see the job's full description.

The Jobs page is accessed by selecting IDM Administration > Click on the context menu (three dots) of the appropriate Driver Set > Driver Set Properties > Advanced tab from the Identity Console main page. The Jobs tab contains a table showing the existing job objects for the selected driver, which is listed with its fully distinguished name in the Driver entry.

The Job Scheduler page allows you to perform the following tasks:

- **Create the Job**: Click + icon to create a new job.

  In the **New Job** pop-up, to create a new job perform the following steps:

  1. Specify the job name.
  2. Select the job type.
  3. Click the ⌄ icon and select the server where you want to run the job, from the available list of servers. Otherwise, specify a server name and then select the server.
  4. Click the Create button.
- **Start the Job**: Select a job by clicking the box to the left of the job, then click ▷ icon.
- **Stop the Job**: Select a job by clicking the box to the left of the job, then click ⊡ icon.
- **Enable the Job**: Select a job by clicking the box to the left of the job, then click ✓ icon.
- **Disable the Job**: Select a job by clicking the box to the left of the job, then click ⊗ icon.
- **Get Status**: Select a job by clicking the box to the left of the job, then click ⓘ icon.
- **Delete the Job**: Select a job by clicking the box to the left of the job, then click 🗑 icon.

Click a job to access the **Job Property** page. Here you can set up how you want the job to run.

General: Shows the Java class name of the job. Use this page to enable or disable the job, delete the job after it runs, select the server or servers where this job should run, specify the email server, and give the job a different display name and description.

Schedule: Allows you set when you want to run the job. Specify the Start job at to set the time, and whether to run the job daily, weekly, monthly, yearly. You can also customize when you want to run the job, or you can choose to enable the toggle to run the job manually.

Scope: Allows you to define the objects that this job applies to. An object can be a container, a dynamic group, a group, or a leaf object. Click Add to select the object that you want this job to apply to. You can use the Browse button to select an object, then click OK. To remove an object from the scope list, select a scope object by clicking the box to the left of the DN object, then click Remove.

When an object is added, select it to display more options. If you select a group object, you have the option to apply the job to the group's members, or to the group only. If you select a container object, you have the option to apply the job to all descendants in that container, to all the children in the container, or to the container only.

Parameters: Allows you to add additional parameters to the job and to view the parameters as they are presently set up. These parameters change, depending on the type of job selected.

Results: Allows you to define what you want to do with the job results. The Results page is divided into two parts: Intermediate Result and Final Result, with the following results allowed: Success, Warning, Error, and Aborted. To the right of the Results column is the Action column. Clicking the Action column allows you to set how you want to be notified for each result. Actions include sending an audit result or sending an email when the result completes. If you do not select an option, no action is taken for the result.

In the **Trace** tab, you can configure trace for a specific driver. For more information, see "Configuring Trace Level" on page 170

Managing Libraries for Specific Driver Set

Library objects store multiple policies and other resources that are shared by one or more drivers. A library object can be created in a driver set object or any eDirectory container. Multiple libraries can exist in an eDirectory tree. Drivers can refer to any library in the tree as long as the server that is running the driver holds a Read/Write or Master replica of the library object.

Style sheets, policies, rules, and other resource objects can be stored in a library and be referenced by one or more drivers.

Using the Library Management module, you can perform the following tasks:

- "Viewing and Deleting an Existing Library" on page 145
- "Viewing and Deleting Objects from Library" on page 145

Viewing and Deleting an Existing Library

To view and delete an existing library, perform the following steps:

1 In Identity Console, select **IDM Administration** > **Click the context menu (three dots) of the appropriate Driver Set** > **Driver Set Properties** > **Advanced** > **Libraries**.

2 Select the appropriate library from the list.

3 Click the 🗑 icon. Click **OK** to confirm.

Viewing and Deleting Objects from Library

You can view and delete policies and mapping tables from library objects. To delete objects, perform the following steps:

1 In Identity Console, select **IDM Administration** > **Click the context menu (three dots) of the appropriate Driver Set** > **Driver Set Properties** > **Advanced** > **Libraries**.

2 Click the appropriate library from the list.

3 To delete policies, select the **Policies** tab.

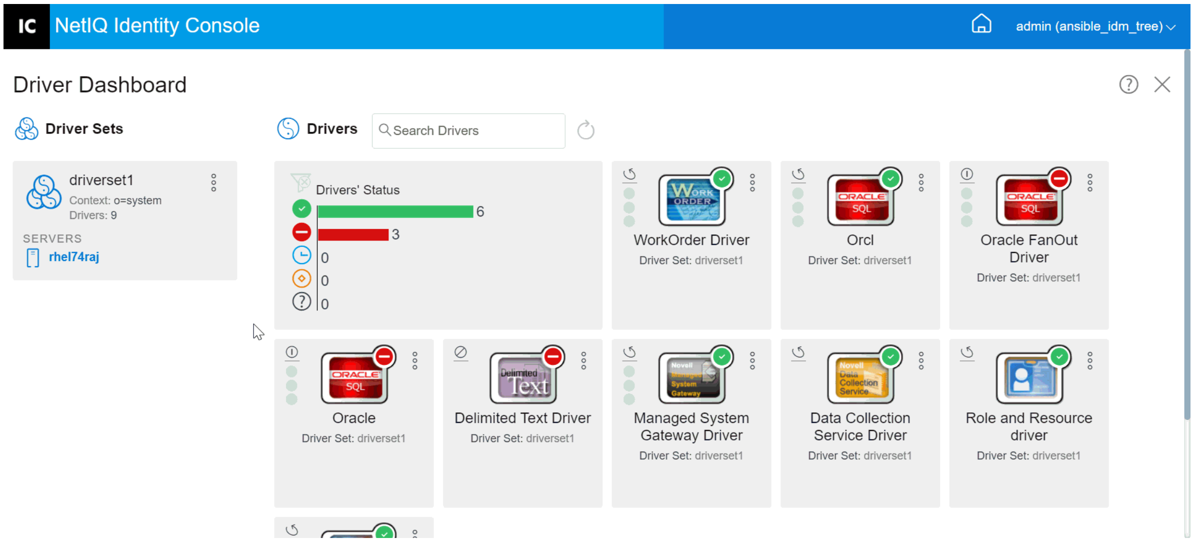
4 Select the appropriate policy from the list and click the 🗑 icon.

5 To delete mapping tables, select the **Mapping Tables** tab.

6 Select the appropriate mapping table from the list and click the 🗑 icon.

7 Click **OK** to confirm.

Figure 23-2 Managing Jobs and Libraries for Driver Sets



Configuring the Log and Trace Levels of Driver Sets

To configure log and trace for your driver sets, select **IDM Administration** > **Click the context menu (three dots) of the appropriate Driver Set** > **Driver Set Properties** > **Log & Trace Configuration** tab from the Identity Console main page. This section is divided into the following categories:

- "Configuring Log Level" on page 146
- "Configuring Trace Level" on page 147
- "Tracing DirXML Script" on page 148

Configuring Log Level

Each driver set has a log level field where you can define the level of errors that should be tracked. The level you indicate here determines which messages are available to the logs. By default, the log level is set to track error messages. (This also includes fatal messages.) To track additional message types, change the log level. To configure the log level, select In Identity Console, select **IDM Administration** > **Click the context menu (three dots) of the appropriate Driver Set** > **Driver Set Properties** > **Log & Trace Configuration** > **Log Level**. The following table describes the log level settings:

Option	Description
Turn off logging to DriverSet, Subscriber and Publisher logs	Turns all logging off for all the drivers on the Driver Set object, Subscriber channel, and the Publisher channel.
Maximum number of entries in the log (50-500)	Number of entries in the log. The default value is 50.

Option	Description
Log Levels	The following log levels are available to select: - **Log errors**: Logs just errors - Log errors and warnings: Logs errors and warnings - **Log specific events**: Logs the events that are selected. Selecting this option enables the following list of events: - **Metadirectory Engine Events** - **Status Events** - **Operation Events** - **Transformation Events** - **Credential Provisioning Events** - **Only update the last log time**: Updates the last log time. - **Logging Off**: Turns logging off for the driver.

Configuring Trace Level

You can configure trace for a specific driver set. Depending on the trace level specified for a driver set, trace displays driver-related events when the engine processes the events. The driver trace level affects only the driver or driver set where trace is set. If you are using the Remote Loader, the Remote Loader trace file is set directly on the Remote Loader and contains only the driver shim trace.

To configure trace for a driver set, select **IDM Administration** > **Click the context menu (three dots) of the appropriate Driver Set** > **Driver Set Properties** > **Log & Trace Configuration** > **Trace** tab. The following table describes the trace settings:

Parameter	Driver
Trace level	As the driver trace level increases, the amount of information displayed in Trace increases. Trace level one shows errors, but not the cause of the errors. If you want to see password synchronization information, set the trace level to five. If you select **Use setting from Driver Set**, the value is taken from the driver set.
XSL trace level	Trace displays XSL events. Set this trace level only when troubleshooting XSL style sheets. If you do not want to see XSL information, set the level to zero.
Java debug port	Allows developers to attach a Java debugger. Restart the Identity Vault after attaching the Java debugger.
Trace file	Specify a file name and location of where the Identity Manager information is written for the selected driver. If you select **Use setting from Driver Set**, the value is taken from the driver set.

Parameter	**Driver**
Trace file encoding	The trace file uses the system's default encoding. You can specify another encoding if desired. If you select **Use setting from Driver Set**, the value is taken from the driver set.
Trace file size limit	Allows you to set a limit for the Java trace file. If you set the file size to unlimited, the file grows in size until there is no disk space left. **NOTE:** If the file size limit is specified the trace file is created in multiple files. Identity Manager automatically divides the maximum file size by ten and creates ten separate files. The combined size of these files equals the maximum trace file size. If you select **Use setting from Driver Set**, the value is taken from the driver set.

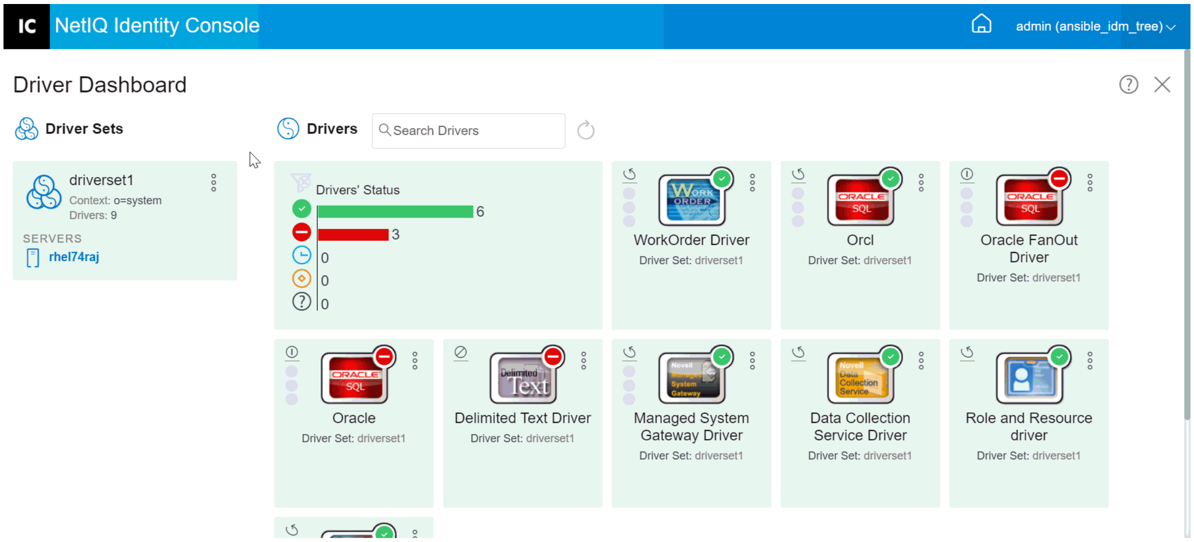
Tracing DirXML Script

The DirXML Script Tracing option allows you to select a trace level for a driver set. The selection gets applied to all the policies in the driver set. The following DirXML script tracing options are available to select:

- All DirXML Script Tracing On
- All DirXML Script Tracing Off
- DirXML Script Rule Tracing On
- DirXML Script Rule Tracing Off

Click to save your changes.

Figure 23-3 Managing Log and Trace Levels of Driver Sets



Managing Driver Set Inspector and Statistics

You can use the Driver Set Inspector to view detailed information about the objects associated with a driver set. This section is divided into the following categories:

- "Viewing Driver Set Statistics" on page 149
- "Viewing Version Information" on page 149
- "Viewing Association Statistics" on page 150

Viewing Driver Set Statistics

You can use Identity Console portal to view a variety of statistics for a single driver or for an entire driver set. This includes statistics such as the cache file size, the size of the unprocessed transactions in the cache file, the oldest and newest transactions, and the total number of unprocessed transactions by category (add, remove, modify, and so forth). To view the driver set statistics:

1. In Identity Console, select **IDM Administration** > **Click the context menu (three dots) of the appropriate Driver Set** > **Driver Set Properties** > **Inspector and Statistics** > **Statistics**.
2. Select the appropriate server from the drop-down.

   A page appears that allows you to view the statistics for all of the drivers contained in the driver set.

   - To refresh the statistics, click ↻ icon.
   - To close the statistics for a driver, click the ✕ button in the upper right corner of the driver's statistics window.
   - To open the statistics for all drivers, click **Actions** > **Show All**.
   - To collapse the list of unprocessed transactions for a driver, click the ⌃ button located above the list. To collapse the list of unprocessed transactions for all drivers, click **Actions** > **Collapse All Transactions**.
   - To expand the list of transactions, click the ⌄ button. To expand the list of unprocessed transactions for all drivers, click **Actions** > **Expand All Transactions**.
   - To close the statistics dashboard of disabled drivers, click **Actions**, then select **Close Disabled Drivers**.

Viewing Version Information

The Identity Manager engine, the driver shims, and the driver configuration files each contain a separate version number. The Version Discovery option in Identity Console helps you find the versions of the Identity Manager engine and the driver shims versions. The driver configuration files contain their own naming convention. To view the version information:

1. In Identity Console, select **IDM Administration** > **Click the context menu (three dots) of the appropriate Driver Set** > **Driver Set Properties** > **Inspector and Statistics** > **Version Discovery**.
2. View a top-level display of versioning information:

   - The eDirectory tree that you are authenticated to

NOTE: eDirectory is referred as Identity Vault when used in Identity Manager environment.

- The driver set that you selected
- Servers that are associated with the driver set

  If the driver set is associated with two or more servers, you can view Identity Manager information on each server.
- Drivers

3. Click the **View** icon to display a textual representation of the same information contained in the top-level view.
4. Click the Export button to export and save the text to a file on your local or network drive.

Viewing Association Statistics

By using the Identity Manager Association Statistics feature, you can find the association details of the identities managed by Identity Manager. Identity Manager uses the association statistics to obtain the association count for the Identity Manager drivers.

To obtain active, inactive, and system managed objects for a driver, run the association statistics job. You can schedule the association statistics job on a daily, weekly, monthly, or yearly basis. By default, the job is scheduled to run every week.

The Association Statistics dashboard displays the association details. Alternatively, you can view the details by exporting the associations to a file.

NOTE:

- The association count for the drivers is per server. If an object is associated with more than one driver, the association count is calculated uniquely for each driver.
- If you have more than 200,000 associations, We recommend you to set the maximum heap size for the driver set to 2 GB or more. For information about setting the heap size, see "Configuring the Java Environment Parameters" on page 142.

To view the association statistics:

1. In Identity Console, select **IDM Administration** > **Click the context menu (three dots) of the appropriate Driver Set** > **Driver Set Properties** > **Inspector and Statistics** > **Association Statistics**.
2. Select the server for which you want to run the association statistics.
3. The association count displays the previously computed result.

   Identity Console displays the association count for active, inactive, and system managed objects for all the drivers associated with the driver set.

   Identity Console considers groups and organization units as system managed objects. Identity Console considers an object inactive, if the `Login Disabled` attribute in the object is set to true and the object has not been modified within the last 120 days. All the remaining objects are considered as active managed objects.
4. Click ⟳ icon to obtain the updated results.

   When a driver is disabled on the server, Identity Console does not display the driver in the dashboard.

5. Click icon to export the system details and association count details for the drivers associated with the server.

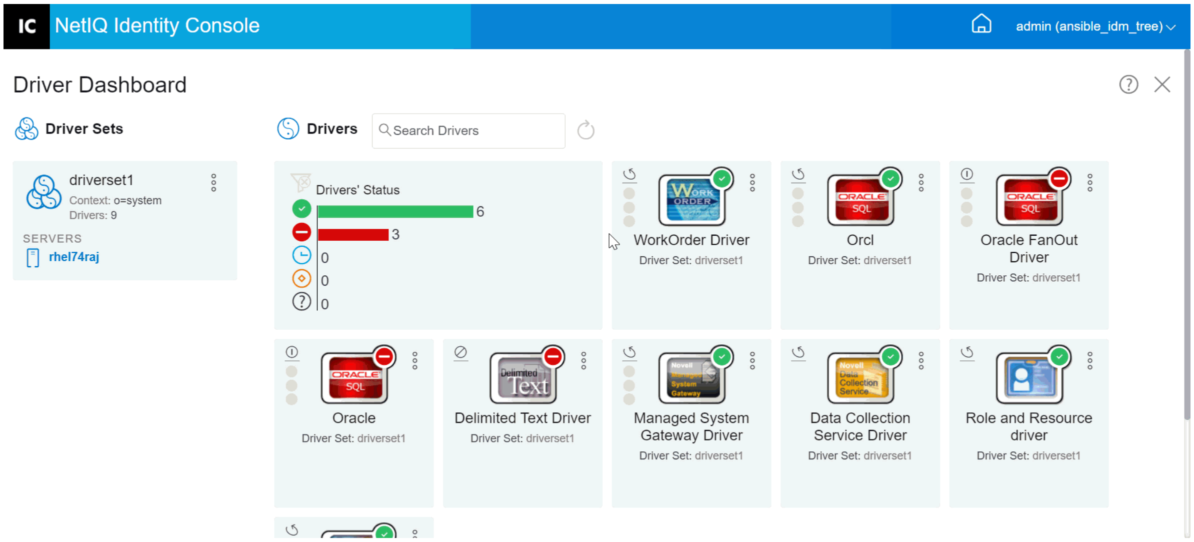
6. To export the objects associated with a specific driver, click next to the required objects and save the file.

NOTE: In case of Fan-Out drivers, only unique objects are exported. If an object is associated with multiple instances of a Fan-Out driver, Identity Console displays all the association counts in the dashboard. However, if you choose to export the objects in a file, Identity Console exports only the unique objects.

---

7. Click **Actions** and select the required option to organize the association count dashboard.

Figure 23-4 Managing Driver Set Statistics



24 Managing Driver Properties

This section provides information about the properties that are common to all drivers. This includes all properties (Named Password, Engine Control Values, Log Level, and so forth).

The activation info for a driver is displayed, that reminds an action for you to activate the expiry driver.

To modify the Driver's configuration, perform the following steps:

1. Click the **Drivers** tab from the Identity Console home screen.
2. Click the respective driver's tile to see the driver's configuration page.

   By default, the **Connection Parameters** page appears. The Driver Configuration options are divided into the following categories:

Connection Parameters

The connection parameters control whether the driver should be running locally or remotely.

- **Java:** Use this option to specify the name of the Java class that is instantiated for the shim component of the driver. This class can be located in the classes directory as a class file, or in the `lib` directory as a `.jar` file. Select this option to run the driver locally. You must also specify the Driver Object Passsword and Driver cache limit. You can set a new password by clicking the **Set Password** link.

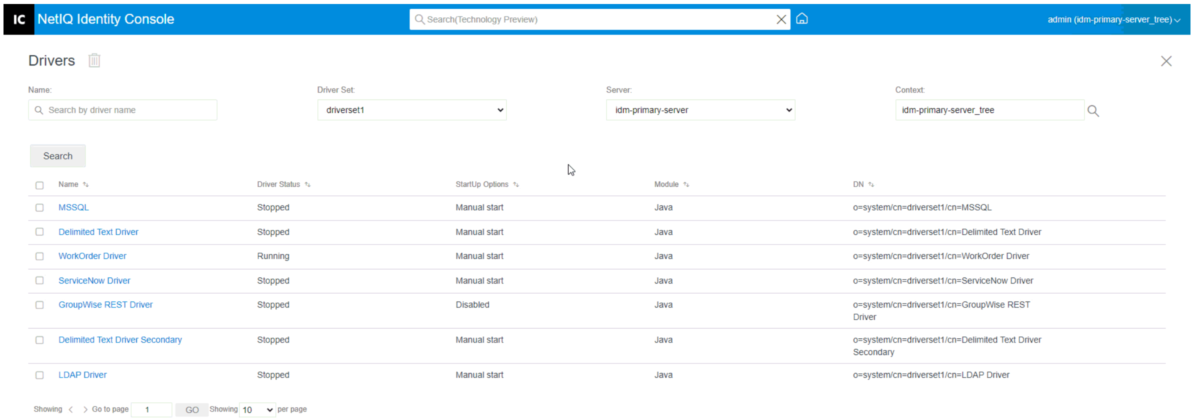
  For example, `com.microfocus.nds.dirxml.driver.scim.SCIMDriverShim`
- **Native:** This option is used to specify name of the `.dll` which is developed in native language (such as C++) for the driver. You must also specify the Driver Object Passsword and Driver cache limit. You can set a new password by clicking the **Set Password** link.

  For example, `addriver.dll`
- **Connect to Remote Loader:** This option is used when the driver is connecting remotely to the connected system. If this option is selected, you must specify the following sub-options:
  - **Remote Loader Connection Parameters**: Includes information of the Remote Loader environment details such as, Host Name, Connection Port, etc.

  - **Remote Loader Password**: The password for the Remote Loader.
  - **Driver Object Password**: Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. The Remote Loader uses this password to authenticate itself to the remote driver shim.
- **Authentication**: The Authentication parameters are used to authenticate the Identity Manager Engine and Remote Loader servers. Specify the following parameters:
  - **Authentication ID**: Specify a user application ID. This ID is used to pass Identity Vault subscription information to the application.
  - **Authentication Context**: Specify the IP address or name of the server the application shim should communicate with.
  - **Application Password**: Option to set the application authentication password.

Once done, click the icon to save the configuration.

Figure 24-1 Managing Connection Parameters



Name: Search by driver name
Driver Set: driverset1
Server: idm-primary-server
Context: idm-primary-server_tree

☐	Name	Driver Status	StartUp Options	Module	DN
☐	MSSQL	Stopped	Manual start	Java	o=system/cn=driverset1/cn=MSSQL
☐	Delimited Text Driver	Stopped	Manual start	Java	o=system/cn=driverset1/cn=Delimited Text Driver
☐	WorkOrder Driver	Running	Manual start	Java	o=system/cn=driverset1/cn=WorkOrder Driver
☐	ServiceNow Driver	Stopped	Manual start	Java	o=system/cn=driverset1/cn=ServiceNow Driver
☐	GroupWise REST Driver	Stopped	Disabled	Java	o=system/cn=driverset1/cn=GroupWise REST Driver
☐	Delimited Text Driver Secondary	Stopped	Manual start	Java	o=system/cn=driverset1/cn=Delimited Text Driver Secondary
☐	LDAP Driver	Stopped	Manual start	Java	o=system/cn=driverset1/cn=LDAP Driver

Go to page 1 Showing 10 per page

Driver Configuration

The driver configuration section lets you configure the driver-specific parameters, Engine Control Values, Global Configuration values etc. When you change the driver parameters, you tune the driver behavior to align with your network environment. This section is divided into the following categories:

- "Driver Parameters" on page 155
- "Global Configuration Values" on page 155
- "Engine Control Values" on page 155
- "Startup Options" on page 159
- "Named Password" on page 159
- "Security Equals" on page 159

- “Excluded Objects” on page 160
- “Managing Valued Attribute List” on page 160

Driver Parameters

The driver parameters are divided into Driver Settings, Subscriber Settings and Publisher Settings. These settings will be populated based on your driver’s configuration. For more information on the driver parameters, refer to the specific driver guide on the Identity Manager Drivers Documentation.

Once done, you can save the parameters by clicking the 📥. If you want to set the parameters to its default value, click ⟳ icon. To modify the driver configuration using the xml file, click the 📝 icon.

Global Configuration Values

Displays an ordered list of Global Configuration objects. The objects contain extension GCV definitions for the driver that Identity Manager loads at the time of driver starts. You can view or modify the objects under the **Global Configuration Values** tab using the XML editor. Click the 📥 icon to save the GCVs. To refresh the list of GCVs, click the ⟳ icon. To delete GCVs, select the appropriate GCV object and click the 🗑 icon.

Engine Control Values

The engine control values are a way that certain default behaviors of the Identity Manager engine can be changed. The values can be accessed only if a server is associated with the Driver Set object.

Option	Description
Subscriber channel retry interval in seconds	The Subscriber channel retry interval controls how frequently the Identity Manager engine retries the processing of a cached transaction after the application shim's Subscriber object returns a retry status.
Qualified form for DN-syntax attribute values	The qualified specification for DN-syntax attribute values controls whether values for DN-syntax attribute values are presented in unqualified slash form or qualified slash form. A True setting means the values are presented in qualified form.
Qualified form from rename events	The qualified form for rename events controls whether the new-name portion of rename events coming from the Identity Vault are presented to the Subscriber channel with type qualifiers. For example, CN=. A True setting means the names are presented in qualified form.
Maximum eDirectory replication wait time in seconds	This setting controls the maximum time that the Identity Manager engine waits for a particular change to replicate between the local replica and a remote replica. This affects only operations where the Identity Manager engine is required to contact a remote eDirectory server in the same tree to perform an operation and might need to wait until some change has replicated to or from the remote server before the operation can be completed (for example, object moves when the Identity Manager server does not hold the master replica of the moved object; file system rights operations for Users created from a template.)

Option	Description
Use non-compliant backwards-compatible mode for XSLT	This control sets the XSLT processor used by the Identity Manager engine to a backwards-compatible mode. The backward-compatible mode causes the XSLT processor to use one or more behaviors that are not XPath 1.0 and XSLT 1.0 standards-compliant. This is done for backward compatibility with existing DirXML style sheets that depend on the non-standard behaviors. For example, the behavior of the XPath “!=” operator when one operand is a node-set and the other operand is other than a node-set is incorrect in DirXML releases up to and including Identity Manager 2.0. This behavior has been corrected; however, the corrected behavior is disabled by default through this control in favor of backward compatibility with existing DirXML style sheets.
Maximum application objects to migrate at once	This control is used to limit the number of application objects that the Identity Manager engine requests from an application during a single query that is performed as part of a Migrate Objects from Application operation. If java.lang.OutOfMemoryError errors are encountered during a Migrate from Application operation, this number should be set lower than the default. The default is 50. **NOTE:** This control does not limit the number of application objects that can be migrated; it merely limits the batch size.
Set creatorsName on objects created in Identity Vault	This control is used by the Identity Manager engine to determine if the creatorsName attribute should be set to the DN of this driver on all objects created in the Identity Vault by this driver. Setting the creatorsName attribute allows for easily identifying objects created by this driver, but also carries a performance penalty. If not set, the creatorsName attribute defaults to the DN of the NCP Server object that is hosting the driver.
Write pending associations	This control determines whether the Identity Manager engine writes a pending association on an object during Subscriber channel processing. Writing a pending association confers little or no benefit but does incur a performance penalty. Nevertheless, the option exists to turn it on for backward compatibility.
Use password event values	This control determines the source of the value reported for the nspmDistributionPassword attribute for Subscriber channel Add and Modify events. Setting the control to False means that the current value of the nspmDistributionPassword is obtained and reported as the value of the attribute event. This means that only the current password value is available. This is the default behavior. Setting the control to True means that the value recorded with the eDirectory event is decrypted and is reported as the value of the attribute event. This means that both the old password value (if it exists) and the replacement password value at the time of the event are available. This is useful for synchronizing passwords to certain applications that require the old password to enable setting a new password.

Option	Description
Retry Out of Band events	This control determines whether the out-of-band sync events should be retried or not if the **retry** status for the out-of-band sync event is received. If the control is set to False, the out-of-band sync is not retried. If it is set to true, the out-of-band sync is retried till its successful.
Use Rhino ECMAScript engine	Determines whether the Identity Manager engine uses the Rhino ECMAScript engine. The engine uses Rhino as the default ECMAScript engine. This control is **true** by default, if you set this control to **false** engine uses Nashorm script.
Enable Subscriber Service Channel	Determines whether the Identity Manager engine processes the out of band queries on the Subscriber Service channel of the driver. Some common examples of these queries are code map refresh, data collection, and queries triggered from dxcmd. When this control is set to true, the channel separately processes these queries without interrupting the normal processing of events. Currently, this control is only available for use with the JDBC Fan-Out driver (enabled by default).
Enable password synchronization status reporting	This control determines whether the Identity Manager engine reports the status of Subscriber channel password change events. Reporting the status of Subscriber channel password change events allows applications such as the Identity Manager User Application to monitor the synchronization progress of a password change that should be synchronized to the connected application.
Combine values from template object with those from add operation	This value determines whether the Identity Manager engine combines like values from a creation template and an add operation when performing the add operation. Setting the value to True causes the template's multi-valued attribute values to be used in addition to the values for the same attribute that are specified in the add operation. Setting the value to False causes the values from the template to be ignored if there are values for the same attribute specified in the Add operation.
Allow event loopback from publisher to subscriber channel	This value determines whether the Identity Manager engine allows an event to loop from the driver’s Publisher channel to the Subscriber channel. Setting the value to False causes the Identity Manager engine to not allow events to loop back. Setting the value to True causes the Identity Manager engine to allow events to loop from the Publisher channel to the Subscriber channel.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Revert to calculated membership value behavior</b></td><td>This value determines the method used by the Identity Manager engine when performing read and search actions related to group membership.

Setting this value to False (the default setting) causes the Identity Manager engine, when reading or searching the Member and Group Member attributes of Identity Vault objects, to return only those values that are “static” values. Static values are objects that received group membership by direct assignment to the group rather than inherited assignment through a nested group.

Setting this value to True causes the Identity Manager engine to revert to the method used prior to Identity Manager 3.6. In pre-3.6 versions, the Identity Manager engine's search of the Member and Group Member attributes retrieved all “calculated” values. Calculated values include objects that are either 1) statically assigned membership or 2) dynamically assigned membership by virtue of the nested group hierarchy calculations used by eDirectory. A search of a Group Member attribute returns any objects that were directly assigned to the group or that were assigned membership through a nested group.</td></tr>
<tr><td><b>Maximum time to wait for driver shutdown in seconds</b></td><td>This setting controls the maximum time that the Identity Manager engine waits for the driver’s Publisher channel to shut down. If the driver does not shut down within the specified time interval, the Identity Manager engine terminates the driver.</td></tr>
<tr><td><b>Regular Expression escape meta-characters</b></td><td>This control determines the meta-characters that will be escaped while expanding the local variable when used in a regular expression context. All characters that need to be escaped must be added as a comma separated list for this control value.

If a meta-character is not present in the control value, then it will not be escaped during local variable expansion containing a regular expression.

While using this control, ensure the following:
- The value is not left empty. By default, it is populated with <b><i>$</i></b>. This character is required for local variable expansion.
- The value should be a valid comma(,) separated list, otherwise you will encounter errors during policy evaluation.
- To escape all meta-characters, specify "\,$,^,.,?,*,+,[,],(,),|" as a value.
- If a meta-character need not be escaped, remove that character from the value.
- To escape any meta character, specify the meta character followed by a back slash (\).</td></tr>
<tr><td><b>Ignore Entitlement Changes of other drivers</b></td><td>This control determines whether the Identity Manager engine ignores or processes entitlement changes of other drivers. The default value is True. This means that the driver automatically ignores the entitlement changes of other drivers. If this control is set to False, the entitlement changes of other drivers are cached and processed by this driver.</td></tr>
</table>

Option	Description
Allow Entitlement event loopback from cprs to subscriber channel	This control determines whether the Identity Manager engine allows an entitlement event that is generated by a CPRS assignment to loopback to the Subscriber channel of the driver. The default value is False. This means that the event is not looped back to the Subscriber channel. If this control is set to True, the event flows to the Subscriber channel of the driver.

Startup Options

The Startup Options allow you to set the driver state when the Identity Manager server is started.

- **Auto start**: The driver starts every time the Identity Manager server is started.
- **Manual**: The driver does not start when the Identity Manager server is started. The driver must be started using the Identity Console portal.
- **Disabled**: The driver has a cache file that stores all of the events. When the driver is set to Disabled, this file is deleted and no new events are stored in the file until the driver state is changed to Manual or Auto Start.

After setting the preferred startup option, click on 🖫 icon the save. To reset the startup option, click on ⟳ icon.

Named Password

Identity Manager allows you to securely store multiple passwords for a driver. This functionality is referred to as named passwords. Each different password is accessed by a key, or name.

You can add named passwords to a driver set or to individual drivers. Named passwords for a driver set are available to all drivers in the set. Named passwords for an individual driver are available only to that driver.

To use a named password in a driver policy, you refer to it by the name of the password, instead of using the actual password, and the Identity Manager engine sends the password to the driver. The method described in this section for storing and retrieving named passwords can be used with any driver without making changes to the driver shim.

To add a new named password, click the + icon. To remove an existing named password, click the 🗑 icon. To save your list, click 🖫 icon.

Security Equals

Use the Security Equals page to view or change the list of objects that the driver is explicitly security equivalent to. This object effectively has all rights of the listed objects.

You can add a new object in the security equals list by clicking the + icon. If you add or delete an object in the list, the system automatically adds or deletes this object in that object's "Security Equal to Me" property. You don't need to add the [Public] trustee or the parent containers of this object to the list, because this object is already implicitly security equivalent to them.

To remove an existing object from this list, click the 🗑 icon. To save your list, click ⤓ icon.

Excluded Objects

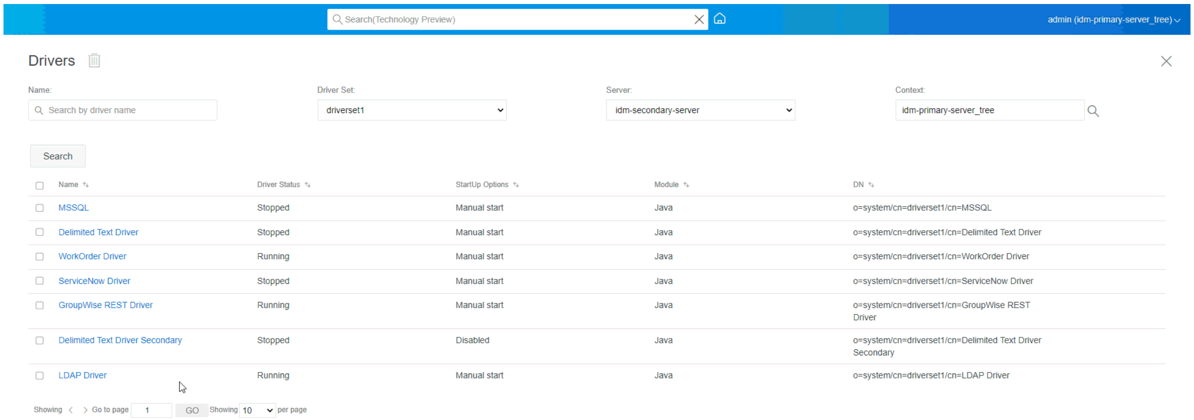
Use this option to create a list of objects that will not be replicated to the application. We recommend that you add all objects that represent an administrative role (for example, the Admin object) to this list. You can add a new object in this list by clicking the + icon. To remove an exiting object from this list, click the 🗑 icon. To save your list, click ⤓ icon.

Managing Valued Attribute List

To add attributes to the valued attribute list for a specific driver, perform the following steps:

1. In Identity Console, select the **Object Management** module.
2. Select **Dir-XML-Driver** type from the drop-down list and click the Search button.
3. Click the appropriate driver from the search list.
4. To add unvalued attribute(s) to the valued list of attributes, click the + icon next to the **Valued Attributes** and select the appropriate unvalued attributes from the list.
5. Once done, click **OK**.

***Figure 24-2** Managing Drivers Configuration*



Name: Search by driver name

Driver Set: driverset1

Server: idm-secondary-server

Context: idm-primary-server_tree

☐	Name	Driver Status	StartUp Options	Module	DN
☐	MSSQL	Stopped	Manual start	Java	o=system/cn=driverset1/cn=MSSQL
☐	Delimited Text Driver	Stopped	Manual start	Java	o=system/cn=driverset1/cn=Delimited Text Driver
☐	WorkOrder Driver	Running	Manual start	Java	o=system/cn=driverset1/cn=WorkOrder Driver
☐	ServiceNow Driver	Stopped	Manual start	Java	o=system/cn=driverset1/cn=ServiceNow Driver
☐	GroupWise REST Driver	Running	Manual start	Java	o=system/cn=driverset1/cn=GroupWise REST Driver
☐	Delimited Text Driver Secondary	Stopped	Disabled	Java	o=system/cn=driverset1/cn=Delimited Text Driver Secondary
☐	LDAP Driver	Running	Manual start	Java	o=system/cn=driverset1/cn=LDAP Driver

Data Transformation and Synchronization

This section is divided into the following categories:

- "Data Synchronization View" on page 161
- "Class Attribute Filters" on page 163

- “ECMA Script” on page 164
- “Reciprocal Attribute Mapping” on page 164

Data Synchronization View

The driver’s overview page is divided into the following categories:

- “Filter” on page 161
- “All Policies” on page 161
- “Migrate Data Into the Identity Vault” on page 162
- “Migrate Data from the Identity Vault” on page 162
- “Synchronize Objects” on page 162
- “Tracing DirXML Script” on page 162

Filter

Filters exist on the driver and enable you to specify which classes and attributes an application can send to and receive from the Identity Vault. If you want a specific class to pass through for the Metadirectory engine to process, you should add the class to the filter on the appropriate channel. You also can filter objects by a specific attribute value you define.

To add classes and attributes you want included for synchronization and modify the driver filter, click **Filter** on the Publisher or Subscriber channel.

NOTE: The graphical depiction of the Overview shows two separate objects for the driver filter on the Publisher and Subscriber channels. Although there are two objects shown, the same filter is used for both channels.

All Policies

By default, the All Policies page appears. You can import an existing policy in the container by clicking the 📥 icon. You can also remove any policy which is not required. To select a trace level for your driver, click 🖥 icon. You can move the policies up and down in the list by using the ↑ and ↓ icons.

NOTE: Adding and deploying new policies for drivers are not supported with Identity Console. We recommend you to use iManager and Identity Designer for adding and deploying new policies.

Migrate Data Into the Identity Vault

Using this task, you can define the criteria Identity Manager uses to migrate objects from an application into the Identity Vault. When you migrate an object, the Metadirectory engine applies all of the Matching, Placement, and Create policies, as well as the Publisher filter, to the object. Objects are migrated into the Identity Vault using the order you specify in the Class list. You can perform the following tasks using this option:

1. **Add Class and Attributes**: To add or remove classes and attributes you want to migrate, click the icon. Then select the class and its respective attributes you want to add. After you select the class and attributes, click **Add** to save your changes.
2. **Edit Attribute Value**: To change the migration attribute value you specified when editing the list, click the Edit Attribute icon.
3. **Re-order the Class List**: Use the ↑ and ↓ buttons to change the order of the classes in the list. Objects are migrated into the Identity Vault using the order you specify in the Class list.
4. **Refresh:** Click the ⟳ icon to refresh the list.

Migrate Data from the Identity Vault

Using the **Export** tab, you can select containers or objects you want to migrate from the Identity Vault to an application. When you migrate an object, the Metadirectory engine applies all Matching, Create, and Placement policies, as well as the Subscriber filter, to the object.

To migrate objects or containers from the Identity Vault to another application, click the + icon. Browse to and select the object you want to migrate, then click **OK** to add the object to the migration list. To remove objects from the migration list, click the icon.

After you have finished selecting the objects you want to migrate, click ▷ to begin migration. The migration progress will be displayed on your screen. If you want to stop the migration, click on the ⊡ button.

Synchronize Objects

The synchronize operation looks for objects that have been modified and synchronizes them. Either you can select **Examine all objects** to start the synchronization immediately. Alternatively, you can set a date/time to start the synchronization.

Tracing DirXML Script

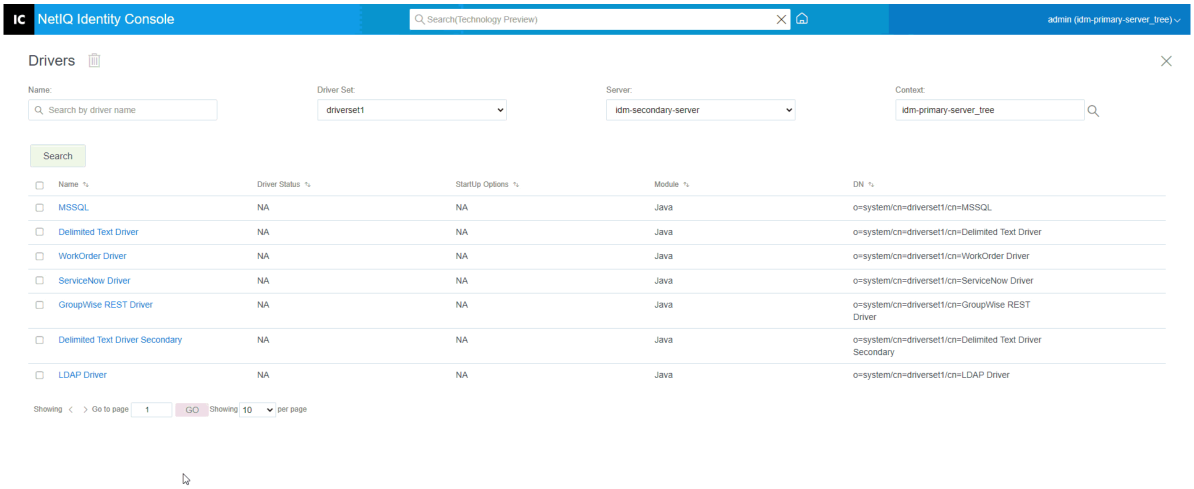
The Tracing DirXML Scripts option allows you to select a trace level for a driver. It also applies trace settings to all Publisher and Subscriber Channels. The following DirXML script tracing options are available to select:

- All DirXML Script Tracing On
- All DirXML Script Tracing Off

- DirXML Script Rule Tracing On
- DirXML Script Rule Tracing Off

Click to save your changes.

Figure 24-3 Managing Data Synchronization of Drivers



Name:

Driver Set: driverset1

Server: idm-secondary-server

Context: idm-primary-server_tree

☐	Name	Driver Status	StartUp Options	Module	DN
☐	MSSQL	NA	NA	Java	o=system/cn=driverset1/cn=MSSQL
☐	Delimited Text Driver	NA	NA	Java	o=system/cn=driverset1/cn=Delimited Text Driver
☐	WorkOrder Driver	NA	NA	Java	o=system/cn=driverset1/cn=WorkOrder Driver
☐	ServiceNow Driver	NA	NA	Java	o=system/cn=driverset1/cn=ServiceNow Driver
☐	GroupWise REST Driver	NA	NA	Java	o=system/cn=driverset1/cn=GroupWise REST Driver
☐	Delimited Text Driver Secondary	NA	NA	Java	o=system/cn=driverset1/cn=Delimited Text Driver Secondary
☐	LDAP Driver	NA	NA	Java	o=system/cn=driverset1/cn=LDAP Driver

Showing 1 · Showing 10 per page

Class Attribute Filters

The class attribute filters enable you to specify which classes and attributes an application can send to and receive from the Identity Vault. If you want a specific class to pass through for the Metadirectory engine to process, you should add the class to the filter on the appropriate channel. You also have the ability to filter objects by a specific attribute value you define. Using this option, you can perform the following actions:

- **Set Template**: Use this option to set the default options for all attributes that are added to the filter. Click the icon next to the Class Attribute Filter label.
- **Add a New Class**: Add a new class by clicking the icon.
- **Add a New Attribute**: Add a new attribute by clicking the icon.
- **Copy Filter From**: This option allows you to copy a filter from another driver. Click the icon to copy filter.
- **Edit XML**: Edit the class and attribute filter settings using the Edit XML file icon.
- **Delete Class or Attributes**: Delete any class or attribute by clicking on the icon next to the respective class or attribute.

You can set the following options for a class and attribute value on both Publisher and Subscriber channels:

- Synchronize

- Ignore
- Notify
- Reset

Merge Authority

If an attribute is not being synchronized in either channel, no merging occurs.

If an attribute is being synchronized in one channel and not the other, then all existing values on the destination for that channel are removed and replaced with the values from the source for that channel. If the source has multiple values and the destination can only accommodate a single value, then only one of the values is used on the destination side.

If an attribute is being synchronized in both channels and both sides can accommodate only a single value, the connected application acquires the values stored in the Identity Vault unless there will be no value in the Identity Vault. In this scenario, the Identity Vault acquires the values from the connected application.

If an attribute is being synchronized in both channels and only one side can accommodate multiple values, the value from the single-valued channel is added to the multi-valued channel if it is not already there. If there is no value on the single side, you can choose the value to add to the single side. You can set the following options for Merge Authority:

- Default
- Identity Vault
- Application
- None

Click ⍗ to save your changes.

ECMA Script

Displays an ordered list of ECMAScript resource files. The files contain the extension functions for the driver that Identity Manager loads at the time of driver starts. You can import additional files by clicking ⤓, remove existing files by clicking 🗑, or change the order the files that are executed. You can also move the scripts up and down in the list. You can save the ECMA Script list by clicking the ⍗ icon.

Reciprocal Attribute Mapping

Reciprocal attribute mappings let you create and manage the backlinks, or references, between objects. For example, the Group object includes a Members attribute that references all User objects that belong to that group. Similarly, each User object includes a Group Membership attribute that references the Group objects of which that user is a member. In order for the Metadirectory engine to keep the Group object > Members attribute synchronized with the User object > Group Membership attribute for all Group objects and User objects in the Identity Vault, these attributes must be linked. The links between object attributes are known as reciprocal attribute mappings.

Using this module, you can perform the following actions:

- “Creating Custom Reciprocal Attribute Mappings” on page 165
- “Adding a New Reciprocal Attribute Mapping” on page 165
- “Removing a Reciprocal Attribute Mapping” on page 166
- “Removing an Attribute from the Reciprocal Mapping List” on page 166
- “Reordering Mapped Attributes” on page 166
- “Removing the Custom Reciprocal Attribute Mapping” on page 166
- “Editing Reciprocal Attribute XML” on page 166

Creating Custom Reciprocal Attribute Mappings

This section applies only if the Reciprocal Attribute Mapping page displays **The driver does not contain custom reciprocal attribute mappings. Click on the '+' icon above to create basic reciprocal attribute mappings** prompt.

1. Click the + icon to create a new custom reciprocal attribute mapping list.
2. The driver's default attribute mappings are displayed. You can now add mappings, modify the existing mappings, or delete mappings.

Adding a New Reciprocal Attribute Mapping

When you create a reciprocal attribute mapping, you must first add one of the attributes to the reciprocal mapping list.

1. Click the + icon next to the Actions drop-down menu.
2. In the new attribute entry, select the desired attribute from the drop-down list.
3. Specify the details of the reciprocal mapping:
   - 3a **Source Class**: Specifies the class name to which the attribute in the mapping list is associated. For example, if you placed the Group Membership attribute in the reciprocal mapping list, the associated Source Class is User.
   - 3b **Destination Class**: Specifies the class name associated with the attribute to which you want to create a reciprocal mapping. For example, if you placed the Group Membership attribute in the reciprocal mapping list, the associated Destination Class is Group.
   - 3c **Reciprocal Attribute**: Specifies the attribute name to which you want to create a reciprocal mapping.
4. If you want to map the attribute to another reciprocal attribute, click the + icon to the right of the attribute name.

   A new section for the attribute is added at the end of the attribute's list. Select the source class, destination class, and reciprocal attribute.

Removing a Reciprocal Attribute Mapping

To remove a reciprocal attribute mapping:

1. Select the check box for the reciprocal attribute mapping that you want to delete in front of the **Source Class**.
2. Click the 🗑 icon next to the attribute drop-down list.

Removing an Attribute from the Reciprocal Mapping List

To remove an attribute from the reciprocal mapping list:

1. Select the attribute you want to remove by selecting check box in front of the attribute.
2. Click the 🗑 icon next to the **Actions** drop-down list.

Reordering Mapped Attributes

The attribute mappings are resolved in the order listed, from top to bottom. You can move the mapped attributes up or down in the list to ensure that they are resolved in the correct order. In general, you should list specific mappings first followed by more general mappings. For example, a mapping for the Member attribute on a Group object should be listed before a mapping for the Member attribute on any objects (the <Any Class> option).

Select the check box in front of the mapped attribute you want to move, then click ↑ to move the attribute up or click ↓ to move it down.

Removing the Custom Reciprocal Attribute Mapping

You can delete the custom attribute mappings you've created. This results in the Metadirectory engine using the default attribute mappings for the driver.

To remove a custom reciprocal attribute mapping, click the 🗑 icon at the top of the screen.

Editing Reciprocal Attribute XML

If desired, you can directly edit the XML for a reciprocal attribute. To do so, click Edit XML icon ✎ on the Custom Reciprocal Attribute Mapping page. This opens a basic XML editor that lets you modify the XML. When you finish, click OK or Cancel to close the XML editor.

Advanced Settings

The advanced settings are divided into the following categories:

- "Managing Entitlements" on page 167
- "Managing Objects Mapping Table" on page 167
- "Managing Jobs for Drivers" on page 167

Managing Entitlements

The Entitlements page contains a table showing all of the entitlements that are currently defined within the selected driver (listed with its fully distinguished name). The following actions are permitted on this page:

- **Edit in XML**: To edit the entitlements in XML file, select the entitlement from the list and click the ✎ icon. Then check the **Enable XML Editing** box.
- **Delete**: To delete an Entitlement, click the box to the left of the entitlement name, then click the 🗑 icon. You see a message stating that the operation cannot be undone and asking if you are sure you want to delete the selected entitlement. Click **OK** to delete the entitlement, or click **Cancel** to stop the operation. You can click multiple boxes to delete multiple entitlements, or click the upper left box to delete all of the entitlements.

Managing Objects Mapping Table

Identity Manager policies use mapping tables to map a set of values to another set of corresponding values. When you install the entitlement package, the policies of this package are added to the driver Startup policy set. The driver executes these policies only once when the driver is started. For more information, see Mapping Table Objects in the *NetIQ Identity Manager Driver Administration Guide*.

Using the Objects Mapping Table, you can perform the following actions:

- **Modify an existing Mapping:** To modify an existing objects mapping table, click on the mapping from the list and perform the following actions on the next screen:
    - Add a new column.

      Specify a value for the column, then select whether the value is case sensitive, case insensitive, or numeric.
    - Add a new row and specify a value for the row.
    - Click the ⤓ icon.
- **Delete Mapping**: To remove a mapping from the list, select the appropriate mapping from the list and click the 🗑 icon.
- **Edit in XML**: To edit a mapping in XML file, click on the mapping from the list and select ✎ icon. Then, check the **Enable XML Editing** box.

Managing Jobs for Drivers

Identity Console enables you to schedule events using the Jobs option for all the individual drivers.

The Job Scheduler page contains the job's name, whether the job is enabled or disabled, when it is scheduled to run, and the job description. Click the job name to bring up the Job page. Click the enable/disable icon under the Enabled column to enable or disable the job. Click the job's description to see the job's full description.

The Jobs tab contains a table showing the existing job objects for the selected driver, which is listed with its fully distinguished name in the driver entry.

The Job Scheduler page allows you to perform the following tasks:

- **Create the Job**: Click + icon to create a new job.

  In the **New Job** pop-up, to create a new job perform the following steps:

  1. Specify the job name.
  2. Select the job type.
  3. Click the ⌄ icon and select the server where you want to run the job, from the available list of servers. Otherwise, specify a server name and then select the server.
  4. Click the **Create** button.

- **Start the Job**: Select a job by clicking the box to the left of the job, then click ▷ icon.
- **Stop the Job**: Select a job by clicking the box to the left of the job, then click ⊡ icon.
- **Enable the Job**: Select a job by clicking the box to the left of the job, then click ✓ icon.
- **Disable the Job**: Select a job by clicking the box to the left of the job, then click ⊗ icon.
- **Get Status**: Select a job by clicking the box to the left of the job, then click ⓘ icon.
- **Delete the Job**: Select a job by clicking the box to the left of the job, then click 🗑 icon.

Click a job to access the **Job Property** page. Here you can set up how you want the job to run.

General: Shows the Java class name of the job. Use this page to enable or disable the job, delete the job after it runs, select the server or servers where this job should run, specify the email server, and give the job a different display name and description.

Schedule: Allows you set when you want to run the job. Specify the Start job at to set the time, and whether to run the job daily, weekly, monthly, yearly. You can also customize when you want to run the job, or you can choose to enable the toggle to run the job manually.

Scope: Allows you to define the objects that this job applies to. An object can be a container, a dynamic group, a group, or a leaf object. Click Add to select the object that you want this job to apply to. You can use the Browse button to select an object, then click OK. To remove an object from the scope list, select a scope object by clicking the box to the left of the DN object, then click Remove.

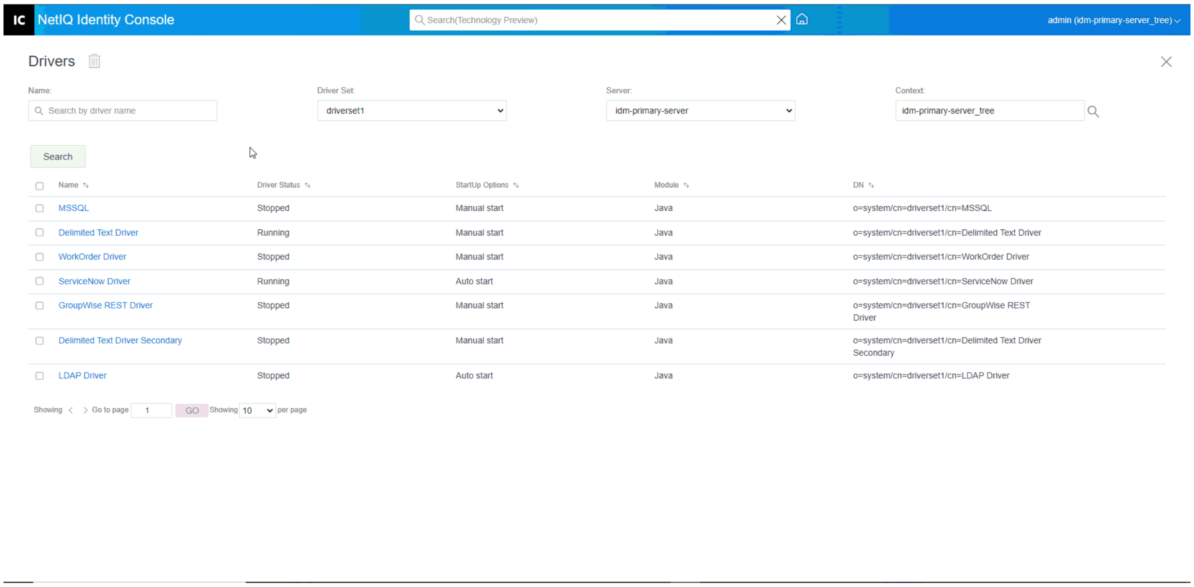
When an object is added, select it to display more options. If you select a group object, you have the option to apply the job to the group's members, or to the group only. If you select a container object, you have the option to apply the job to all descendants in that container, to all the children in the container, or to the container only.

Parameters: Allows you to add additional parameters to the job and to view the parameters as they are presently set up. These parameters change, depending on the type of job selected.

Results: Allows you to define what you want to do with the job results. The Results page is divided into two parts: Intermediate Result and Final Result, with the following results allowed: Success, Warning, Error, and Aborted. To the right of the Results column is the Action column. Clicking the Action column allows you to set how you want to be notified for each result. Actions include sending an audit result or sending an email when the result completes. If you do not select an option, no action is taken for the result.

In the **Trace** tab, you can configure trace for a specific driver. For more information, see “Configuring Trace Level” on page 170

***Figure 24-4** Managing Advanced Settings*


IC NetIQ Identity Console
Search(Technology Preview)
admin (idm-primary-server_tree)
Drivers
Search
Showing
Go to page
GO
per page

Name: Search by driver name
Driver Set: driverset1
Server: idm-primary-server
Context: idm-primary-server_tree

☐	Name	Driver Status	StartUp Options	Module	DN
☐	MSSQL	Stopped	Manual start	Java	o=system/cn=driverset1/cn=MSSQL
☐	Delimited Text Driver	Running	Manual start	Java	o=system/cn=driverset1/cn=Delimited Text Driver
☐	WorkOrder Driver	Stopped	Manual start	Java	o=system/cn=driverset1/cn=WorkOrder Driver
☐	ServiceNow Driver	Running	Auto start	Java	o=system/cn=driverset1/cn=ServiceNow Driver
☐	GroupWise REST Driver	Stopped	Manual start	Java	o=system/cn=driverset1/cn=GroupWise REST Driver
☐	Delimited Text Driver Secondary	Stopped	Manual start	Java	o=system/cn=driverset1/cn=Delimited Text Driver Secondary
☐	LDAP Driver	Stopped	Auto start	Java	o=system/cn=driverset1/cn=LDAP Driver

Go to page 1, Showing 10 per page

Configuring the Log and Trace Levels of Drivers

To configure log and trace for your drivers, select the **Drivers** > **Log & Trace Configuration** tab from the Identity Console main page. This section is divided into the following categories:

- “Configuring Log Level” on page 169
- “Configuring Trace Level” on page 170

Configuring Log Level

Each driver has a log level field where you can define the level of errors that should be tracked. The level you indicate here determines which messages are available to the logs. By default, the log level is set to track error messages. (This also includes fatal messages.) To track additional message types, change the log level. To configure the log level, select the **Log & Trace Configuration** > **Log Level** tab. The following table describes the log level settings:

Option	Description
Use log settings from the Driver Set	If this is selected, the driver logs events based on the log settings of the Driver Set object.
Turn off logging to Driver Set, Subscriber and Publisher logs	Turns all logging off for this driver on the Driver Set object, Subscriber channel, and the Publisher channel.
Maximum number of entries in the log (50-500)	Number of entries in the log. The default value is 50.

Option	Description
Log Levels	The following log levels are available to select: - **Log errors**: Logs just errors - Log errors and warnings: Logs errors and warnings - **Log specific events**: Logs the events that are selected. Selecting this option enables the following list of events: - **Metadirectory Engine Events** - **Status Events** - **Operation Events** - **Transformation Events** - **Credential Provisioning Events** - **Only update the last log time**: Updates the last log time. - **Logging Off**: Turns logging off for the driver.

Configuring Trace Level

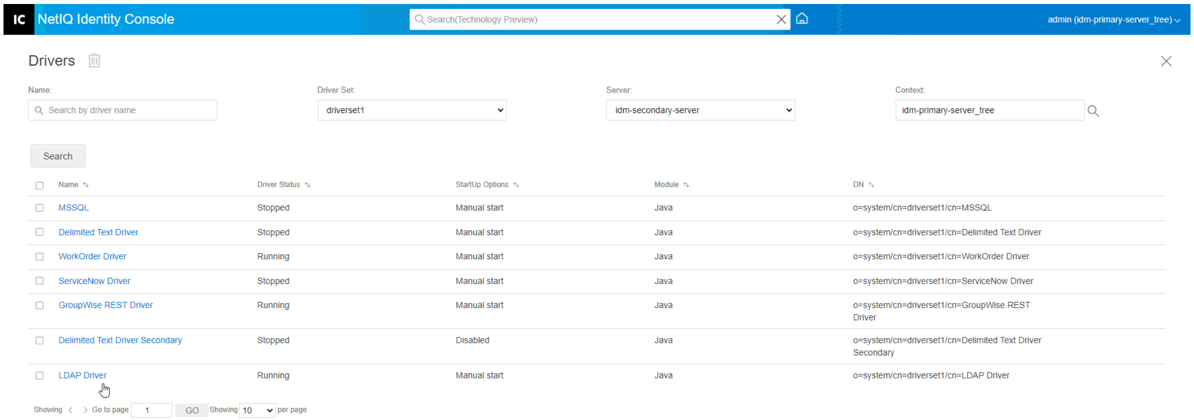
You can configure trace for a specific driver. Depending on the trace level specified for a driver, trace displays driver-related events when the engine processes the events. The driver trace level affects only the driver or driver set where trace is set. If you are using the Remote Loader, the Remote Loader trace file is set directly on the Remote Loader and contains only the driver shim trace.

To configure trace for a driver, select the **Log & Trace Configuration** > **Trace** tab. The following table describes the trace settings:

Parameter	Driver
Trace level	As the driver trace level increases, the amount of information displayed in Trace increases. Trace level one shows errors, but not the cause of the errors. If you want to see password synchronization information, set the trace level to five. If you select **Use setting from Driver Set**, the value is taken from the driver set.
Trace file	Specify a file name and location of where the Identity Manager information is written for the selected driver. If you select **Use setting from Driver Set**, the value is taken from the driver set.
Trace name	The driver trace messages are pre-pended with the value entered instead of the driver name. Use if the driver name is very long.
Trace file encoding	The trace file uses the system’s default encoding. You can specify another encoding if desired.

Parameter	Driver
Trace file size limit	Allows you to set a limit for the Java trace file. If you set the file size to unlimited, the file grows in size until there is no disk space left. **NOTE:** If the file size limit is specified the trace file is created in multiple files. Identity Manager automatically divides the maximum file size by ten and creates ten separate files. The combined size of these files equals the maximum trace file size. If you select **Use setting from Driver Set**, the value is taken from the driver set.

Figure 24-5 *Managing Log and Trace Levels of Drivers*


IC NetIQ Identity Console
Search(Technology Preview)
admin (idm-primary-server_tree)
Drivers
Search
Showing
Go to page
GO
per page

Name: Search by driver name

Driver Set: driverset1

Server: idm-secondary-server

Context: idm-primary-server_tree

☐	Name	Driver Status	StartUp Options	Module	DN
☐	MSSQL	Stopped	Manual start	Java	o=system/cn=driverset1/cn=MSSQL
☐	Delimited Text Driver	Stopped	Manual start	Java	o=system/cn=driverset1/cn=Delimited Text Driver
☐	WorkOrder Driver	Running	Manual start	Java	o=system/cn=driverset1/cn=WorkOrder Driver
☐	ServiceNow Driver	Stopped	Manual start	Java	o=system/cn=driverset1/cn=ServiceNow Driver
☐	GroupWise REST Driver	Running	Manual start	Java	o=system/cn=driverset1/cn=GroupWise REST Driver
☐	Delimited Text Driver Secondary	Stopped	Disabled	Java	o=system/cn=driverset1/cn=Delimited Text Driver Secondary
☐	LDAP Driver	Running	Manual start	Java	o=system/cn=driverset1/cn=LDAP Driver

Go to page 1 · Showing 10 per page

Inspecting Drivers

You can use the Driver Inspector to view detailed information about the objects associated with a driver. This section is divided into the following categories:

- “Driver Inspector” on page 172
- “Driver Cache Inspector” on page 173
- “Out of Band Sync Cache Inspector” on page 173
- “Driver Manifest” on page 174
- “Monitoring Driver’s Health” on page 174

Driver Inspector

To view the objects associated with a driver:

1. In Identity Console, Select **Drivers** > **Inspector** > **Driver Inspector** tab.
2. In the **Driver** field, specify the fully distinguished name of the driver that you want to inspect, or click the browse icon to browse to and select the desired driver.
3. After you have selected the driver to inspect, click **OK** to display the Driver Inspector page.

   The page displays information about the objects associated with the selected driver. You can perform any of the following actions:

   - **Delete:** Removes the association between the driver and an object. Select the check box in front of the object you no longer want associated with the driver, click the 🗑 icon, then click **OK** to confirm the deletion.
   - **Refresh:** Select the refresh ↻ icon this option to re-read all of the objects associated with the driver and refresh the information.
   - **Show:** Select the number of associations to display per page. You can select a predefined number (25, 50, or 100) or specify another number of your choice. The default is 10 associations per page. If there are more associations than the number displayed, you can use the arrow buttons to display the next and previous pages of associations.
   - **Actions:** Perform actions on the objects associated with the driver. Click **Actions**, then select one of the following options:
     - **Show All Associations:** Displays all objects associated with the driver.
     - **Filter for Disabled Associations:** Displays all objects associated with the driver that have a Disabled state.
     - **Filter for Manual Associations:** Displays all objects associated with the driver that have a Manual state.
     - **Filter for Migrate Associations:** Displays all objects associated with the driver that have a Migrate state.
     - **Filter for Pending Associations:** Displays all objects associated with the driver that have a Pending state.
     - **Filter for Processed Associations:** Displays all objects associated with the driver that have a Processed state.
     - **Filter for Undefined Associations:** Displays all objects associated with the driver that have an Undefined state.
     - **Association Summary:** Displays the state of all objects associated with the driver.
   - **Object DN:** Displays the DN of the associated objects.
   - **State:** Displays the association state of the object.
   - **Object ID:** Displays the value of the association.

Driver Cache Inspector

You can view the transactions in a driver’s cache file using Identity Console. The **Driver Cache Inspector** displays information about the cache file, including a list of the events to be processed by the driver.

1. In Identity Console, Select **Drivers** > **Inspector** > **Driver Cache Inspector** tab.
2. In the **Driver** field, specify the fully distinguished name of the driver whose cache you want to inspect, or click the browse icon to browse to and select the desired driver, then click **OK** to display the Driver Cache Inspector page.

   A driver’s cache file can be read only when the driver is not running. If the driver is stopped, the Driver Cache Inspector page displays the cache. If the driver is running, the page displays a `Driver not stopped, cache cannot be read` note in place of the cache entries. To stop the driver, click the ⏹ button; the cache is then read and displayed.

   - **Driver’s cache on Server:** Lists the server that contains this instance of the cache file. If the driver is running on multiple servers, you can select another server in the list to view the driver’s cache file for that server.
   - **Start/Stop Driver icons:** Displays the current state of the driver and allows you to start or stop the driver. The cache can be read only while the driver is stopped.
   - **Delete:** Select entries in the cache, then click the 🗑 icon to remove them from the cache file.
   - **Actions:** Allows you to perform actions on the entries in the cache file. Click **Actions** to expand the menu, then select one of the following options:
     - **Clear all Cached Events:** Enables you to clear all cached events.
     - **Cache Summary:** Summarizes all of the events stored in the cache file.

Viewing the Connected System Details for Drivers

To view the connected system details for a specific driver, perform the following actions:

1. In Identity Console, click the **Object Inspector** module.
2. Browse and select the specific driver object for which you want to display the connected systems.
3. All the connected system details for the selected driver object will be displayed on your computer.

Out of Band Sync Cache Inspector

To view events in the Out of Band Sync cache:

1. In Identity Console, Select **Drivers** > **Inspector** > **Out of Band Sync Cache Inspector** tab.
2. In the **Driver** field, specify the fully distinguished name of the driver whose cache you want to inspect, or click the browse icon to browse to and select the desired driver, then click **OK**.

A driver’s cache file can be read only when the driver is not running. If the driver is stopped, the Driver Cache Inspector page displays the cache. If the driver is running, the page displays a `Driver not stopped, cache cannot be read` note in place of the cache entries. To stop the driver, click the ⏹ button; the cache is then read and displayed.

- **Cache filename:** Displays the filename of the cache.
- **Driver’s cache on Server:** Lists the server that contains this instance of the cache file. If the driver is running on multiple servers, you can select another server in the list to view the driver’s cache file for that server.
- **Start/Stop Driver icons:** Displays the current state of the driver and allows you to start or stop the driver. The cache can be read only while the driver is stopped.
- **Delete:** Select entries in the cache, then click the 🗑 icon to remove them from the cache file.
- **Actions:** Allows you to perform actions on the entries in the cache file. Click **Actions** to expand the menu, then select one of the following options:
  - **Cache Summary:** Summarizes all of the events stored in the cache file.
  - **Clear All Cached Events:** Enables you to clear all cached events.

Driver Manifest

The Driver Manifest is like a resume for the driver. It states what the driver supports, and includes a few configuration settings. The Driver Manifest should be provided by the driver developer. A network administrator usually does not need to edit the Driver Manifest. In case if the administrator wants to edit the driver manifest, can do so by selecting **Drivers** > **Inspector** > **Driver Manifest** > **Enable XML Editing** option.

Monitoring Driver’s Health

Driver health monitoring allows you to view a driver’s current state of health as green, yellow, or red, and to define the actions to perform in response to each of these health states.

You create the conditions (criteria) that determine each of the health states, and you also define the actions you performed whenever the driver’s health state changes. For example, if the driver’s health changes from a green state to a yellow state, you can perform such actions as restarting the driver, shutting down the driver, and sending an email to the person designated to resolve issues with the driver.

Using this module, you can perform the following tasks:

- “Modifying the Driver’s Health Conditions” on page 175
- “Modifying the Driver’s Health Actions” on page 177
- “Creating a Custom State” on page 178
- “Modifying a Custom State” on page 179

Modifying the Driver's Health Conditions

You control the conditions that determine each health state. The green state is intended to represent a healthy driver, and a red state is intended to represent an unhealthy driver.

The conditions for the green state are evaluated first. If the driver fails to meet the green conditions, the yellow conditions are evaluated. If the driver fails to meet the yellow conditions, the driver is automatically assigned a red health state.

To modify the conditions for a state:

1. In Identity Console, open the Driver Health Configuration page for a driver whose conditions you want to modify:
   - **1a** Open the Identity Console home page.
   - **1b** Select **Drivers** > **Click on the appropriate Driver from the list** > **Inspector** > **Driver Health Configuration**.
2. Click the tab for the state (Green or Yellow) you want to modify.

   The tab displays the current conditions for the health state. Conditions are organized into groups, and logical operators, either AND or OR, are used to combine each condition and each group. Consider the following example for the green state:

   ```
   GROUP1
   Condition1 and
   Condition2
   Or
   GROUP2
   Condition1 and
   Condition2 and
   Condition3
   ```

   In the example, the driver is assigned a green state if either the GROUP1 conditions or the GROUP2 conditions evaluate as true. If neither group of conditions is true, then the conditions for the yellow state are evaluated.

   The conditions that can be evaluated are:

   - **Driver State:** Running, stopped, starting, not running, or shutting down. For example, one of the default conditions for the green health state is that the driver is running.
   - **Driver in Cache Overflow:** The state of the cache used for holding driver transactions. If the driver is in cache overflow, all available cache has been used. For example, the default condition for the green health state is that the Driver in Cache Overflow condition is false and the default for the yellow health state is that the Driver in Cache Overflow condition is true.
   - **Newest:** The age of the newest transaction in the cache.
   - **Oldest:** The age of the oldest transaction in the cache.
   - **Total Size:** The size of the cache.
   - **Unprocessed Size:** The size of all unprocessed transactions in the cache.
   - **Unprocessed Transactions:** The number of unprocessed transactions in the cache. You can specify all transactions types or specific transaction types (such as adds, removes, or renames).

- **Transactions History:** The number of transactions processed at various points in the Subscriber or Publisher channel over a given period of time. This condition uses multiple elements in the following format:

  <*transaction type*> <*transaction location and time period* > <*relational operator*> <*transaction number*>.

  - <*transaction type*>: Specifies the type of transaction being evaluated. This can be all transactions, adds, removes, renames, and so forth.
  - <*transaction location and time period*>: Specifies the place in the Subscriber or Publisher channel and the time period being evaluated. For example, you might evaluate the total number of transactions processed as Publisher reported events over the last 48 hours. By default, transaction history data is kept for two weeks, which means that you cannot specify a time period greater than two weeks unless you change the default Transaction Data Duration setting.
  - <*relational operator*>: Specifies that the identified transactions must be equal to, not equal to, less than, less than or equal to, greater than, or greater than or equal to the <transaction number>.
  - <*transaction number*>: Specifies the number of transactions being used in the evaluation.

  The following provides an example of a Transactions History condition:

  ```
  <number of adds> <as publisher commands> <over the last 10 minutes>
  <is less than> <1000>
  ```

- **Available History:** The amount of transaction history data that is available for evaluation. The primary purpose for this condition is to ensure that a Transactions History condition does not cause the current state to fail because it does not have enough transaction history data collected for the time period being evaluated.

  For example, assume that you want to use the Transactions History condition to evaluate the number of adds as Publisher commands over the last 48 hours (the example shown in the Transactions History section above). However, you don't want the condition to fail if there is not yet 48 hours worth of data, which can be the case after the initial setup of the driver's health configuration or if the driver's server restarts (because transaction history data is kept in memory). Therefore, you create condition groups similar to the following:

  ```
  Group1 Available History <is less than> <48 hours> or Group2
  Available History <is greater than or equal to> <48 hours> and
  Transactions History <number of adds> <as publisher commands> <over
  the last 48 hours> <is less than> <1000>
  ```

  The state evaluates to true if either condition group is true, meaning that a) there is less than 48 hours of data, or b) there is at least 48 hours of data and the number of adds as Publisher commands over the last 48 hours is less than 1000.

  The state evaluates to false if both conditions evaluate to false, meaning that a) there is at least 48 hours of data and b) the number of adds as publisher commands over the last 48 hours is greater than 1000.

3 Modify the criteria as desired.

- To add a new group, click the + icon next to the **Condition Groups**.

    - To add a condition, click the + icon next to the logical operators (AND/OR). Alternatively, you can also click on **Add new condition** link.
    - To reorder condition groups or individual conditions, select the check box next to the group or condition you want to move, then click the arrow buttons to move it up and down. You can also use the arrow buttons to move a condition from one group to another.

4. Once done, save your changes by clicking the **Save** button.
5. If you want to change the actions associated with the conditions you have set, continue with "Modifying the Driver's Health Actions" on page 177.

Modifying the Driver's Health Actions

You can determine the actions that you want performed when the driver health state changes. For example, if the state changes from green to yellow, you can shut down or restart the driver, generate an event, or start a workflow. Or, if the state changes from yellow to green, any actions associated with the green state are performed.

A health state's actions are performed only once each time the conditions are met; as long as the state remains true, the actions are not repeated. If the state changes because its conditions are no longer met, the actions are performed again the next time the conditions are met.

1. In Identity Console, open the Driver Health Configuration page for a driver whose actions you want to modify:
    - 1a Open the Identity Console home page.
    - 1b Select **Drivers** > **Click the appropriate Driver from the list** > **Inspector** > **Driver Health Configuration**.
2. Click the **Green**, **Yellow**, or **Red** tab for the state whose actions you want to modify.
3. Click the plus (+) icon next to the **Actions** heading to add an action, then select the type of action you want:
    - **Start Driver:** Starts the driver.
    - **Stop Driver:** Stops the driver.
    - **Restart Driver:** Stops and then starts the driver.
    - **Clear Driver Cache:** Removes all transactions, including unprocessed transactions, from the cache.
    - **Send Email:** Sends an email to one or more recipients. The template you want to use in the email message body must already exist. To include the driver name, server name, and current health state information in the email, add the `$Driver$`, `$Server$`, and `$HealthState$` tokens to the email template and then include the tokens in the message text. For example:

      ```
      The current health state of the $Driver$ driver running on $Server$
      is $HealthState$.
      ```

      IMPORTANT: To send emails to multiple users, separate each email address only with a comma (,). Do not use semi-colon instead of comma.
    - **Write Trace Message:** Writes a message to the Driver Health job's log file or the driver set's log file if the trace file is not configured on the Driver Health job.

- **Generate Event:** Generates an event that can be used by Audit and Sentinel.
- **Execute ECMAScript:** Executes an existing ECMAScript.

  For information about how to construct ECMA scripts, refer to Using ECMAScript in Policies in the *NetIQ Identity Manager - Using Designer to Create Policies*.
- **Start Workflow:** Starts a provisioning workflow.
- **On Error:** If an action fails, instructs what to do with the remaining actions, the current health state, and the Driver Health job.
  - **Affect actions by:** You can continue to execute the remaining actions, stop execution of the remaining actions, or default to the current setting. The current setting applies only if you have multiple On Error actions and you set the Affect actions by option in one of the preceding On Error actions.
  - **Affect state by:** You can save the current state, reject the current state, or default to the current setting. Saving the state causes the state's conditions to continue to evaluate as true. Rejecting the state causes the state's conditions to evaluate as false. The current setting applies only if you have multiple On Error actions and you set the Affect state by option in one of the preceding On Error actions.
  - **Affect Driver Health Job by:** You can continue to run the job, abort and disable the job, or default to the current setting. Continuing to run the job causes the job to finish evaluating the conditions to determine the driver's health state and perform any actions associated with the state. Aborting and disabling the job stops the job's current activity and shuts down the job; the job does not run again until you enable it. The current setting applies only if you have multiple On Error actions and you set the Affect Driver Health Job by setting in one of the preceding On Error actions.

4. Once done, save your changes by clicking the **Save** button.

Creating a Custom State

You can create one or more custom states to perform actions independent of the driver's current health state (green, yellow, red). If a custom state's conditions are met, its actions are performed regardless of the current health state.

As with the green, yellow, and red health states, a custom state's actions are performed only once each time the conditions are met; as long as the state remains true, the actions are not repeated. If the state changes because its conditions are no longer met, the actions are performed again the next time the conditions are met.

1. In Identity Console, open the Driver Health Configuration page for a driver for which you want to create a custom state:

   1a Open the Identity Console home page.

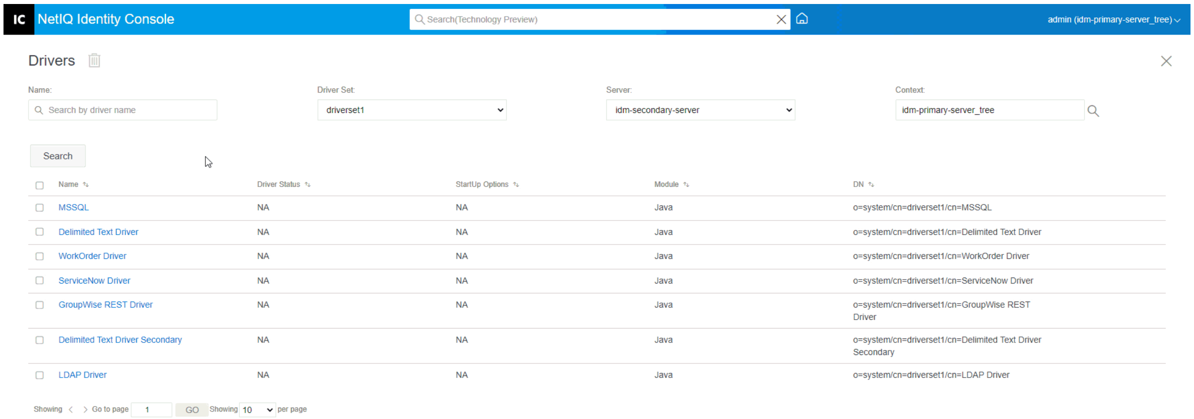
   1b Select **Drivers** > **Click on the appropriate Driver from the list** > **Inspector** > **Driver Health Configuration**.
2. Click the + icon next to the driver's health status icons (green, yellow and red)
3. Follow the instructions in "Modifying the Driver's Health Conditions" on page 175 and "Modifying the Driver's Health Actions" on page 177 to define the custom state's conditions and actions.

Modifying a Custom State

To modify custom states, perform the following steps:

1. In Identity Console, open the Driver Health Configuration page for a driver for which you want to create a custom state:
   - **1a** Open the Identity Console home page.
   - **1b** Select **Drivers** > **Click on the appropriate Driver from the list** > **Inspector** > **Driver Health Configuration**.
2. Click the ✎ icon next to the driver's health status icons (green, yellow and red)
3. Follow the instructions in "Modifying the Driver's Health Conditions" on page 175 and "Modifying the Driver's Health Actions" on page 177 to define the custom state's conditions and actions.

Figure 24-6 *Managing Driver Inspectors*



Name: Search by driver name

Driver Set: driverset1

Server: idm-secondary-server

Context: idm-primary-server_tree

☐	Name	Driver Status	StartUp Options	Module	DN
☐	MSSQL	NA	NA	Java	o=system/cn=driverset1/cn=MSSQL
☐	Delimited Text Driver	NA	NA	Java	o=system/cn=driverset1/cn=Delimited Text Driver
☐	WorkOrder Driver	NA	NA	Java	o=system/cn=driverset1/cn=WorkOrder Driver
☐	ServiceNow Driver	NA	NA	Java	o=system/cn=driverset1/cn=ServiceNow Driver
☐	GroupWise REST Driver	NA	NA	Java	o=system/cn=driverset1/cn=GroupWise REST Driver
☐	Delimited Text Driver Secondary	NA	NA	Java	o=system/cn=driverset1/cn=Delimited Text Driver Secondary
☐	LDAP Driver	NA	NA	Java	o=system/cn=driverset1/cn=LDAP Driver

Showing < > Go to page 1 GO Showing 10 per page

25

Managing Driver Set Statistics

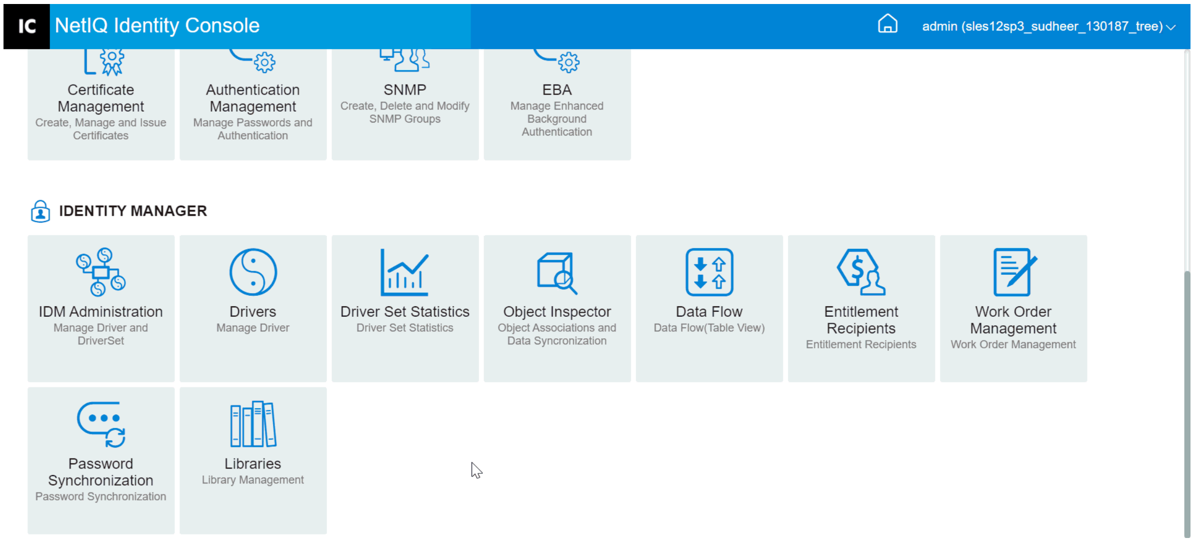
You can use Identity Console portal to view a variety of statistics for a single driver or for an entire driver set. This includes statistics such as the cache file size, the size of the unprocessed transactions in the cache file, the oldest and newest transactions, and the total number of unprocessed transactions by category (add, remove, modify, and so forth). To view the driver set statistics:

1. In Identity Console, open the **Driver Set Statistics** page.
2. Select the appropriate server from the drop-down.

   A page appears that allows you to view the statistics for all of the drivers contained in the driver set.

   - To refresh the statistics, click ↻ icon.
   - To close the statistics for a driver, click the ✕ button in the upper right corner of the driver's statistics window.
   - To open the statistics for all drivers, click **Actions** > **Show All**.
   - To collapse the list of unprocessed transactions for a driver, click the ˄ button located above the list. To collapse the list of unprocessed transactions for all drivers, click **Actions** > **Collapse All Transactions**.
   - To expand the list of transactions, click the ˅ button. To expand the list of unprocessed transactions for all drivers, click **Actions** > **Expand All Transactions**.
   - To close the statistics dashboard of disabled drivers, click **Actions**, then select **Close Disabled Drivers**.

Figure 25-1 Managing Driver Set Statistics



26 Inspecting Identity Manager Objects

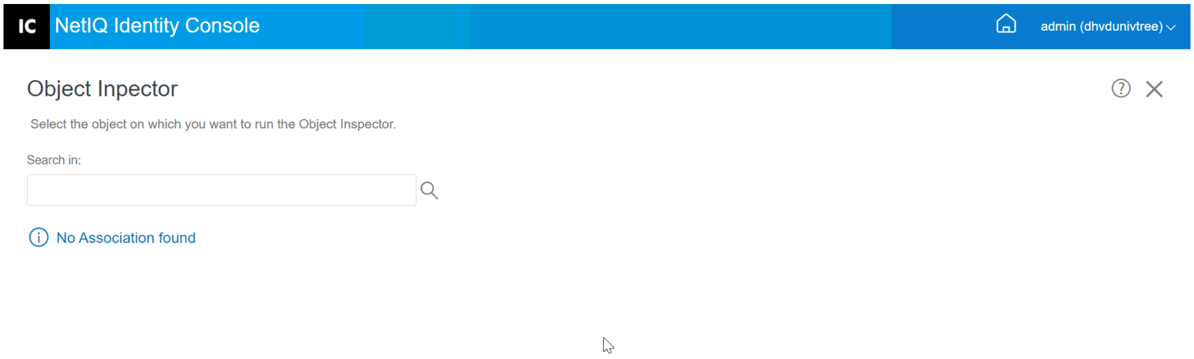
You can use the Object Inspector to view detailed information about how an object participates in Identity Manager relationships. These relationships include the connected systems that are associated with the object, how data flows between the Identity Vault and the connected systems, the attribute values that are currently stored in the Identity Vault and on the connected systems, the connected system driver configurations, and so forth.

To inspect Identity Manager objects, click on the **Object Inspector** option from the Identity Console main page. Specify the fully distinguished name of the object that you want to inspect, or click the browse icon to browse to and select the desired object.

The Connected Systems section lists each of the connected systems with which the object is associated. Using the **Object Inspector** page, you can perform the following actions:

- **Adding an Association**: To add a new association with a connected system, click the + icon. Browse and select the **Integration Driver Object** and specify the **Associated Object ID**.
- **Deleting an Association**: To delete an association with a connected system, select the check box to the left of the association and click the 🗑 icon. To delete all associations, select the check box beneath the Delete column, then click the 🗑 icon.

Figure 26-1 *Inspecting Identity Manager Objects*



Select the object on which you want to run the Object Inspector.

No Association found

27 Managing Data Flow

Data flow illustrates the Publisher and Subscriber channels for several drivers in a single view. You can view and update data ownership for all drivers using this option.

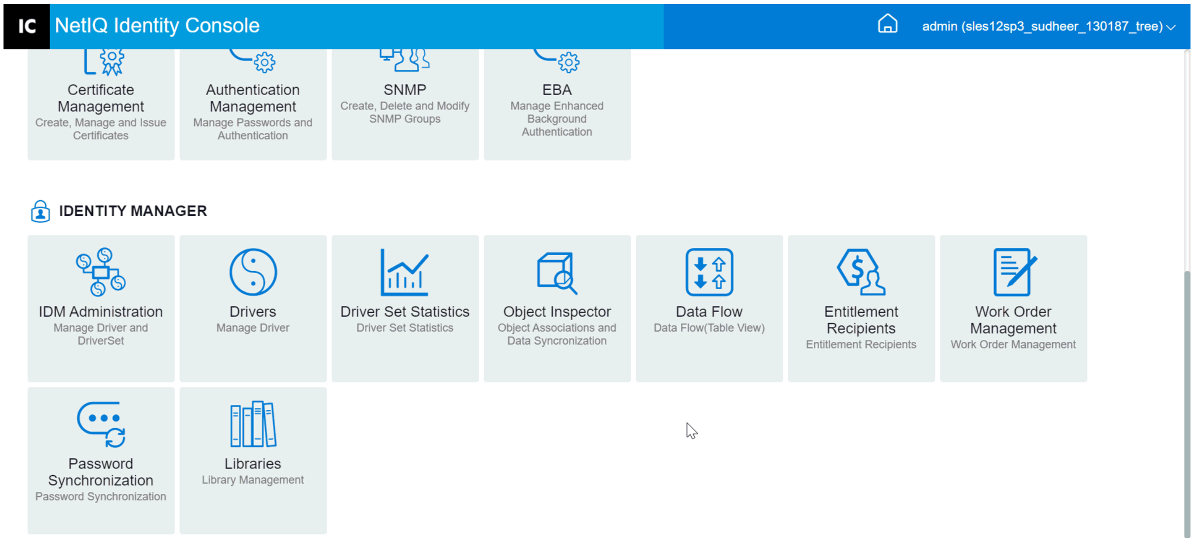
To access the table view of data flow, click on the **Data Flow (Table View)** module from the Identity Console main page. Then, browse and select the appropriate container to display the list of the drivers.

To manage the data ownership of individual drivers, perform the following steps:

1. Each driver has two buttons to manage the data flow over the Publisher and the Subscriber channels. The button on the left hand side manages the data flow over the Publisher channel and the button on the right hand side manages the data flow over the Subscriber channel.
   - 1a **Synchronize**: Select this option to synchronize the specific attribute. The icon will be changed to ↑ on the Publisher channel and to ↓ on the subscriber channel after selecting this option.
   - 1b **Ignore**: Select this option to stop synchronizing the specific attribute. The icon will be changed to ⊘ after selecting this option.
   - 1c **Notify**: Select this option to get notified for any changes made to a specific attribute. But the change will not be synchronized automatically. The icon will be changed to 🔔 after selecting this option.
   - 1d **Reset**: Select this option to reset the attribute value to the value specified by the other channel. The icon will be changed to ⟳ after selecting this option.

   NOTE: You can set this value on either the Publisher or the Subscriber channel. You can not set this value on both the channels simultaneously.

Figure 27-1 Managing Data Flow



28

Managing Entitlement Recipients

Entitlement references and results are maintained on objects that have had an entitlement granted on them or revoked from them. Entitlement references and results contain information about whether the entitlement is currently granted or revoked on that object. Entitlement recipients are any objects that contain references to an entitlement.

Entitlement References

To view the entitlement references and results, click on the **Entitlement Recipients** option from the Identity Console main page and select Entitlement Reference. Then fill in the Fully Distinguished Name of the object that is a `DirXML-EntitlementRecipient`. You can click the Object Selector 🔍 button to select the object.

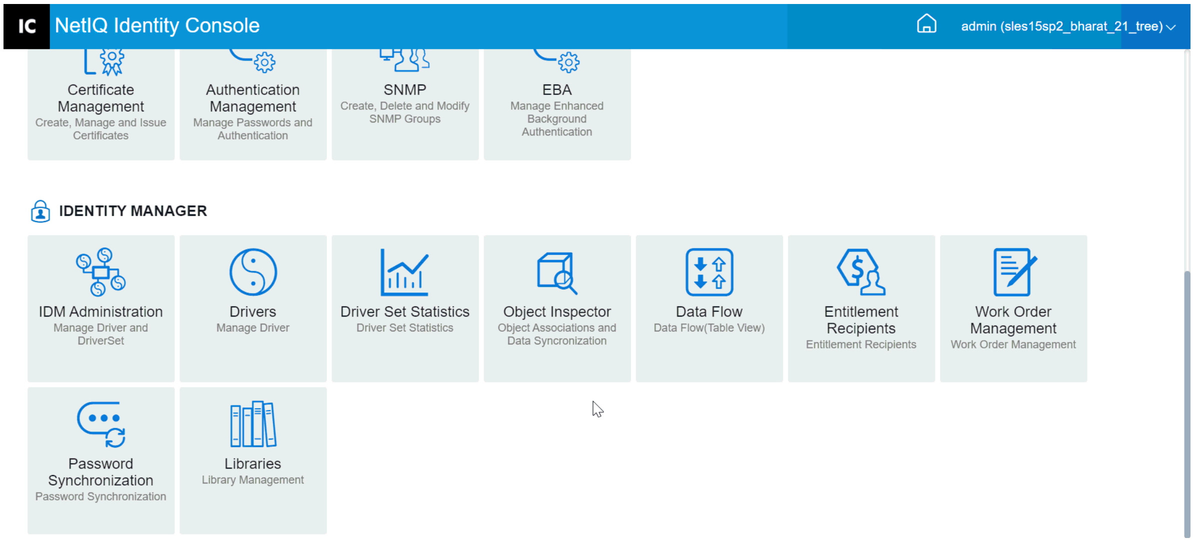
Entitlement Results

The Identity Console Entitlement Results table lists the entitlement results that are associated with the selected object. To view the associated entitlement, select the Entitlement DN. To view the entitlement's results in XML format, select the corresponding Result ID.

- **Entitlement Results Column Headings**: The column headings include the entitlement's fully distinguished name, its present state of being granted or revoked, where the results came from (source), the status of the result, any messages that came with the result, the result's time stamp, and the result's identification.
    - **Entitlement DN**: Click the Entitlement fully distinguished name of the object to bring up the Modify Object page. This page allows you to view how eDirectory attributes have been assigned to the object. You can also use this page to modify the object's attributes. The number of categories shown on the Modify Object page depends on the object selected.
    - **State**: Displays whether the entitlement was granted or revoked. If the plug-in finds any other value in the XML stream, it displays that value directly.
    - **Message**: Any messages that the the DirXML shim associated with the results status. The information that is stored in the <msg></msg> portion of the XML results file. Click the Results ID entry to see the full details of the result in an XML Viewer page.
    - **Timestamp**: The time when the entitlement engine processed and wrote the result. Click the Results ID entry to see the full details of the result in an XML Viewer page.
    - **Result ID**: Click the Results ID entry to see the full details of the result in an XML Viewer page. When you are finished viewing the results, click Close.

To delete an entitlement results entry, click the check box to the left of the entitlement results entry and select **Delete**.

Figure 28-1 Managing Entitlement Recipients



29 Managing Work Orders

Identity Manager drivers can create work orders as a result of events processed by the drivers. For example, if you use a Human Resource driver (SAP HR, PeopleSoft, and so forth), you can have the driver generate a work order whenever a new user is added.

You can use Identity Console to create and manage work orders created for various drivers that support this specific functionality.

Creating a New Work Order

To create a new work order, perform the following steps:

1. Click the **Work Order** option from the Identity Console landing page.
2. Click the + icon to create a new work order.
3. Specify a name for the work order, then click **OK**.

   The name is used for the WorkOrder object’s name in the Identity Vault.
4. Fill in the following fields:

   Status: The status of a new work order can be either **Pending** or **On Hold**. Normally, work order status is **Pending**. You can stop a work order by selecting **On Hold**. After a work order has been processed, the resulting work order status appears in this field.

   Due Date: You can choose to have the driver do the work order immediately or schedule the work order. To schedule a due date, click the calendar icon. Use the calendar to choose the date. Use the arrows to select the month, year, and time.

   Repeat Work Order: Select this option to have the work order processed multiple times. Specify the time interval by choosing the number of weeks, days, hours, or minutes before the work order is to be repeated. The work order stops repeating on the delete date unless it is manually deleted, edited, or the driver sends back an error message.

   Delete Date: Use the calendar control to select a date to delete work orders that have been configured. Work orders with an error status are not deleted unless you select **Delete Work Order Even if the Work Order Has an Error**.

   Dependent Work Orders: When you create a new work order, you can make it dependent on one or more work orders. Click 🔍 to browse for and select dependent work orders. To remove a work order from the list, select the work order, then click 🗑.

   Type: Use this field to specify a work order type. The driver does not change this attribute. The attribute is passed through to the WorkToDo object when the work order is processed.

Work Order Number: A unique work order number. This value can be assigned by a corporate work order system other than NetIQ eDirectory, such as a work order database.

Contact Information: Contact information for the person responsible for the work order.

Work Order Processing Log: After a work order has been processed, the driver logs the results of the work order, including the status, in this field. This allows you to check the work order's current status and identify any problems the driver encountered while attempting to configure the work order.

The work order's status attribute remains pending until the work order is processed. The work order is processed when the due date has expired. The driver reports the processing results by setting the status attribute to Configured, Warning, or Error. If the work order is On Hold, it ignores the work order.

- **Pending:** The driver is waiting for the due date to complete the work order.
- **Configured:** The work order has been successfully processed.
- **Error:** The driver was unable to perform the work order.
- **Warning:** There is a warning regarding the work order. For example, if the work order has a dependent work order with a later due date, the driver sends a warning.

Description: The work order description.

Work Order Content: The data in this field is used by the driver’s rules to process the work order. For example, it might be the XML that the Command Transformation uses to process the work order.

Deleting An Existing Work Order

To delete an existing work order, perform the following steps:

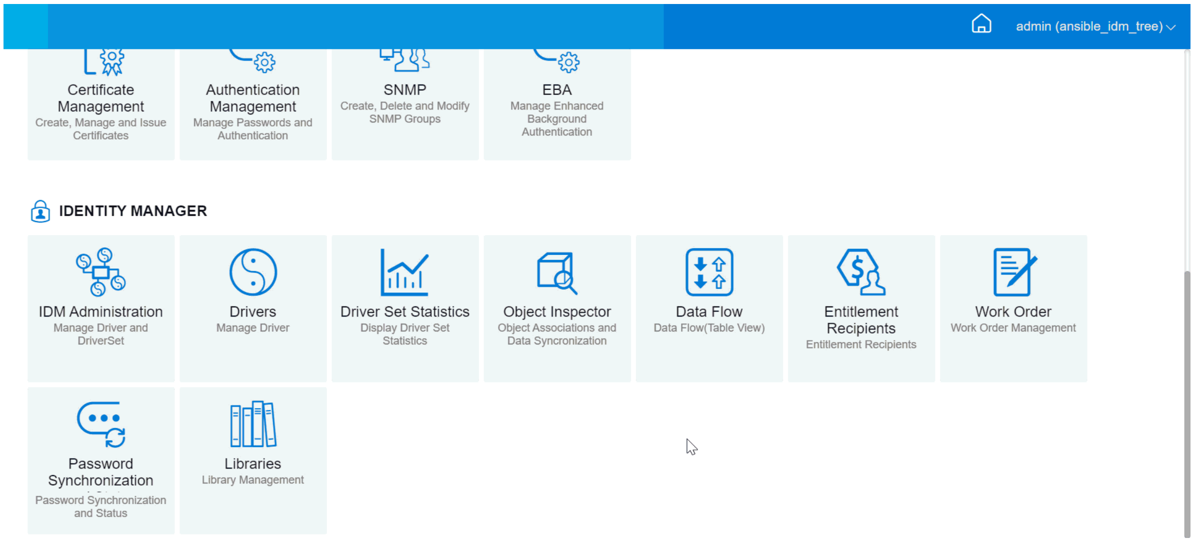
1. Click the **Work Order** option from the Identity Console landing page.
2. Select the work order that you want to delete.
3. Click the 🗑 icon.

Filtering the Work Order List

To filter out the list of work orders, perform the following steps:

1. Click the **Work Order** option from the Identity Console landing page.
2. Click **Actions** under Work Order Management.
3. From the drop-down menu, select the filter type:
    - **Show all:** All work orders associated with the driver are listed.
    - **Configured:** Only configured work orders associated with the driver are listed.
    - **Error:** Only work orders with an error status are listed.
    - **On Hold:** Work orders that have been manually placed on hold are listed.
    - **Pending:** Work orders that are not yet due are listed.

Figure 29-1 Managing Work Orders


admin (ansible_idm_tree)
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
IDENTITY MANAGER
IDM Administration
Manage Driver and DriverSet
Drivers
Manage Driver
Driver Set Statistics
Display Driver Set Statistics
Object Inspector
Object Associations and Data Syncronization
Data Flow
Data Flow(Table View)
Entitlement Recipients
Entitlement Recipients
Work Order
Work Order Management
Password Synchronization
Password Synchronization and Status
Libraries
Library Management

30 Managing Password Status and Synchronization

You can verify the password synchronization and password status of individual drivers using the Identity Console portal. To verify, select the **Password Synchronization** module from the Identity Console main page.

You can perform the following actions using this module:

- "Checking Password Synchronization Status" on page 193
- "Verifying Password Synchronization Settings" on page 194

Checking Password Synchronization Status

You can determine whether the Distribution password for a specific user is the same as the password in the connected system. Perform the following steps to check the password synchronization status:

1. In Identity Console, select **Password Synchronization** > **Password Status**.
2. Browse and select a user for which you want to check the password status.
3. The following password statuses can be seen:
    - Passwords are synchronized.
    - Passwords are NOT synchronized.
    - The password status is unknown, because the connected system cannot be contacted to request a password check.
    - An error has occurred.

NOTE: To see more details about each of the above statuses, you must mouse-over the status under the **Password Status** column.

The Password Status task causes the driver to perform a Check Object Password action. Not all drivers support password check. Those that do must contain a password-check capability in the driver's manifest. Identity Console does not allow password check operations to be sent to drivers that do not contain this capability in the manifest.

The Check Object Password action checks the Distribution password. If the Distribution password is not being updated, Check Object Password might report that passwords are not synchronized.

The Distribution password is not updated if either of the following occurs:

- You are using the synchronization method using NDS Password to Synchronize or Using Universal Password to Synchronize. For more information, see "Creating a Password Policy with Custom Settings" on page 112.

NOTE: The Password Status action checks the NDS Password instead of the Universal password for Identity Vault. Therefore, if the user's password policy does not specify to synchronize the NDS password with the Universal password, the passwords are always reported as being not synchronized. In fact, the Distribution password and the password on the connected system might be in sync, but Check Password Status won't be accurate unless both the NDS password and the Distribution password are synchronized with the Universal password.

Verifying Password Synchronization Settings

Password Synchronization lets you synchronize passwords across connected systems using Identity Manager. To view your Password Synchronization settings for connected systems, select the appropriate driver set from the drop-down.

By using Password Synchronization, you can set up connected systems to do the following:

- Publish passwords to Identity Manager.
- Subscribe to passwords from Identity Manager or other connected systems.
- Enforce Password Policies on connected systems.
- Send notification emails.

Perform the following steps to check the password synchronization settings:

1. In Identity Console, select **Password Synchronization** > **Password Synchronization** from the main page.
2. Select the driver set that contains the driver whose settings you want to check.
3. Click the name of the driver from the list.

   NOTE: The settings that are enabled and disabled vary depending on the driver. Only those settings for features supported by the driver are available.

4. Verify that the settings are configured properly.

   Identity Manager accepts passwords (Publisher Channel): If this option is enabled, Identity Manager allows passwords to flow from the connected system into the Identity Vault. Disabling this option means that no `<password>` elements are allowed to flow to Identity Manager. They are stripped out of the XML by a password synchronization policy on the Publisher channel.

   This setting applies to user passwords that are provided by the connected system itself, and password values that are created by a policy on the Publisher channel.

   If this option is enabled but the Distribution Password option below it is disabled, a `<password>` value coming from the connected system is written directly to the Universal password in the Identity Vault. If the user’s password policy does not enable Universal Password, the password is written to the NDS password.

   Use Distribution Password for password synchronization: This setting is available only if the **Identity Manager accepts passwords (Publisher Channel)** setting is enabled.

   If this option is enabled, a password value coming from the connected system is written to the Distribution password. The Distribution password is reversible, which means that it can be retrieved from the Identity Vault data store for password synchronization. It is used by Identity

Manager for bidirectional password synchronization with connected systems. For Identity Manager to distribute passwords from this system to other systems, this option must be enabled.

Accept password only if it complies with user's Password Policy: This setting is available only if the **Use Distribution Password for password synchronization** setting is enabled.

If this option is selected, Identity Manager does not write a password from this connected system to the Distribution password in the Identity Vault or publish it to connected systems unless the password complies with the user's password policy.

If a password does not comply, enable the **Reset the user's password to the Distribution Password** setting to reset the user's password on the connected system. This allows you to enforce the password policy on the connected system as well as in your Identity Vault. If you do not select this option, user passwords can become out-of-sync on connected systems. However, you need to consider the connected system's password policies when deciding whether to use this option. Some connected systems might not allow the reset because they don't allow you to repeat passwords.

By using the **Notify the user of password synchronization failure via email setting**, you can inform users when a password fails to be set or reset. Notification is especially helpful for this option. If the user changes to a password that is allowed by the connected system but rejected by Identity Manager because of the password policy, the user won't know that the password has been reset until the user receives a notification or tries to log in to the connected system with the old password.

Always accept password; ignore Password Policies: This setting is available only if the **Use Distribution Password for password synchronization** setting is enabled.

If you select this option, Identity Manager does not enforce the user's password policy for this connected system. Identity Manager writes the password from this connected system to the Distribution password in the Identity Vault and distributes it to other connected systems regardless of password policy compliance.

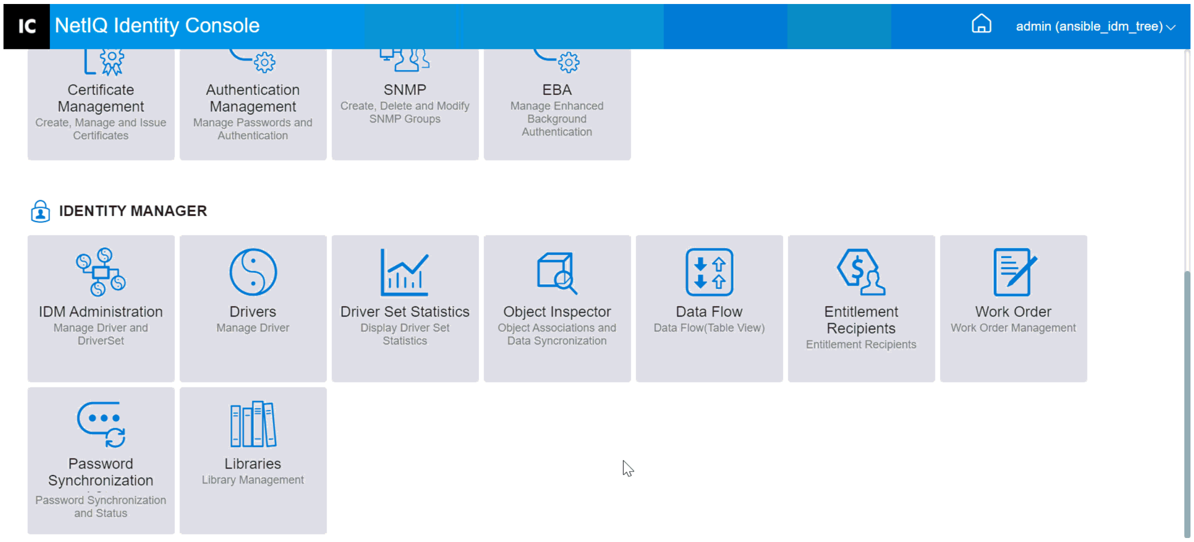
Application accepts passwords (Subscriber Channel): If you enable this option, the driver sends passwords from the Identity Vault to this connected system. This also means that if a user changes the password on a different connected system that is publishing passwords to the Distribution password in the Identity Vault, the password is changed on this connected system.

By default, the Distribution password is the same as the Universal password in the Identity Vault, so changes to the Universal password made in the Identity Vault are also sent to the connected system.

Notify the user of password synchronization failure via email: If you enable this option, email is sent to the user if a password is not synchronized, set, or reset. The email that is sent to the user is based on an email template. This template is provided by the Password Synchronization application. However, for the template to work, you must customize it and specify an email server to send the notification messages. For instructions, see Configuring E-Mail Notification in the *NetIQ Identity Manager Password Management Guide*.

5. When you are finished, click **Save** to save your changes. The settings are saved as Global Configuration Values.

Figure 30-1 *Managing Password Synchronization*



31

Managing Libraries

Library objects store multiple policies and other resources that are shared by one or more drivers. A library object can be created in a driver set object or any eDirectory container. Multiple libraries can exist in an eDirectory tree. Drivers can refer to any library in the tree as long as the server that is running the driver holds a Read/Write or Master replica of the library object.

Style sheets, policies, rules, and other resource objects can be stored in a library and be referenced by one or more drivers.

Using the Library Management module, you can perform the following tasks:

- "Viewing and Deleting an Existing Library" on page 197
- "Viewing and Deleting Objects from Library" on page 197

Viewing and Deleting an Existing Library

To view and delete an existing library, perform the following steps:

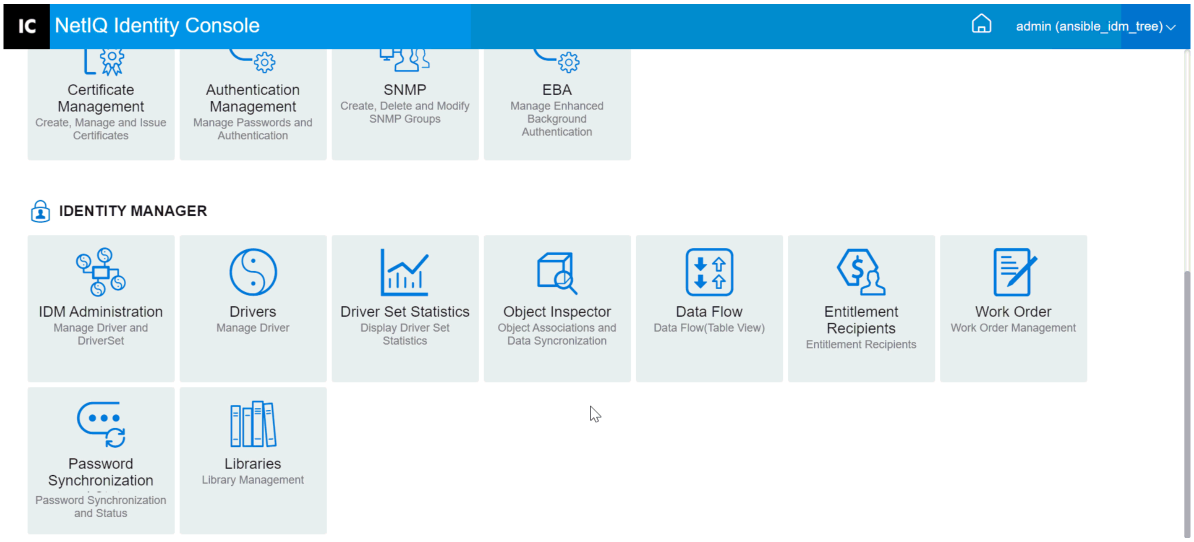
1. In Identity Console, select **Libraries** module from the home page.
2. Select the appropriate library from the list.
3. Click the 🗑 icon. Click **OK** to confirm.

Viewing and Deleting Objects from Library

You can view and delete policies and mapping tables from library objects. To delete objects, perform the following steps:

1. In Identity Console, select **Libraries** module from the home page.
2. Click the appropriate library from the list.
3. To delete policies, select the **Policies** tab.
4. Select the appropriate policy from the list and click the 🗑 icon.
5. To delete mapping tables, select the **Mapping Tables** tab.
6. Select the appropriate mapping table from the list and click the 🗑 icon.
7. Click **OK** to confirm.

Figure 31-1 Managing Libraries



32 Managing Email Server Options

You can use the Email Server Options to specify the settings for your SMTP email server. This server sends notification emails from applications that use the Edit Email templates.

There are two option through which you can authenticate the servers:

- "Authenticate to the Server by Using Basic Authentication" on page 199
- "Authenticate to the Server by Using Modern Authentication" on page 200

NOTE: Identity Manager 4.9 now supports email-based approval through modern authentication. You can configure modern authentication for the email server from the Identity Console portal, starting from version 1.7.2. In previous versions of Identity Console, you could only authenticate to the server using credentials (basic authentication).

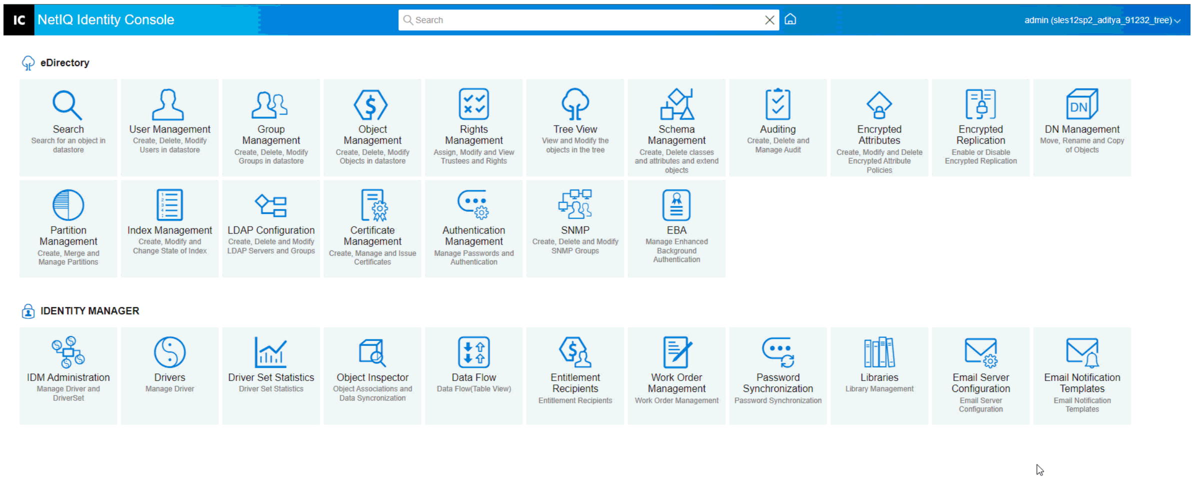
Authenticate to the Server by Using Basic Authentication

To configure a username and password for authenticating to the server:

1. On the Identity Console home page, click **Email Server Configuration**.
2. On the **Email Server Options** page, specify the values for your email notification server.
   - **Host Name:** Specify the hostname or IP address of your SMTP server along with the port number. Use colon (:) to separate the hostname or IP address and port.

     For example, `smtp.example.com:587`
   - **From:** Specify the sender's email address. The email server performs reverse lookups or authentication using this value.
   - **Time Out Value:** The timeout option allows you to set the time limit (in seconds) to send notification emails.
   - **Enable SSL:** Select to enable SSL, if required.
3. Specify **User Id** and **Password**.
4. Click **Save**.
5. To verify the connectivity, click **Test Server Connection**.

Figure 32-1 Email Server Configuration


IC NetIQ Identity Console
Search
admin (sles12sp2_aditya_91232_tree)
eDirectory
Search
Search for an object in datastore
User Management
Create, Delete, Modify Users in datastore
Group Management
Create, Delete, Modify Groups in datastore
Object Management
Create, Delete, Modify Objects in datastore
Rights Management
Assign, Modify and View Trustees and Rights
Tree View
View and Modify the objects in the tree
Schema Management
Create, Delete classes and attributes and extend objects
Auditing
Create, Delete and Manage Audit
Encrypted Attributes
Create, Modify and Delete Encrypted Attribute Policies
Encrypted Replication
Enable or Disable Encrypted Replication
DN Management
Move, Rename and Copy of Objects
Partition Management
Create, Merge and Manage Partitions
Index Management
Create, Modify and Change State of Index
LDAP Configuration
Create, Delete and Modify LDAP Servers and Groups
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
IDENTITY MANAGER
IDM Administration
Manage Driver and DriverSet
Drivers
Manage Driver
Driver Set Statistics
Driver Set Statistics
Object Inspector
Object Associations and Data Syncronization
Data Flow
Data Flow(Table View)
Entitlement Recipients
Entitlement Recipients
Work Order Management
Work Order Management
Password Synchronization
Password Synchronization
Libraries
Library Management
Email Server Configuration
Email Server Configuration
Email Notification Templates
Email Notification Templates

Authenticate to the Server by Using Modern Authentication

Modern authentication helps you to securely manage email approvals. You can configure modern authentication for email notification server in Identity Manager 4.9 and later.

To authenticate the server using modern authentication:

1. On the Identity Console home page, click **Email Server Configuration**.
2. On the **Email Server Options** page, specify the values for your email notification server.
    - **Host Name:** Specify the hostname or IP address of your SMTP server along with the port number. Use colon (:) to separate the hostname or IP address and port.

      For example, `smtp.example.com:587`
    - **From:** Specify the sender's email address. The email server performs reverse lookups or authentication using this value.
    - **Time Out Value:** The timeout option allows you to set the time limit (in seconds) to send notification emails.
    - **Enable SSL:** Select to enable SSL, if required.
3. For Authentication Required, select **Modern Authentication** and specify values for the following parameters:

    NOTE: You must register the Identity Console application with Azure AD to get the values for these parameters. For more information on how to register your application, see Azure AD portal for registering applications (https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app).

    - **User Id**: Specifies the account required for server authentication.
    - **Tenant Id**: Specify the tenant ID of your registered application.

- **Client Id**: Specify the client ID assigned to your application.
- **Client Secret**: Specify the client secret password.
- **Scope**: Specify the scope of the server.
- **Request Url**: Specifies the request URI of your email server, to which Identity Manager sends authentication requests containing the client secret, scope, grant type, and auth mechanism in the payload.

  For example, `https://login.microsoftonline.com/<tenantID>/oauth2/v2.0/token`
- **Grant type**: Used by Identity Console to obtain an access token to access their own resources, not on behalf of a user. The Grant Type parameter is set to `client_credentials` by default and cannot be modified.
- **Auth mechanism**: Specifies the format used by the application to encode and transmit the access token to the authentication server. The access token authenticates a user's Outlook account. By default, Auth Mechanism is set to `XOAUTH2` and cannot be modified.

4 Click **Save**.

33

Managing Email Templates

This list shows the notification templates that are available. You use these templates to send an email message to users in this tree. You can customize these templates with your own text.

Some applications provide their own templates. These Template objects are in the Security container, usually found at the root of your tree.

You can sort the list by name, date, or subject.

Subject

The text that a user views in an email's Subject headline. To edit a template, click the template's Subject headline. By using the Edit Email Notification Template interface, you can modify the template and its details.

Template Name

Each template has a unique name. The application sending the email references this name.

Last Modified

The date and time that the template was last modified.

New

Enables you to create a new email template.

1. Click + icon.
2. Specify a name for the new template (for example, Approval) and click **OK**.

If you have disabled pop-ups, you return to the Edit Email Notification Template pop-up. The new template name appears in the Name column, but [No Subject] appears in the Subject headline column. In this case, click [No Subject] so that you can provide details in the new template.

Edit Email Notification Template

The Edit Email Notification Template page enables you to modify the email template. You can customize the template with your own text.

Template Name

Displays the name of the template.

Subject

The text that a user views in an email's Subject headline. You can change the text of the subject line. The actual name of the template remains the same.

Send As

The format that the SMTP server uses to send the email: Text or HTML.

Tokens or Replacement Tags

The replacement tags help you personalize the message for the user. You can copy replacement tags from the list of available tags and paste them into the message.

Each template includes default tokens or replacement tags, which are variables needed to personalize the email for the user. For example, the Forgot Password email template for sending a password to the user includes the default token or replacement tag named ‘CurrentPassword.’

Add: You can define other tokens or replacement tags for use in the body of the message.

To add a token or replacement tag, perform the following steps:

1. Click + icon.
2. Specify the **Name** and **Description** in **Add Replacement Tag** window.
3. Click **Ok**.
4. The new token or replacement tag lists in Replacement Tags column.

Copy Tag: Click ⧉ to copy the selected tag to the system buffer, and then you can click mouse to paste it and utilize in subject line or body of the message.

Delete: Select a token or replacement tag in the list and click 🗑 to delete the tag from the list. Ensure you don't remove tags that are needed for the body of the message.

Message Body

The text of the email message.

Click **Update** after specifying all the email notification template modifications.

Delete

Removes (from the Identity Vault) templates that you have created. You cannot delete default templates that are shipped with applications such as Identity Manager.

1. Select the template that you want to delete.

   If you click the template Subject headline, Identity Console provides the Edit Email Templates dialog box.
2. Click the Delete icon.
3. Click **OK**.

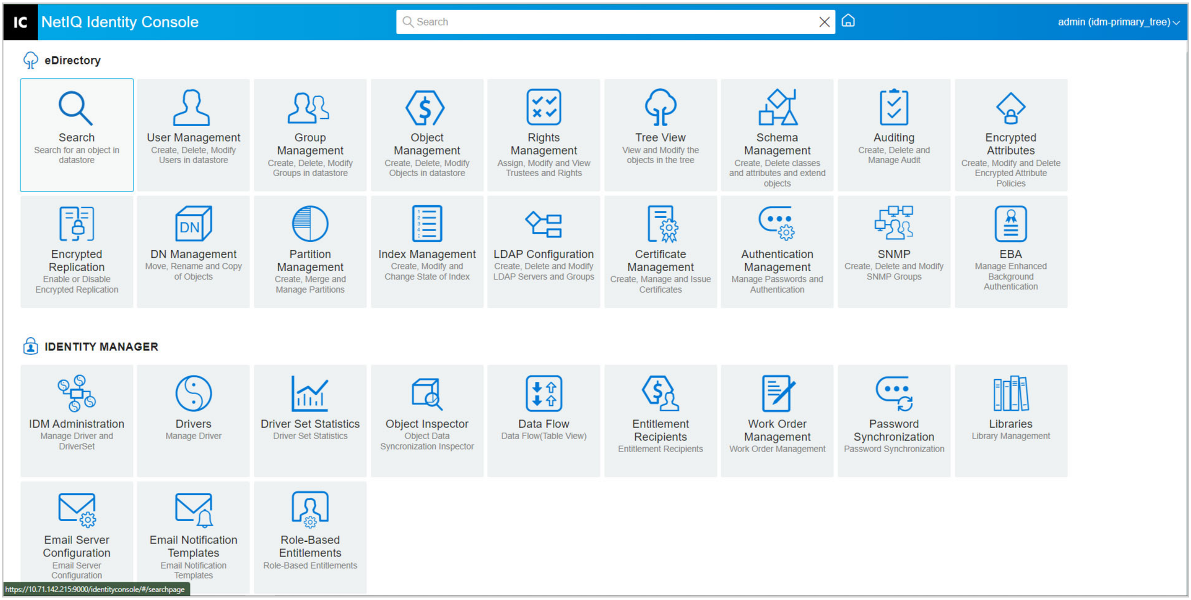
Filter Templates

Enables you to filter which email template you want to display. Only the selected templates will be displayed. The Filter by all option displays all the templates.

Refresh Templates

Click the ↻ icon to refresh and remove any applied filter templates.

__Figure 33-1__ Email Notification Templates


IC
NetIQ Identity Console
Search
admin (idm-primary_tree)
eDirectory
Search
Search for an object in datastore
User Management
Create, Delete, Modify Users in datastore
Group Management
Create, Delete, Modify Groups in datastore
Object Management
Create, Delete, Modify Objects in datastore
Rights Management
Assign, Modify and View Trustees and Rights
Tree View
View and Modify the objects in the tree
Schema Management
Create, Delete classes and attributes and extend objects
Auditing
Create, Delete and Manage Audit
Encrypted Attributes
Create, Modify and Delete Encrypted Attribute Policies
Encrypted Replication
Enable or Disable Encrypted Replication
DN Management
Move, Rename and Copy of Objects
Partition Management
Create, Merge and Manage Partitions
Index Management
Create, Modify and Change State of Index
LDAP Configuration
Create, Delete and Modify LDAP Servers and Groups
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
IDENTITY MANAGER
IDM Administration
Manage Driver and DriverSet
Drivers
Manage Driver
Driver Set Statistics
Driver Set Statistics
Object Inspector
Object Data Syncronization Inspector
Data Flow
Data Flow(Table View)
Entitlement Recipients
Entitlement Recipients
Work Order Management
Work Order Management
Password Synchronization
Password Synchronization
Libraries
Library Management
Email Server Configuration
Email Server Configuration
Email Notification Templates
Email Notification Templates
Role-Based Entitlements
Role-Based Entitlements
https://10.71.142.215:9000/identityconsole/#/searchpage

34 Managing Role-based Entitlements

RBE lets you grant entitlements on connected systems to a group of NetIQ® Identity Console users. Through RBE policies, you can streamline the management of business policies and reduce the need to configure your Identity Manager drivers.

The Role-based Entitlement module has the following:

- “Role-based Entitlement” on page 207
- “Re-Evaluate Membership” on page 216

Role-based Entitlement

An RBE policy is an Identity Console dynamic group object with additional features added to let you grant RBEs on connected systems. When you create an RBE policy, you define the membership for the policy and the entitlements that should be granted to the members of the RBE policy. Each RBE policy is associated with a single Driver Set object assigned to a particular server. Like an Identity Manager driver, each Entitlement policy can manage only objects that are in a master or read/write replica on the server to which it is assigned.

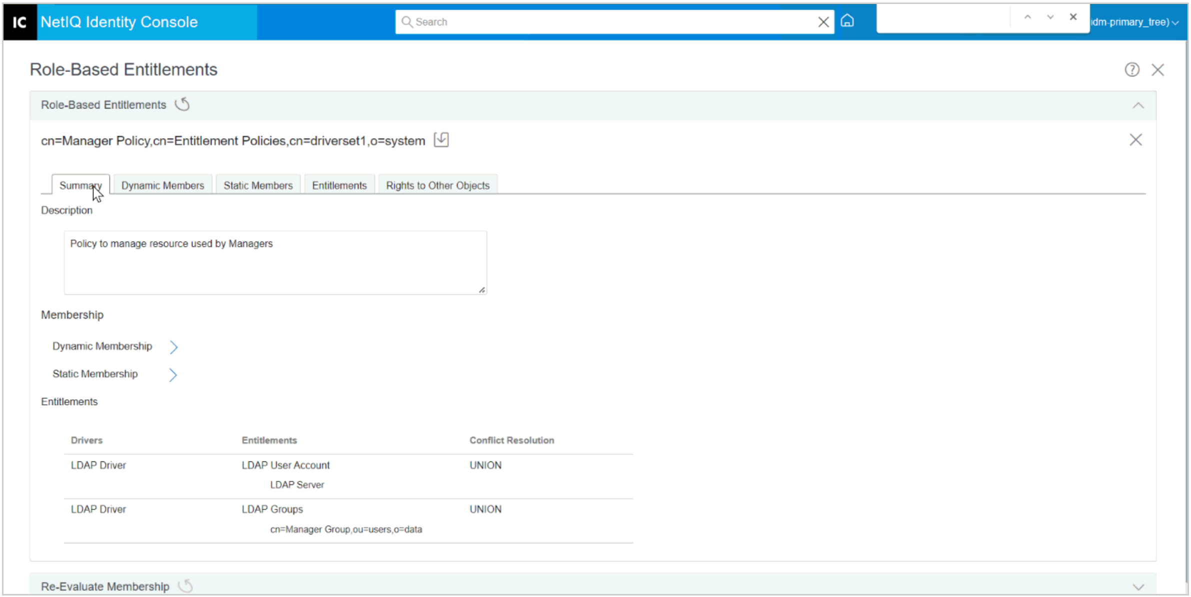
The following sections explain in detail about Role-based Entitlement:

- “Summary” on page 207
- “Dynamic Members” on page 209
- “Static Members” on page 211
- “Entitlements” on page 212
- “Rights to other Objects” on page 212
- “Prioritize RBE Policies” on page 214

Summary

This page summarizes a high-level view of the membership criteria and entitlements for the Entitlement policy.

***Figure 34-1** Summary Page*



cn=Manager Policy,cn=Entitlement Policies,cn=driverset1,o=system

Description: Policy to manage resource used by Managers

Drivers	Entitlements	Conflict Resolution
LDAP Driver	LDAP User Account LDAP Server	UNION
LDAP Driver	LDAP Groups cn=Manager Group,ou=users,o=data	UNION

Membership:

The criteria specified for dynamic membership are displayed in the syntax of an LDAP filter. Search Identity indicates which object's rights are used when querying for dynamic membership, and the Base DN and Scope indicate what part of the tree is included in the query.

You can view the static membership inclusions and exclusions by selecting the check box.

The combined list of all members is not displayed on the Summary page because the list might be long. To see a combined list of all the members of the Entitlement policy, both dynamic and static, use the Membership > View Membership tab.

Entitlements:

The entitlements on connected systems that are granted to members of the Entitlement policy. Keep in mind that Role-Based Entitlements are loosely consistent with the connected systems. This means that the status of an entitlement on a connected system is not displayed in the Entitlement Policy interface. If you grant an entitlement to an Entitlement policy, and later that entitlement is no longer available on the connected system, the entitlement is still listed in the Entitlement policy until you manually remove it from the list.

Conflict Resolution:

For RBEs that have values, these method are used to determine which values are granted to a user if two or more RBE policies grant different values to that user. An example of an entitlement that has values is membership in email distribution lists, where the values are the names of the distribution lists.

The conflict resolution method is set separately for each individual entitlement on each driver object. If an entitlement is used in multiple RBE policies, the conflict resolution method is the same across all RBE policies. To change the conflict resolution method for an entitlement, change the setting for that entitlement in the driver manifest for the driver.

- **Unrecognized:** The RBE policy has not been completed in the wizard, or the setting has been typed incorrectly in the driver manifest.
- **Merge:** The default setting is Merge (`union` in the driver manifest). This means that a user is granted all values for this entitlement from all RBE policies he or she is a member of.

  When using the default setting of Merge, the priority order of the list of policies is not important for this particular entitlement.

  For example, a user is granted membership in email distribution lists for GroupWise® Driver A by two different RBE policies, the Managers policy and the Team Members policy. In Policy 1, the user is granted membership in the Managers email distribution list, and in Policy 2, the user is granted membership in the Team Members email distribution list. With a setting of Merge, the user is granted membership in both email distribution lists.
- **Priority:** This setting means that if multiple RBE policies grant a user different values for the same entitlement from the same driver object, the user is granted only the values that are specified in the RBE policy that is highest in the list.

  When using the Priority setting, the priority order of the list of policies is important for this particular entitlement.

  For example, a user is granted membership in email distribution lists for GroupWise Driver A by two different RBE policies, the Managers policy and the Team Members policy. In the Managers policy, the user is granted membership in the Managers email distribution list, and in the Team Members policy, the user is granted membership in the Team Members email distribution list. The Managers policy is listed higher in the list of policies than the Team Members policy. With a setting of Priority, the user is granted membership only in the Managers email distribution list.

  Using priority for conflict resolution might be useful if, for example, an attribute on the connected system only allows a single value. If two different RBE policies grant a value for that attribute to the same user, the user receives the value that is granted by the RBE policy that is highest in the list.

NOTE: A conflict resolution setting is not provided for entitlements that have no values, such as an account. Entitlements that have no values are always granted to members of the RBE policy, regardless of the priority of policies in the list.

Dynamic Members

The criteria specified for dynamic membership are displayed in the syntax of an LDAP filter. Search Identity indicates which object's rights are used when querying for dynamic membership, and the Base DN and Scope indicate what part of the tree is included in the query.

Membership Filter

You can define criteria for membership, such as location in the tree and attributes of the object. For example, membership could be dependent on whether the user is in the Active container, or whether the job title includes the word Manager. Users who meet the criteria are automatically members of the RBE policy, without requiring you to specifically add each user to the policy. The dynamic membership is the same as a Dynamic Group object.

If an object changes so that it no longer meets the criteria for dynamic membership, the entitlements are automatically revoked the next time when the user is reevaluated.

Set Search Parameters

Specify the location of the users you want the Entitlement policy to manage. Choose the container that holds the users (Base DN), and how far down from that container you want the search to go (Scope of Search). For the Entitlement policy to manage users in the containers you specify, the users must be in a read/write or master replica on the server.

The following options are provided for Scope of Search:

- This container and its subcontainers: Users below this container in the tree are members of the Entitlement policy if they meet the criteria specified for dynamic membership. Users inside subcontainers are also members if they meet the criteria.
- This container only: Users inside this container are members of the Entitlement policy only if they meet the criteria specified for dynamic membership. Users inside subcontainers below this container are not members even if they meet the criteria.

Define Filter Criteria

Specify the characteristics that determine which users are members of the Entitlement policy.

In the Summary page for an Entitlement policy, the dynamic membership criteria you specify are displayed in the syntax of an LDAP filter.

By default, dynamic membership is set to include all User class objects (and objects of classes derived from the User class) within the search scope as members of the Entitlement policy.

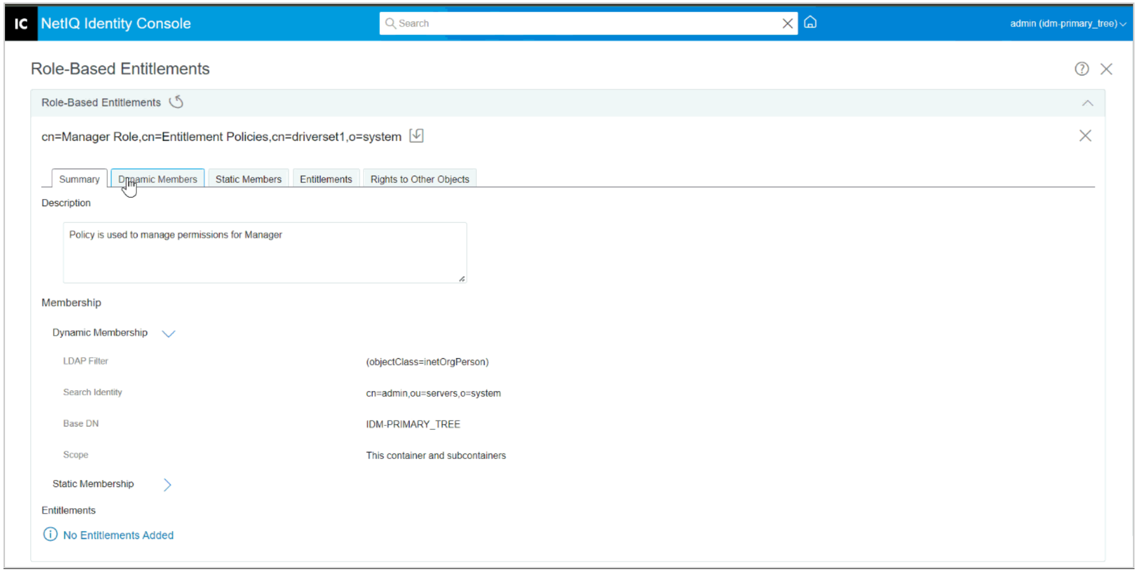
NOTE: If you create a new object class derived from User, an existing Entitlement policy does not become aware of that class until you make a modification to the Entitlement policy. This prevents users of a new class from being granted entitlements unintentionally. When any modification is made to the Entitlement policy, the list of user-derived classes for that policy is updated.

Creating Dynamic Membership

On the Dynamic Members tab, perform the following:

1. Click the **Dynamic Members** tab.
2. Use the **Search Identity**, **Begin Search at,** and the **Search Scope** filters as per your requirement.
3. Click the specific **Create Group** to create a new condition or a row, then provide the required search criteria or condition.

Figure 34-2 *Dynamic Members*



cn=Manager Role,cn=Entitlement Policies,cn=driverset1,o=system

Description

Policy is used to manage permissions for Manager

Membership

Dynamic Membership

LDAP Filter (objectClass=inetOrgPerson)

Search Identity cn=admin,ou=servers,o=system

Base DN IDM-PRIMARY_TREE

Scope This container and subcontainers

Static Membership

Entitlements

No Entitlements Added

Search Scope: The Search Scope indicates the set of entries at or below the search base DN that may be considered potential matches for a search operation.

Search Criteria: You can limit a search to help you locate a specific record or group of records from a large number of records.

Base DN: A Base DN is the point from where a server will search for users.

LDAP Group: It is a hierarchical organization of Users, Groups, and Organisational Units which are containers for users and groups.

NOTE: The user can create single or multiple groups with conditions. The conditions consist of attributes, operators, and value. By default, **Object Class** > **is equal** > **User** is populated.

Static Members

Static Members are class of members that are declared using static keywords. A static member has certain limited accesses.

On the Static Members tab, the following operations can performed:

Include Members:

Add members statically who are not included by the dynamic membership filter.

Exclude Members:

Exclude members that meet the filter’s criteria but should not be included in the entitlement policy.

Entitlements

RBE lets you grant entitlements on connected systems and rights in Identity Manager. Entitlements can be any of the following:

- Accounts on connected systems.
- Membership in email distribution lists on connected systems.
- Group membership on connected systems.
- Attributes for the corresponding objects in connected systems, populated with the values you specify.

NOTE: The Entitlements functionality is part of Identity Manager, so, you must have Identity Manager drivers installed and configured to support Entitlements before you can grant entitlements on connected systems.

Create Entitlement

On the Entitlements tab, perform the following:

1. Click the **Entitlement** tab.
2. Click + to **Add Drivers** and to provide entitlements on connected systems.

   Add Driver screen appears.
3. Select the driver from the drop-down menu.
4. Click **Add**.

   The **Add Entitlements** screen appears.
5. From the drop-down menu **Select an Entitlement** group that you want to add.
6. Select the **Query Type**:
   - **Cached:** When queries are previously run.
   - **External Query:** When queries are new.

   The **Add Group Entitlement** screen appears.
7. Select group entitlement from the drop-down menu, then click **Select**.

Rights to other Objects

Use this page to give an Entitlement policy trustee rights to an eDirectory object. Each member of the Entitlement policy becomes a trustee of the object.

In addition to assigning rights to all attributes, you can click Add Property to assign rights to specific properties.

The Inherit check box determines whether the rights flow down in the tree. For example, if you are assigning rights to a container object, and you want the Entitlement policy to have the same rights to the objects and sub-containers that are below that container, select the Inherit check box.

Rights to objects in eDirectory are granted to members of the Entitlement policy after you complete your changes on this page. By contrast, entitlements in connected systems are granted to each member of the Entitlement policy the next time an attribute used for dynamic membership is modified for that user, or the user is moved or renamed. (The same is true when rights and entitlements are revoked.) Use the Reevaluate Membership task to force an update.

Create Rights to other Objects

To create rights:

1 Click on the **Rights to Other Objects** tab

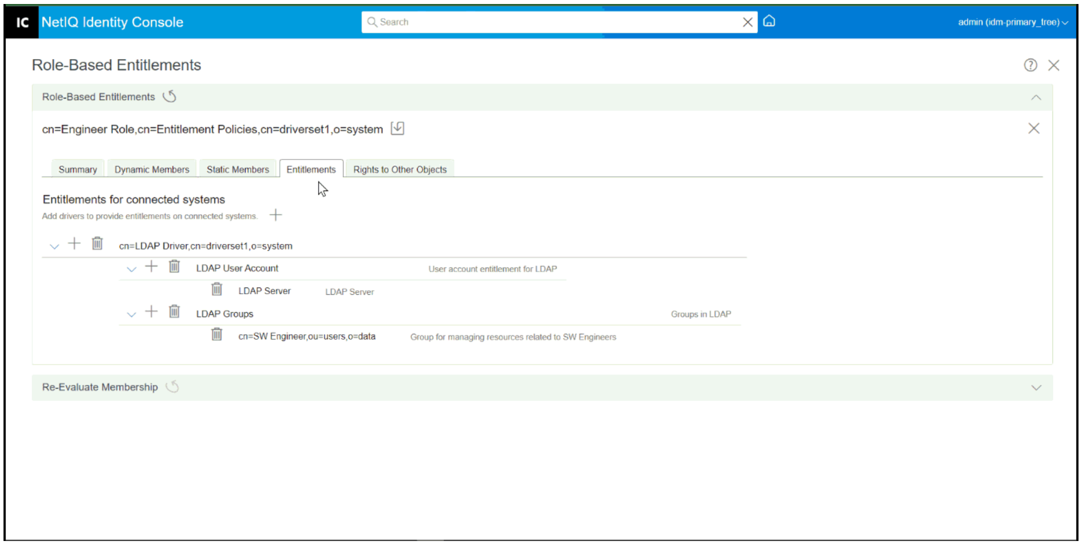
Here you can add a new Object, and browse for those Objects that you want this Entitlement Policy to be a trustee.

1a To add an object click + button.

The **CONTEXT BROWSER** page appears. The page consists of `Objects`.

1b Expand the `Objects` and select Groups or individual Users as per your requirement and assign rights to them.

Figure 34-3 *Rights to other Objects*



cn=Engineer Role,cn=Entitlement Policies,cn=driverset1,o=system

Add drivers to provide entitlements on connected systems.

cn=LDAP Driver,cn=driverset1,o=system

LDAP User Account — User account entitlement for LDAP

LDAP Server — LDAP Server

LDAP Groups — Groups in LDAP

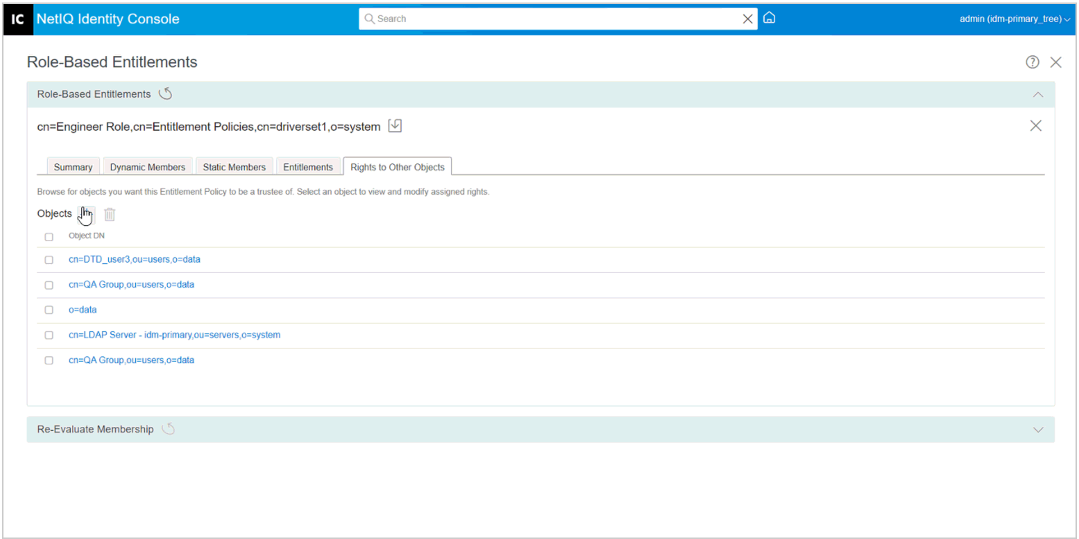
cn=SW Engineer,ou=users,o=data — Group for managing resources related to SW Engineers

1c To add more properties, click +.

The **SELECT PROPERTIES** page appears. This page has the list of Properties that an Object can have.

1d Click **Done.**

Figure 34-4 Select Properties



cn=Engineer Role,cn=Entitlement Policies,cn=driverset1,o=system

Browse for objects you want this Entitlement Policy to be a trustee of. Select an object to view and modify assigned rights.

☐ Object DN

☐ cn=DTD_user3,ou=users,o=data

☐ cn=QA Group,ou=users,o=data

☐ o=data

☐ cn=LDAP Server - idm-primary,ou=servers,o=system

☐ cn=QA Group,ou=users,o=data

2 (Optional) Using the **Up** and **Down** ↑ ↓ arrows prioritize the RBE Policies.

Prioritizing the policy is to resolve entitlement conflicts between multiple policies. The topmost policy has highest priority. For more information see: "Prioritize RBE Policies" on page 214

Prioritize RBE Policies

When you create RBE policies, it is possible that the policies affecting a particular user might conflict.

The order of RBE policies in the list represents priority. You can change the order of the list by using the up-arrow and down-arrow buttons.

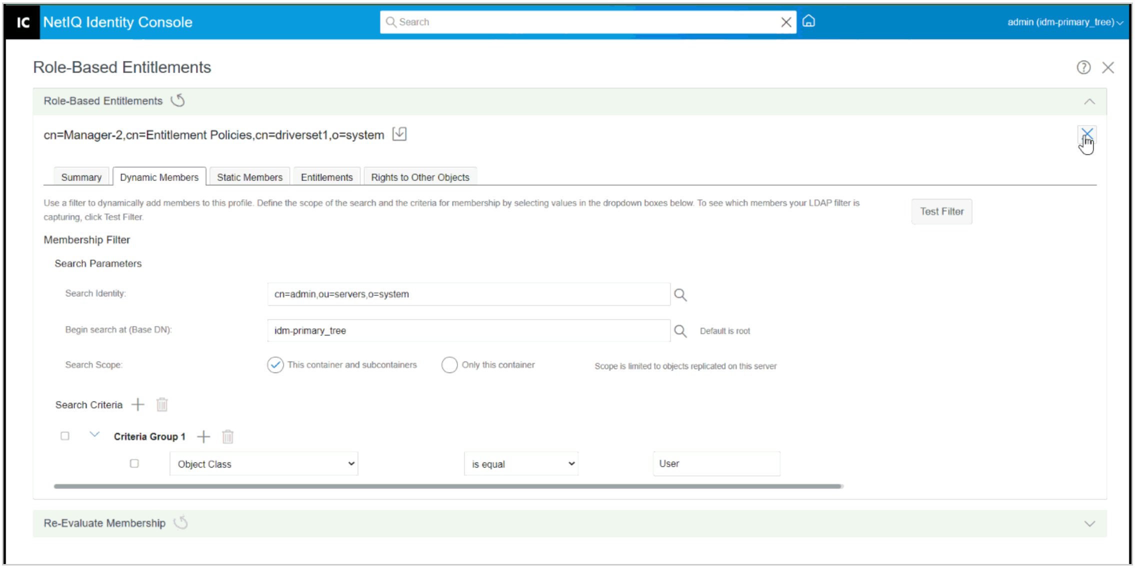
- This setting might be useful if, for example, an attribute on the connected system allows only a single value. If two different RBE policies grant a value for that attribute to the same user, the user receives the value that is granted by the highest RBE policy in the list. As another example, perhaps you configured your environment to use Entitlements to place users in a hierarchical structure on another system. You would want the user to be placed in either one place or another, not two places at the same time.
- Keep in mind that the setting is independent for each entitlement offered by each driver.
- As a rule, you should place administrator or manager policies higher in the list than policies for end users or individual contributors. You should put groups with narrower membership higher than groups with broader membership.

To prioritize RBE policies:

1 Select the Entitlement Policy that you want to upgrade or down-grade.

2 By using **Up** or **Down** ↑ ↓ arrow prioritize the RBE Policies.

Figure 34-5 Prioritizing the Policies



cn=Manager-2,cn=Entitlement Policies,cn=driverset1,o=system

Use a filter to dynamically add members to this profile. Define the scope of the search and the criteria for membership by selecting values in the dropdown boxes below. To see which members your LDAP filter is capturing, click Test Filter.

Membership Filter

Search Parameters

Search Identity: cn=admin,ou=servers,o=system

Begin search at (Base DN): idm-primary_tree Default is root

Search Scope: ☑ This container and subcontainers ○ Only this container Scope is limited to objects replicated on this server

Search Criteria

☐ Criteria Group 1

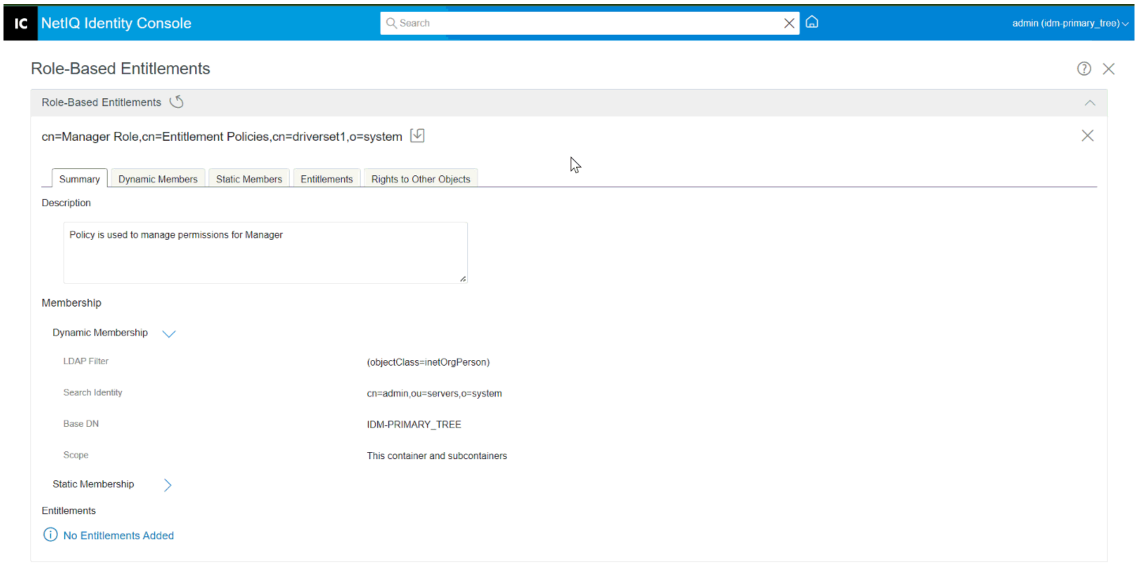
☐ Object Class is equal User

3 Click Save button.

The summary of the policy membership details is displayed in the **Summary** tab.

4 Restart the driver.

Figure 34-6 Close and Restart



cn=Manager Role,cn=Entitlement Policies,cn=driverset1,o=system

Description

Policy is used to manage permissions for Manager

Membership

Dynamic Membership

LDAP Filter	(objectClass=inetOrgPerson)
Search Identity	cn=admin,ou=servers,o=system
Base DN	IDM-PRIMARY_TREE
Scope	This container and subcontainers

Static Membership

Entitlements

No Entitlements Added

NOTE: You must restart the driver for the changes to take effect.

Re-Evaluate Membership

The **Role-based Entitlements** feature lets you grant entitlements on connected systems to a group of users.

When you create or edit an RBE policy, each user's membership must be reevaluated to determine whether entitlements on connected systems need to be granted, changed, or revoked. By default, reevaluation takes place for users one at a time, the next time an attribute that affects membership is changed for each user, or when a user is moved or renamed. This default behavior minimizes the use of system resources, but it means that there might be a significant delay between the time the RBE policy is changed, and the time entitlements are granted, changed, or revoked for a particular user.

You can make sure that the user entitlements are updated all at once by using the "Re-Evaluate RBE Policies" on page 216 task to specify users who should be immediately reevaluated. We recommend that you do this each time you create or edit an RBE policy.

Prior to Identity Manager 3.6, reevaluating membership was performed for all RBE policies in a driver set, not for an individual Entitlement policy. However, Identity Manager 3.6 allows you to **Evaluate** an RBE policy and **Add** its members to the selected **Objects List**. If you have defined an Entitlement policy and have created a membership list, you will see the Evaluate an Entitlement Policy to **Add** its members to the list heading next to the selected Objects entry. Select the policy, then click the + icon to add the policy's members to the selected **Objects List**. You can add or remove members or objects from the selected **Objects List**.

To make the best use of system resources, you should make all your changes to RBE policies in a particular driver set before using "Re-Evaluate RBE Policies" on page 216.

NOTE: Reevaluating entitlements is necessary only for entitlements on connected systems. When Identity Console rights are changed for an RBE policy, the changes are effective immediately for each user. You must have the Entitlements Service driver running for membership re-evaluations to be performed.

Re-Evaluate RBE Policies

To re-evaluate the membership:

1. Click **Re-Evaluate Membership** > **Select Driver Set**.

   A list of policies that are created will appear.

2. Select the policy that needs to be evaluated, and click **Evaluate** Evaluate.

   At the **Objects** tab, users that are part of the group will appear.

3. (Optional) To add a specific user click +.

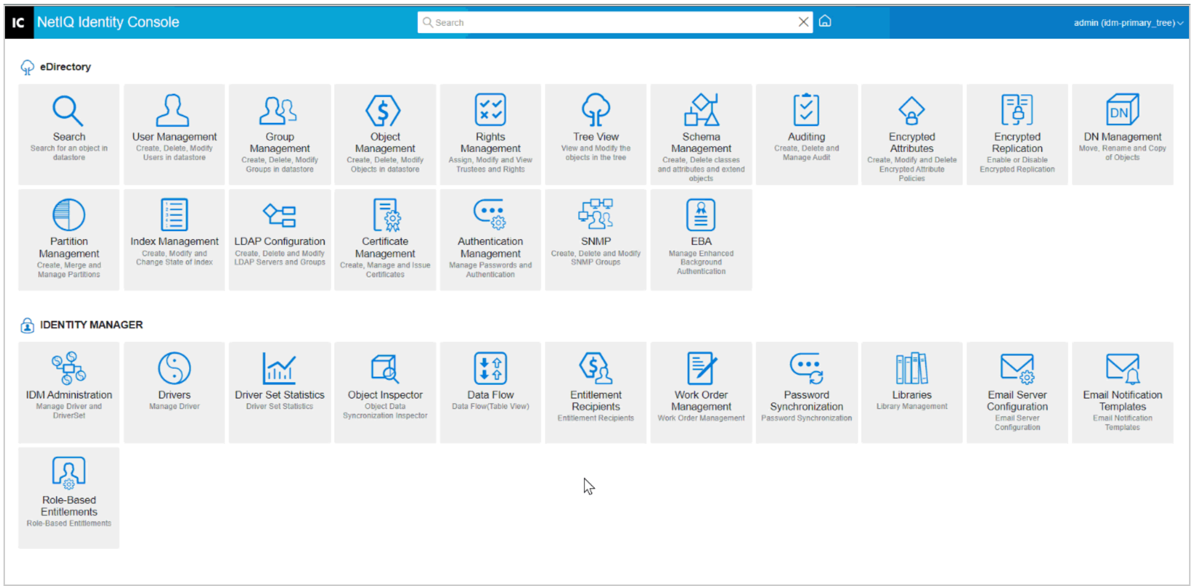
   When users are missing from the list, and you want to add specific users, only then you can use this **Add** + feature.

4. (Optional) To remove specific user click 🗑.

When specific users need to be removed from the list, only then you can use the **Delete** feature.

5 Click Re-evaluate Membership button .

***Figure 34-7** Re-evaluate Membership*


IC NetIQ Identity Console
Search
admin (idm-primary_tree)
eDirectory
Search
Search for an object in datastore
User Management
Create, Delete, Modify Users in datastore
Group Management
Create, Delete, Modify Groups in datastore
Object Management
Create, Delete, Modify Objects in datastore
Rights Management
Assign, Modify and View Trustees and Rights
Tree View
View and Modify the objects in the tree
Schema Management
Create, Delete classes and attributes and extend objects
Auditing
Create, Delete and Manage Audit
Encrypted Attributes
Create, Modify and Delete Encrypted Attribute Policies
Encrypted Replication
Enable or Disable Encrypted Replication
DN Management
Move, Rename and Copy of Objects
Partition Management
Create, Merge and Manage Partitions
Index Management
Create, Modify and Change State of Index
LDAP Configuration
Create, Delete and Modify LDAP Servers and Groups
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
IDENTITY MANAGER
IDM Administration
Manage Driver and DriverSet
Drivers
Manage Driver
Driver Set Statistics
Driver Set Statistics
Object Inspector
Object Data Syncronization Inspector
Data Flow
Data Flow(Table View)
Entitlement Recipients
Entitlement Recipients
Work Order Management
Work Order Management
Password Synchronization
Password Synchronization
Libraries
Library Management
Email Server Configuration
Email Server Configuration
Email Notification Templates
Email Notification Templates
Role-Based Entitlements
Role-Based Entitlements

35 Managing Roles and Access

Roles and Access Control (RAC) assigns the rights within eDirectory to perform tasks. To perform certain tasks, you must have rights in the eDirectory tree. When you assign a role to a user, RAC assigns the necessary rights to perform the tasks of that role.

This section covers the following topics:

IMPORTANT: Setting up the RAC feature is optional, but we recommend setting it up to optimize your Identity Console application. Moreover, the RAC objects must be managed only through Identity Console.

IMPORTANT: When you have Role Based Services (RBS) collections in iManager, create a corresponding RAC configuration, as the iManager RBS Collections will not get recognized in Identity Console. It is recommended that either you use iManager RBS or RAC Configuration, as both cannot co-exist. As the iManager is being deprecated, it is recommended to create a new RAC Collection in Identity Console. For more information see: "Existence of RBS collection in iManager" on page 230

Understanding Roles and Access Control

Identity Console provides the ability to assign specific responsibilities to users and present them with the tools and their accompanying rights required to perform these responsibilities.

RAC is an extension of the eDirectory schema. RAC defines several object classes and attributes which is a mechanism for administrators to grant a user access to management tasks based on the user's role in the RAC configuration. This provides access to users to only those tasks which needs to be performed.

NOTE: NetIQ Identity Console RAC grants rights based on the Access Control List (ACL) capability of NetIQ eDirectory. The ACLs allow a trustee to be granted rights to a specific object or its subordinate objects. ACLs are not granted based on specific object types. Each NetIQ Identity Console task defines its applicable object types and necessary ACLs. However, these ACLs allow the user to perform those operations with other object types through the eDirectory APIs or other tools.

RAC feature also helps to create specific roles within your organization. The roles contain tasks that an assigned user can perform within Identity Console, such as creating a new user or changing a password. Tasks are preassigned to roles but can be replaced, reassigned, or removed.

Furthermore, the users are associated with roles with a specified scope, which is a container in the tree, in which the user has the requisite permissions to perform a task. A role requires this threefold association of role, members, and scope to be completed.

A Role object creates an association between users and tasks. An administrator grants a user access to a task by making the user a member of the Role to which the task is assigned.

A user can be assigned to a Role in the following ways:

- Directly as a user.
- Through a group assignments.

  If a user is a member of a group or a dynamic group that is assigned to a role, then the user has access to the role.
- Through container assignment.

  A User object has access to all the roles that its parent container is assigned. This could also include the containers such as organization and organization unit.

A user can be associated with a role multiple times, each with a different scope.

Roles and Access Control Objects in eDirectory

The following table lists the RAC objects. Identity Console extends the eDirectory schema to include these objects when you install RAC.

Object	Description
RAC Configuration	A container object that holds all the Role and Module objects. RAC Configuration objects are the uppermost containers for all RAC objects. A tree can have any number of RAC Configuration objects. These objects have owners, which are users who have management rights over the Configurations. RAC Configuration objects can be created in any of the following containers: ◆ Domain. ◆ Location. ◆ Country. ◆ Organization. ◆ Organizational Unit.
RAC Role	Defining a role includes creating an RAC Role object and specifying the tasks that the role can perform. RAC Roles are container objects that can be created only in an RAC Configuration container. Role members can be User, Group, Organization, or Organizational Unit, and role members are associated with a role in a specific scope of the tree. The RAC Task objects are assigned to RAC Role objects.

Object	Description
RAC Task	A leaf object that holds a specific function, such as creating a user, or a group. RAC Task objects are located only in RAC Module containers.
RAC Scope	A leaf object is used for ACL assignments (instead of making assignments for each User object). RAC Scope objects represent the context in the tree where a role is performed and are associated with RAC Role objects. They inherit from the Group class. User objects are assigned to an RAC Scope object. These objects have a reference to the scope of the tree that they are associated with. The objects are dynamically created when needed, then automatically deleted when no longer needed. They are located only in RAC Role containers. RAC Scope can be Organization and Organizational Unit. **WARNING:** Never change the configuration of an RAC Scope object. Doing so has serious consequences and could possibly break the system.
RAC Module	Represents a container object that holds RAC Task objects. RAC Module objects have a module name attribute, which represents the name of the product that defines the tasks (for example, Certificate Management, Authentication Management, User Management and so on). RAC Module objects can be created only in the RAC Configuration containers.

Configuration of RAC

- “Setting up RAC Configuration” on page 222
- “Managing RAC Roles” on page 223
- “Viewing Modules List” on page 226
- “Viewing Task List” on page 226
- “Editing Configuration Owner” on page 226
- “Editing Member Association for Configuration” on page 227

The RAC Configuration provides complete control over RAC objects. It is a central place for managing and configuring RAC objects. You can list and modify RAC objects. The configuration also provides useful information, such as searching and displaying the selected modules from the list. The Roles section lists the Associated Tasks for each role.

On the NetIQ Identity Console home page, select **RAC** to open the RAC Configuration page.

The page includes two tabs:

RAC Configuration: Displays current RAC Configurations.

Edit Member Association: Displays a list of roles from all the Configurations.

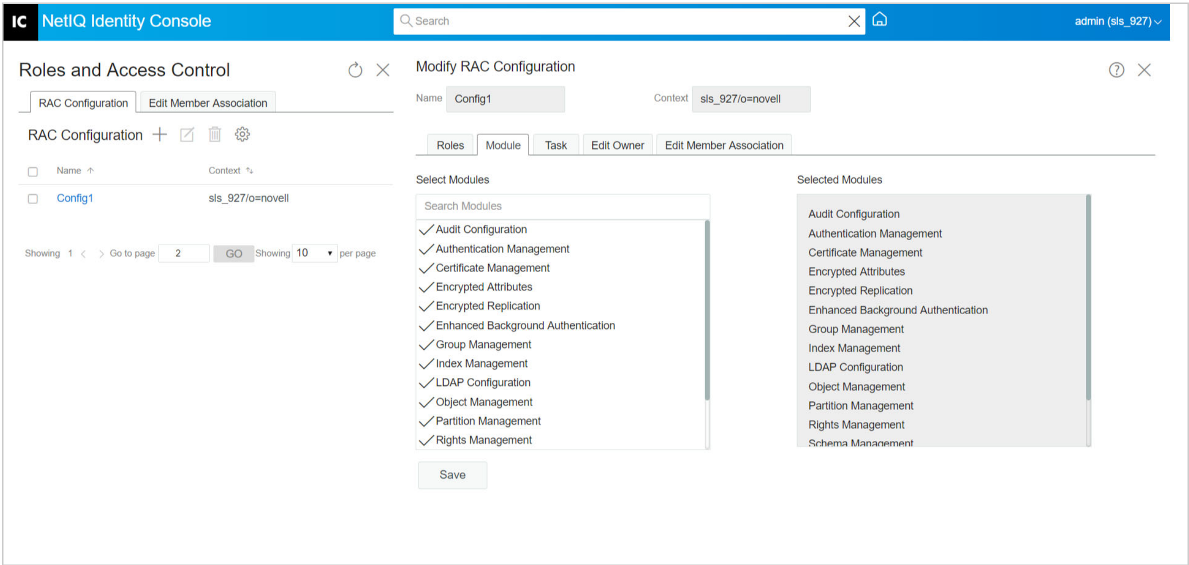
Identity Console displays Configurations that you own and includes the following information on each Configuration:

Module: Indicates the number of modules on the selected RAC Configuration.

To work with a particular Configuration, select it from the list. This opens a configuration-specific view, as shown in figure:

NOTE: For the administrator to access all the modules, it is advisable to create a separate RAC Configuration for the administrator with all the Modules selected.

Figure 35-1 *Indicates the Selected Modules*



Config1 sls_927/o=novell

Name: Config1

Context: sls_927/o=novell

Select Modules:
- ✓ Audit Configuration
- ✓ Authentication Management
- ✓ Certificate Management
- ✓ Encrypted Attributes
- ✓ Encrypted Replication
- ✓ Enhanced Background Authentication
- ✓ Group Management
- ✓ Index Management
- ✓ LDAP Configuration
- ✓ Object Management
- ✓ Partition Management
- ✓ Rights Management

Selected Modules:
- Audit Configuration
- Authentication Management
- Certificate Management
- Encrypted Attributes
- Encrypted Replication
- Enhanced Background Authentication
- Group Management
- Index Management
- LDAP Configuration
- Object Management
- Partition Management
- Rights Management
- Schema Management

The remainder of this section describes the various tabs on the RAC Configuration page.

Setting up RAC Configuration

At the **RAC Configuration** tab, you can see the list of configurations for the specific user. To create a new RAC Configuration, follow the steps:

1. On the **RAC Configuration** tab, Click +.
2. Enter a **Name**.
3. In the Context field, Click **Search** 🔍 and select the required Container.
4. Assign a role to the user or group of users, by selecting the module from the **Select Modules** list.
5. Select a required **Scope**.
6. (Optional) Provide a **Description**.
7. Select the required check box, to specify how you want the rights that are related to this role to be assigned to the member.

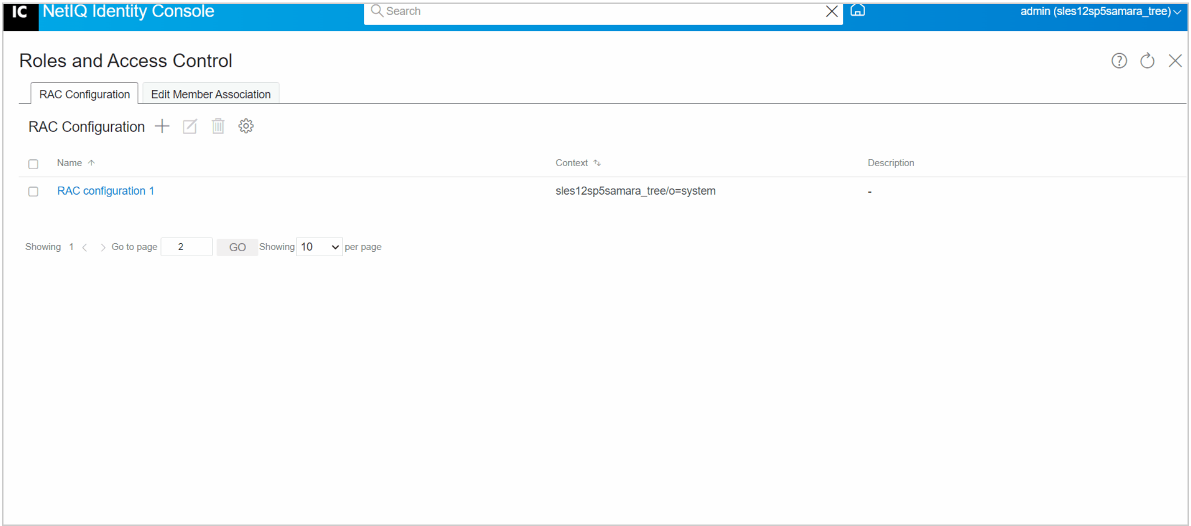
   Assign Rights: Instructs eDirectory to automatically grant the member rights necessary to perform the assigned role. When not selected, the member is assigned the role but might not have rights to perform all tasks associated with the role. The member’s rights assignments are handled separately.

Inheritable: Select **subtree** to indicate that the member's scope includes all sub-containers in the specified context. Select **base object** to indicate that the member can perform the role only in the specified container.

8. Click **Create**.

The RAC Configuration is created.

Figure 35-2 *RAC Configuration*



☐	Name ↑	Context ⇅	Description
☐	RAC configuration 1	sles12sp5samara_tree/o=system	-

Managing RAC Roles

The RAC Configuration **Role** tab allows you to manage the RAC roles in the configuration. On the **Roles** tab, you can see the list of Roles that were selected while creating the Configuration. From this tab you can perform the following:

- "Creating a New Role" on page 223
- "Removing a Role" on page 224
- "Importing the Removed Role" on page 225
- "Adding Task to Selected Role" on page 226

Creating a New Role

This wizard steps you through naming or customizing the role, assigning tasks and categories to the role, and assigning role members and scopes to the role.

In the **Roles** tab, you can view the modules that are assigned at the **Role** menu. If you click on the module, you can see the appropriate task assigned to that role at the **Associated Tasks** menu.

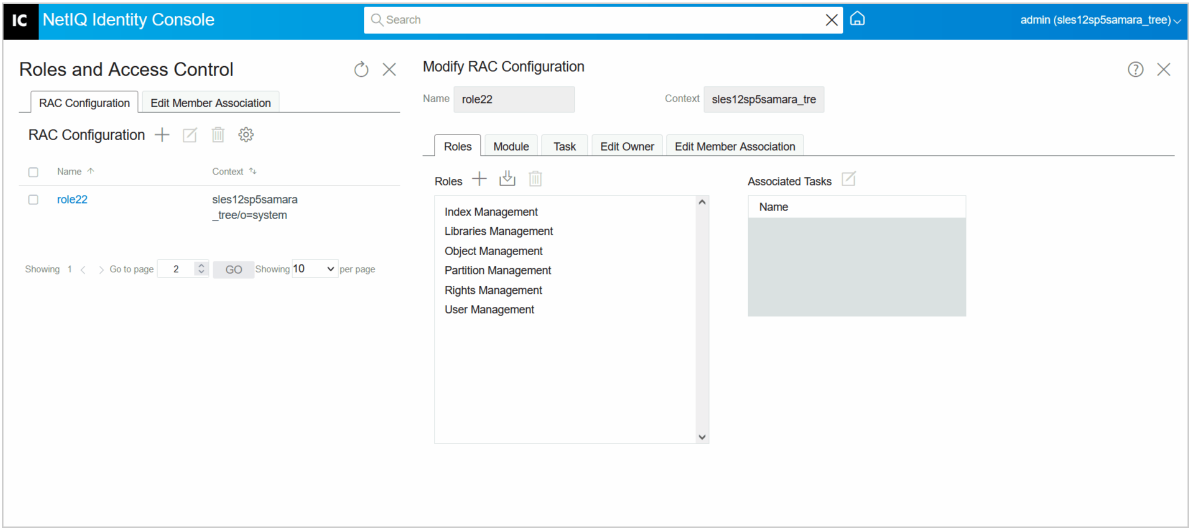
To create a new role in the Configuration:

1. In the **Role**s tab, click **Create Role** +.
2. On the **Create Role** window, click **Add Scope** 🔍, and select a **Scope**.
    - **2a** Enter the **Name**.
    - **2b** Select the **Member** or the group of members that you want to associate with the Role.

3. From the **Select Task (s)** menu, select the tasks that need to be assigned to the Role.
4. Click **Create**.

A new Role is created. Close the window and open the Configuration again to view the changes.

Figure 35-3 *Create New Role*



Name	Context
role22	sles12sp5samara_tree/o=system

Name: role22

Context: sles12sp5samara_tre

Go to page: 2

Showing: 10

Index Management
Libraries Management
Object Management
Partition Management
Rights Management
User Management

Removing a Role

To remove a role in the Configuration:

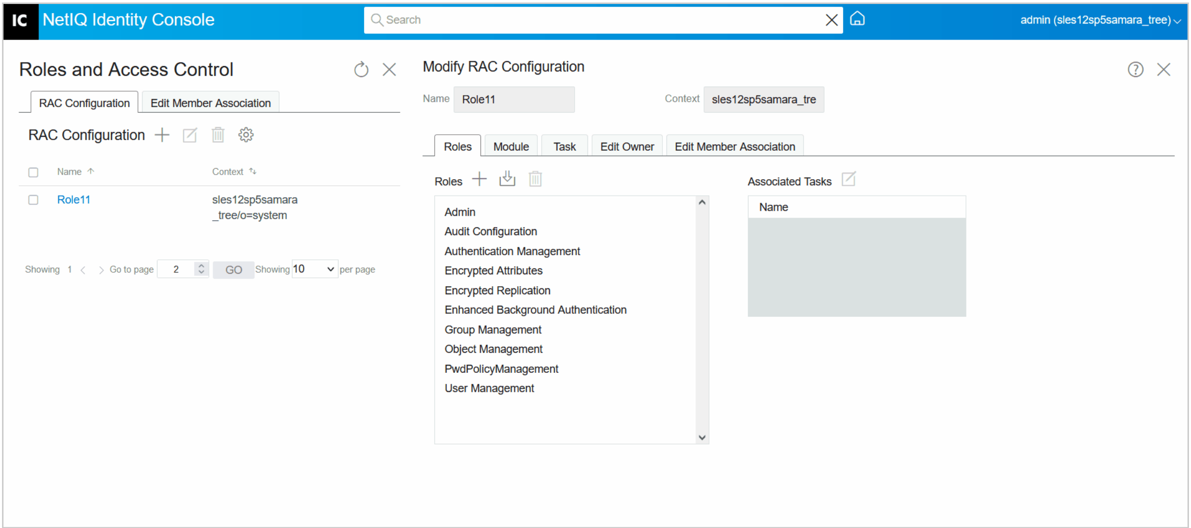
NOTE: When deleted, the custom created roles cannot be imported again. Be careful before deleting them.

---

1. In the **Role**s tab, select the role that you want to delete, and click **Remove role** .
2. Click **OK**.

A Role is removed. Close the window and open the Configuration again to view the changes

Figure 35-4 *Remove Role*



Name: Role11

Context: sles12sp5samara_tre

Role11 sles12sp5samara_tree/o=system

Importing the Removed Role

To import a removed Role in the Configuration:

1. In the **Roles** tab, click **Import Removed Role**.

   The **SELECT ROLE(S)** list appears.

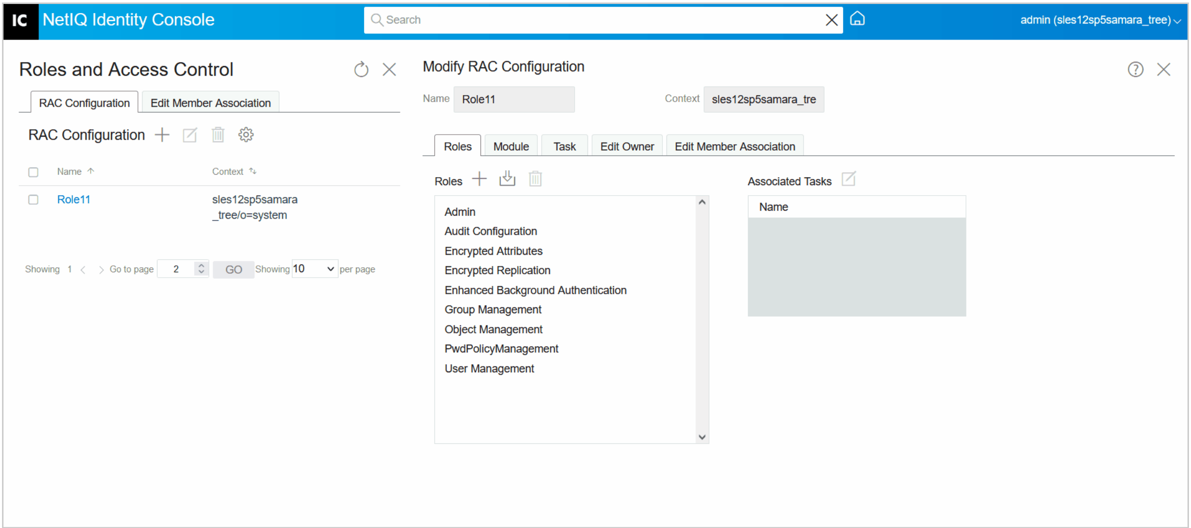
2. Select the Role that needs to be imported.

   The role is imported and visible on the **Roles** menu.

3. Click **OK**.

A new Role is imported. Close the window and open the Configuration again to view the changes

Figure 35-5 *Import the Removed Role*



Name: Role11

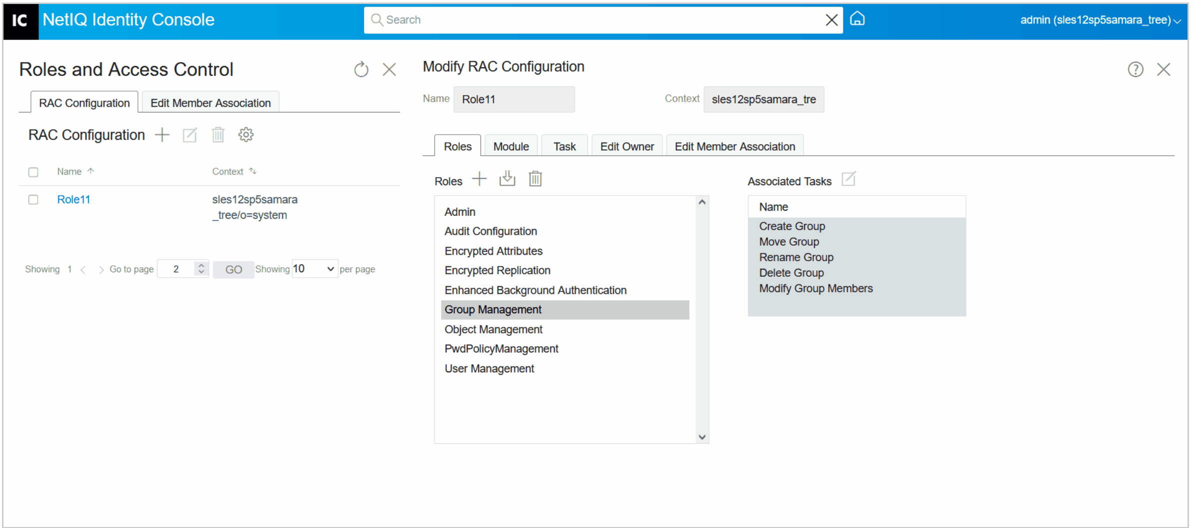
Context: sles12sp5samara_tre

Role11 sles12sp5samara_tree/o=system

Adding Task to Selected Role

To add additional tasks to a particular Role, at the **Associated Tasks** menu click **Add** ⊞.

Figure 35-6 Add Task to Selected Role



☐	Name	Context
☐	Role11	sles12sp5samara_tree/o=system

Name: Role11
Context: sles12sp5samara_tre

Roles:
- Admin
- Audit Configuration
- Encrypted Attributes
- Encrypted Replication
- Enhanced Background Authentication
- Group Management
- Object Management
- PwdPolicyManagement
- User Management

Name
Create Group
Move Group
Rename Group
Delete Group
Modify Group Members

Viewing Modules List

The **Module** tab contains the lists the RAC modules currently installed on a selected Configuration. Each Module contains RAC tasks. From this page, you can add or delete a Module.

The RAC Configuration > **Module** tab allows you to perform the following operations:

Viewing Task List

You can view the list of Tasks available for the list of Configuration.

A task is a distinct management function, such as creating a user or setting a password. Identity Console lists the tasks by group in the navigation area.

The RAC Configuration > **Task** tab allows you to perform the following operations:

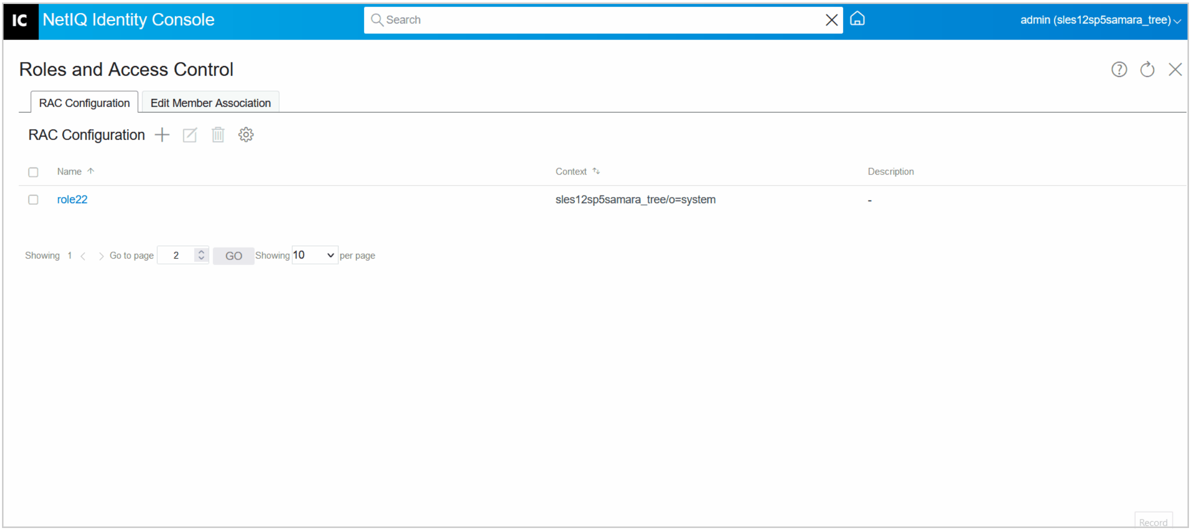
Editing Configuration Owner

On this screen, you can see the list of owners of a specified Configuration. You can add the Configuration owners or delete the existing Configuration owners. To add a Configuration owner, follow the procedure:

1. Click **Add Configuration Owner** ⊞.
2. On the **Context Browser** window, select the user, then click **OK**.

By using the **Search** box, you can search for a user or the objects.

Figure 35-7 *Edit Configuration Owner*



☐	Name	Context	Description
☐	role22	sles12sp5samara_tree/o=system	-

Editing Member Association for Configuration

The **Edit Member Association** tab helps to associate a member to a role by selecting the member.

To add a member to an existing role:

1. Click **Select Member** 🔍.

   The Context Browser window opens. On the Context Browser window, you have the option to select user, group, organization unit, or organization.

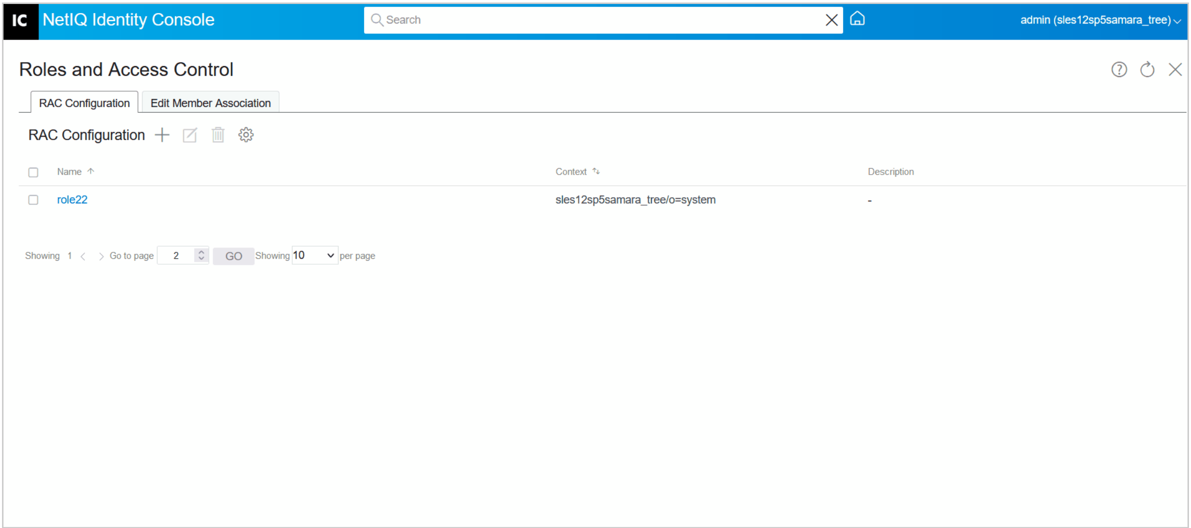
2. On the Context Browser window, select the user as per your requirement.

   The list of associations that the user is already part of are displayed.

3. Click **Edit Member Association** +.
4. On the **Add Roles** window, select the role that is required.
   - **Add Role**: Specify, or use the Object Selector to find the desired object to be a role member.
   - **Add Scope**: Specify, or use the Object Selector to find the scope within which this member can perform the role.
5. Click **OK**.

The roles are added successfully. Close the window and open the Configuration again to view the changes

Figure 35-8 Edit Member Association



Name	Context	Description
role22	sles12sp5samara_tree/o=system	-

Editing Member Associations

- “Modifying: Scope, Assign Rights, Inheritable” on page 229

On the **Edit Member Association** tab, multiple configurations that are created in the RAC that need to be associated with user, group, organization, or organization unit can be performed.

To assign a single or multiple roles to a selected member:

1. Click **Select Member** 🔍.
2. On the **Context Browser** window, select the user as per your requirement.

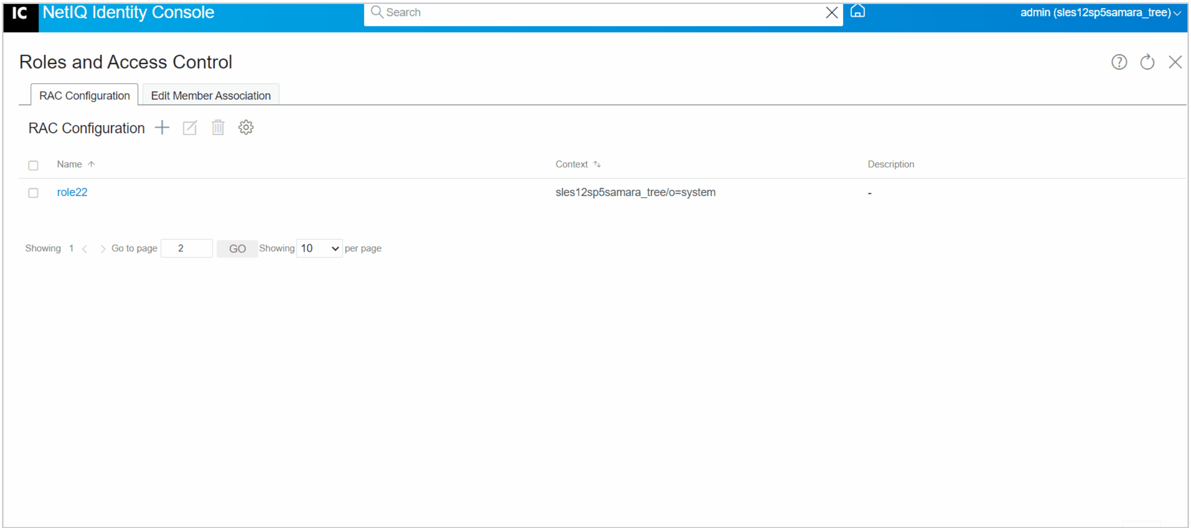
   The list of associations if the user is already part of are displayed.
3. Select the Configuration, and click **Edit Member Association** +.

   The **Add Roles** window appears.
4. Click **Add Roles** +.
5. Select the Configuration that needs to be associated with the particular role, and click **Add**.
6. Click **Scope** 🔍.

   The **Context Browser** window opens. On the **Context Browser** window, you have the option to select user, group, organization unit, or organization.
7. Click **OK**.

Role assignment is complete. Close the window and open the Configuration again to view the changes

Figure 35-9 Edit Member Association



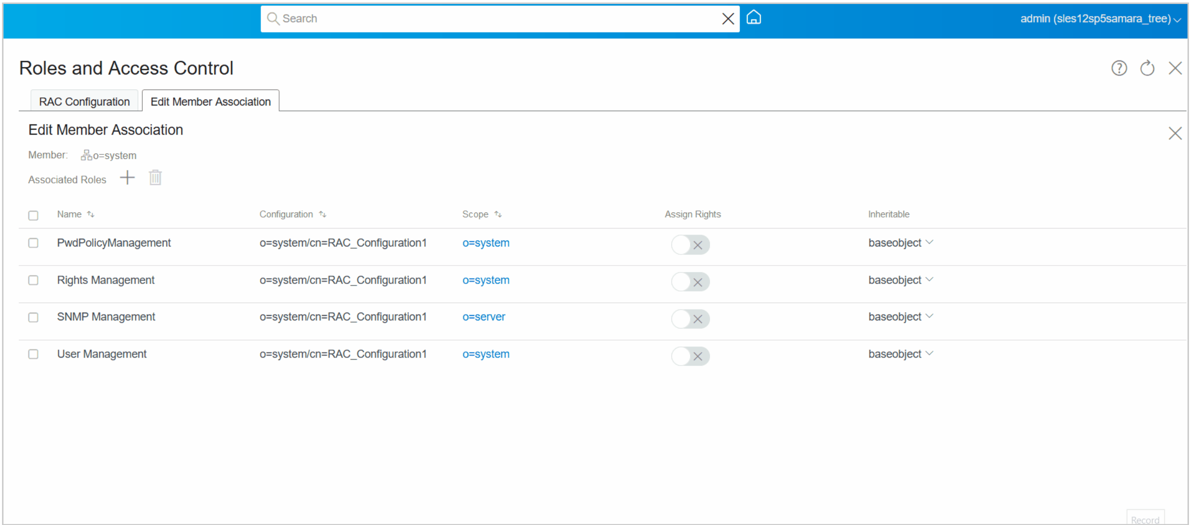
	Name	Context	Description
☐	role22	sles12sp5samara_tree/o=system	-

Modifying: Scope, Assign Rights, Inheritable

Identity Console comes with an option to modify the configuration of the added role. Here, you can modify **Scope**, **Assign Rights**, or **Inheritable**. For a better user experience, the modifications that are made here are saved instantly.

NOTE: When you set the **Assign Rights** as True ✓, only then you can modify the **Inheritable** to **Subtree** or **Base Object**.

Figure 35-10 Modify Scope, Assign Rights, and Inheritable



	Name	Configuration	Scope	Assign Rights	Inheritable
☐	PwdPolicyManagement	o=system/cn=RAC_Configuration1	o=system	✕	baseobject
☐	Rights Management	o=system/cn=RAC_Configuration1	o=system	✕	baseobject
☐	SNMP Management	o=system/cn=RAC_Configuration1	o=server	✕	baseobject
☐	User Management	o=system/cn=RAC_Configuration1	o=system	✕	baseobject

Understanding Force Unrestricted Access

When you start Identity Console, you are granted an access mode based on the rights you have been assigned.

Unrestricted Access: Unrestricted Access is the default access that Identity Console grants before you configure RAC. This access allows you to view the installed roles and tasks. However, to perform any task on Identity Console, you need appropriate access rights.

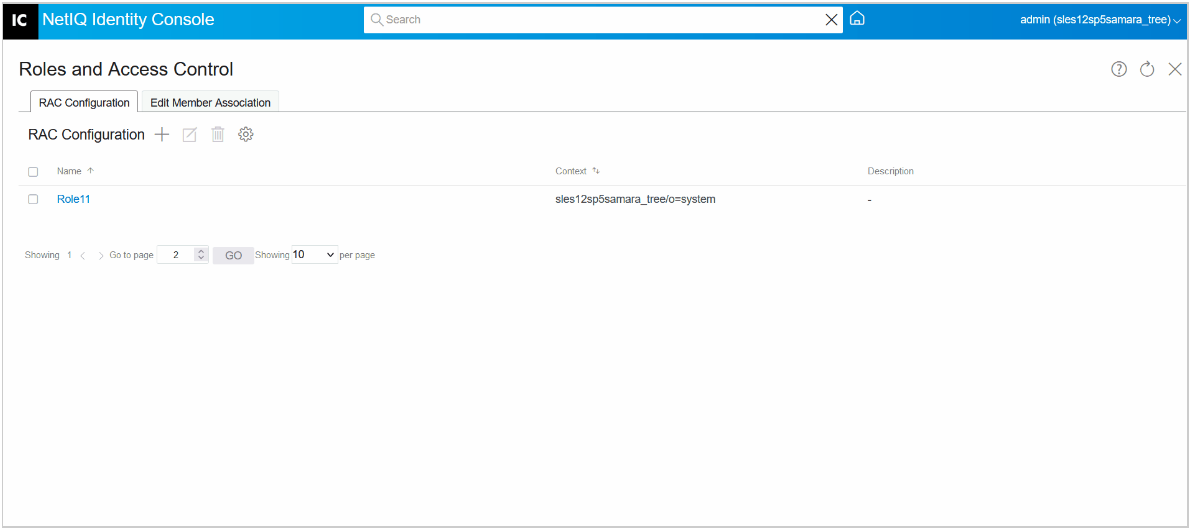
If you are an unauthorized user, and want to view all the Roles and Tasks follow the procedure.

1 Click **Force Unrestricted Access** ⚙.

2 On the RAC CONFIGURATION window, select the check box **Force Unrestricted Access**.

3 Click **Save**.

Figure 35-11 Force Unrestricted Access



☐	Name	Context	Description
☐	Role11	sles12sp5samara_tree/o=system	-

Existence of RBS collection in iManager

When Role Based Service (RBS) collection is not present in the tree, and a new RAC Configuration is created from Identity Console, the next time when iManager is accessed as administrator, it will show the user as Collection Owner, but it will display no roles or tasks available. To override the scenario, enable the **Force Unrestricted Access** in the iManager application as explained:

1 On the iManager home page, Click **Configure** tab.

2 Click **iManager Server** > **Configure iManager** > **RBS**.

3 On the **Configure iManager** window, select the checkbox **Force Unrestricted Access**.

4 Click **Save**.

In another scenario, there are chances of iManager having its own collections. The user may see Identity Console controlled RAC collections under the RBS configuration list. Please do not open or edit the collections objects that are created through Identity Console RAC Management. You can still create new RBS collections in iManager and modify the existing RBS collections created from iManager, but do not change the configurations that are created through Identity Console.

NOTE: RBS Collections that are created through iManager should be managed or edited through iManager only, it is not recommended to edit or modify the Identity Console created Collections through iManager.

Using the eMBox Client

The eMBox Client is a command-line Java client that gives you access to tools such as backup, restore, tree repair, merge, sync, and so on. You can also configure roll-forward logging for multiple servers from a single machine if you have access behind the firewall or through a VPN.

By Configuring RAC (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/b8qqsec.html) in Identity Console (version 1.7.1 onwards), you can perform eMBox tasks remotely using the eMBox Client.

NOTE: While "Setting up RAC Configuration" on page 222, the user must be provided with Tree root level scope to perform eMBox operations in the eDirectory. The eDirectory Maintenance role can also be configured in RAC.

For more information about using the eMBox Client in eDirectory, see: Using the eMBox Client for Backup and Restore (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/agabn4a.html)

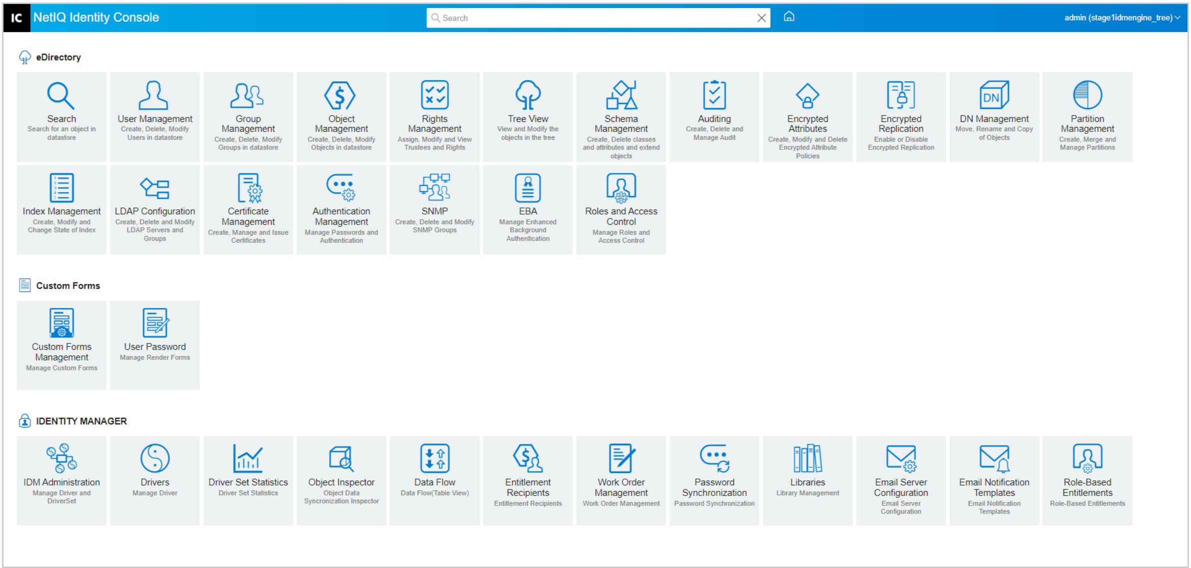
36 Managing Custom Forms

The Custom Forms feature simplifies and reduces the time to create multiple objects. It offers a quick and easy way to streamline the tasks. Use Custom Forms to dynamically create tasks for your most frequently used operations. You can also edit and delete tasks here. For example, to modify a user, instead of selecting Modify Object, you can create a dynamic UI to edit only the attributes that you have selected, such as first name or title. These Tasks can be performed on a single screen without navigating to multiple screens.

NOTE: While using the Custom Forms, NetIQ recommends that you do not run multiple Identity Console servers using the same RAC.

- "Managing Custom Forms" on page 233
- "Managing Render Forms" on page 237
- "Tasks to Modify" on page 238
- "Tasks to Delete" on page 239

Figure 36-1 *Home Screen with Custom Forms & Rendered Form*


IC
NetIQ Identity Console
Search
admin (stage1idmengine_tree)
eDirectory
Search
Search for an object in datastore
User Management
Create, Delete, Modify Users in datastore
Group Management
Create, Delete, Modify Groups in datastore
Object Management
Create, Delete, Modify Objects in datastore
Rights Management
Assign, Modify and View Trustees and Rights
Tree View
View and Modify the objects in the tree
Schema Management
Create, Delete classes and attributes and extend objects
Auditing
Create, Delete and Manage Audit
Encrypted Attributes
Create, Modify and Delete Encrypted Attribute Policies
Encrypted Replication
Enable or Disable Encrypted Replication
DN Management
Move, Rename and Copy of Objects
Partition Management
Create, Merge and Manage Partitions
Index Management
Create, Modify and Change State of Index
LDAP Configuration
Create, Delete and Modify LDAP Servers and Groups
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
Roles and Access Control
Manage Roles and Access Control
Custom Forms
Custom Forms Management
Manage Custom Forms
User Password
Manage Render Forms
IDENTITY MANAGER
IDM Administration
Manage Driver and DriverSet
Drivers
Manage Driver
Driver Set Statistics
Driver Set Statistics
Object Inspector
Object Data Syncronization Inspector
Data Flow
Data Flow(Table View)
Entitlement Recipients
Entitlement Recipients
Work Order Management
Work Order Management
Password Synchronization
Password Synchronization
Libraries
Library Management
Email Server Configuration
Email Server Configuration
Email Notification Templates
Email Notification Templates
Role-Based Entitlements
Role-Based Entitlements

Managing Custom Forms

The following sections explain how to create, modify, delete, and import or export forms.

- "Task to Create Custom Forms" on page 234
- "Modifying Custom Forms" on page 235
- "Deleting Custom Forms" on page 236

- “Copying Custom Forms” on page 236
- “Importing Custom Forms” on page 237
- “Exporting Custom Forms” on page 237

Task to Create Custom Forms

The following procedure explains how to create a Custom Form.

NOTE: Before creating the Custom Forms, ensure that the RAC Configuration exists in the tree.

---

1 Click **Custom Forms Management**.

2 On the **Custom Forms Management** page, click ⊞.

The **Custom Forms Builder** page opens.

3 Select the **Task Type**.

4 Select the class from the **Available Classes**.

5 (Optional) Add a description in the **Description** field.

6 If you want to specify any additional attribute, select **Add Aux Class** checkbox.

The available Aux Classes list appears.

6a Select the required Aux Class that provides the required attributes.

7 Click **Next**.

A **Custom Forms Builder** page with **Available Attributes (Class)** list and **Control Properties** appears.

8 Enter a name in the **Name** field.

9 Select the **RAC Configuration**.

10 Select a **Module Name**.

10a If a new module is required, click ⊞.

11 (Optional) Select a **Role**.

12 Select the required attributes from the list.

You can change the hierarchy of the attributes by double-click on any Attribute > drag up or down.

13 (Optional) Double-click on the attribute to add the **Control Properties**. The following are the options to customize your Attributes.

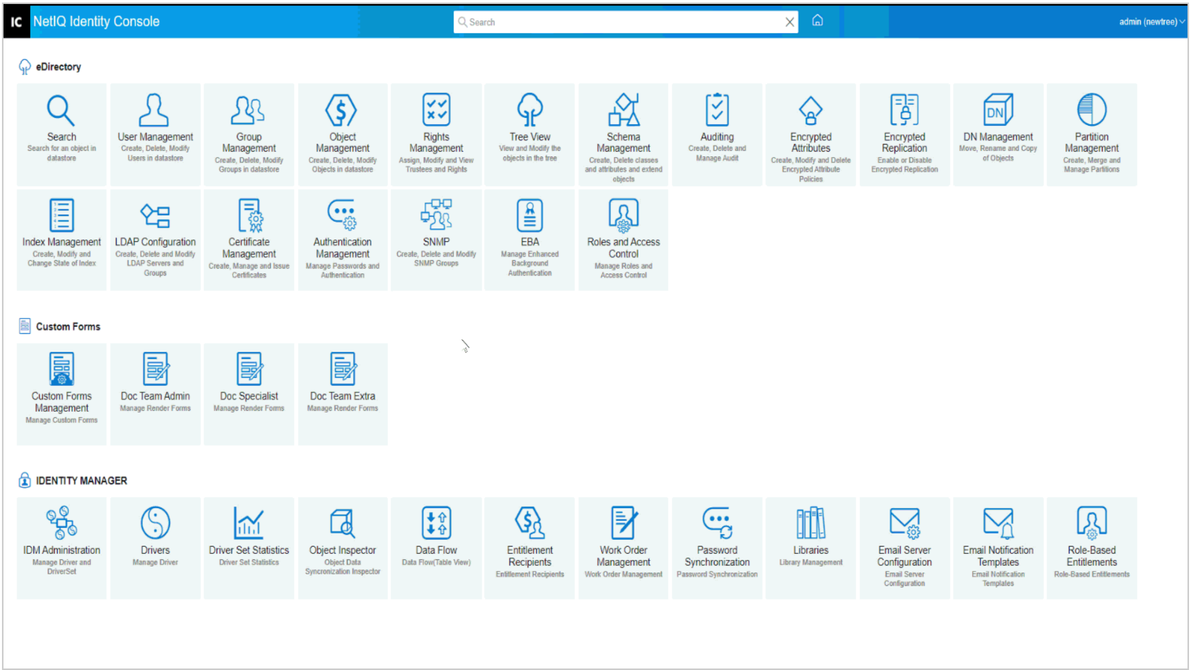
- **Mandatory:** When the mandatory checkbox is selected, the user cannot leave the field empty.
- **Read Only:** Read-only fields allow the user to view information, but not change the data. In addition, eDirectory attribute fields that are marked readonly gives only read rights through Roles and Access Control.
- **Single Valued:** If a control is marked as single valued, the control will not let the user enter more than one value.
- **Label:** Customize the name of the attribute as per your requirement, for example: Change the text **Last-name** to **Surname**.

- **Regular Expression:** A Java-script regular expression that all values must match. If values do not match the regular expression, the error message that is created will be shown.
- **Error Message:** An error message that will be shown if a value does not match the regular Expression parameter.
- **Pre-defined Values:** This field can be utilized to create a predefined list of value(s).
- **Lower Bound:** The lower bound that will be used to validate the field values. If the syntax of the field is Counter, Integer, or Interval the field is a numerical lower bound. Otherwise, it is the lower bound on the length of the string.
- **Upper Bound:** The upper bound that will be used to validate the field values. If the syntax of the field is Counter, Integer, or Interval the field is a numerical upper bound. Otherwise, it is the upper bound on the length of the string.

14 Click Create.

The **Custom Form Created Successfully** message appears.

Figure 36-2 *Task to Create Custom Forms*


IC
NetIQ Identity Console
Search
admin (newtree)
eDirectory
Search
Search for an object in datastore
User Management
Create, Delete, Modify Users in datastore
Group Management
Create, Delete, Modify Groups in datastore
Object Management
Create, Delete, Modify Objects in datastore
Rights Management
Assign, Modify and View Trustees and Rights
Tree View
View and Modify the objects in the tree
Schema Management
Create, Delete classes and attributes and extend objects
Auditing
Create, Delete and Manage Audit
Encrypted Attributes
Create, Modify and Delete Encrypted Attribute Policies
Encrypted Replication
Enable or Disable Encrypted Replication
DN Management
Move, Rename and Copy of Objects
Partition Management
Create, Merge and Manage Partitions
Index Management
Create, Modify and Change State of Index
LDAP Configuration
Create, Delete and Modify LDAP Servers and Groups
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
Roles and Access Control
Manage Roles and Access Control
Custom Forms
Custom Forms Management
Manage Custom Forms
Doc Team Admin
Manage Render Forms
Doc Specialist
Manage Render Forms
Doc Team Extra
Manage Render Forms
IDENTITY MANAGER
IDM Administration
Manage Driver and DriverSet
Drivers
Manage Driver
Driver Set Statistics
Driver Set Statistics
Object Inspector
Object Data Syncronization Inspector
Data Flow
Data Flow(Table View)
Entitlement Recipients
Entitlement Recipients
Work Order Management
Work Order Management
Password Synchronization
Password Synchronization
Libraries
Library Management
Email Server Configuration
Email Server Configuration
Email Notification Templates
Email Notification Templates
Role-Based Entitlements
Role-Based Entitlements

Modifying Custom Forms

The following procedure explains how to modify a Custom Form.

1 Click **Custom Forms Management**.

The **Custom Forms Management** page appears.

2 Select the checkbox against the Form that needs to be modified > click **Update Form** .

The **Custom Forms Builder** page opens with a list of all the Attributes.

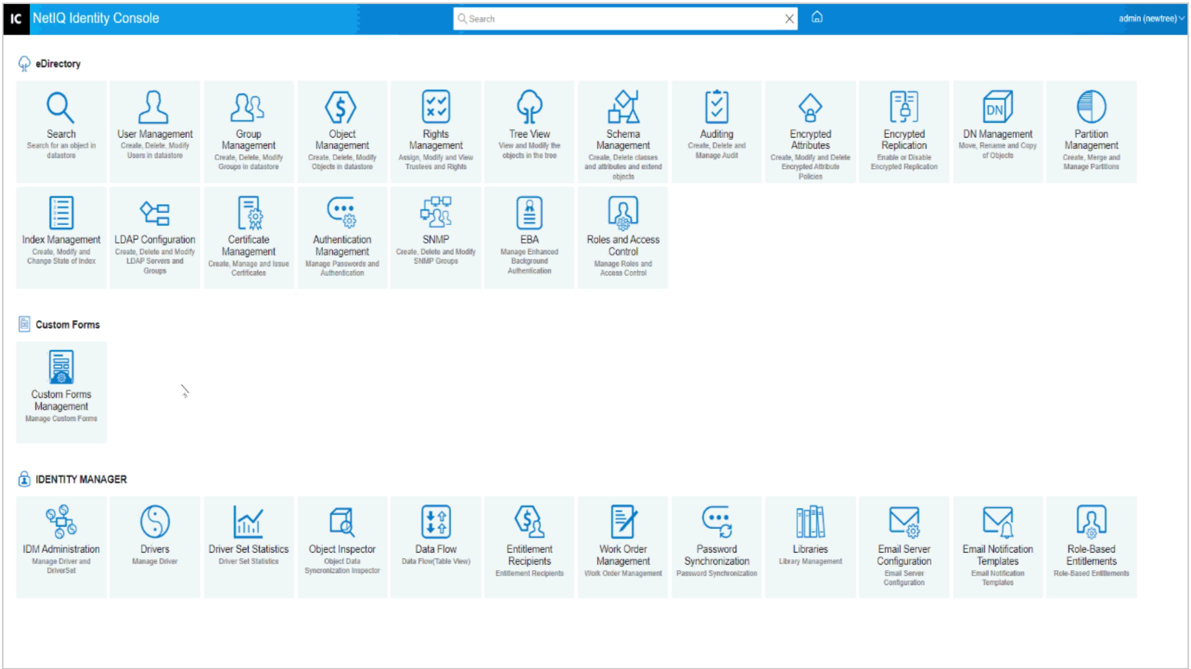
NOTE: The user cannot modify the **Name, RAC Configuration, Module Name, and Role (Optional)** fields.

---

3. Edit or add the required **Available Attributes (Class).**
4. Edit or add the required **Control Properties**.
5. Click Save.

   The **Form Modified Successfully** message appears.

Figure 36-3 Modify Custom Form


IC
NetIQ Identity Console
Search
admin (newtree)
eDirectory
Search
Search for an object in datastore
User Management
Create, Delete, Modify Users in datastore
Group Management
Create, Delete, Modify Groups in datastore
Object Management
Create, Delete, Modify Objects in datastore
Rights Management
Assign, Modify and View Trustees and Rights
Tree View
View and Modify the objects in the tree
Schema Management
Create, Delete classes and attributes and extend objects
Auditing
Create, Delete and Manage Audit
Encrypted Attributes
Create, Modify and Delete Encrypted Attribute Policies
Encrypted Replication
Enable or Disable Encrypted Replication
DN Management
Move, Rename and Copy of Objects
Partition Management
Create, Merge and Manage Partitions
Index Management
Create, Modify and Change State of Index
LDAP Configuration
Create, Delete and Modify LDAP Servers and Groups
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
Roles and Access Control
Manage Roles and Access Control
Custom Forms
Custom Forms Management
Manage Custom Forms
IDENTITY MANAGER
IDM Administration
Manage Driver and DriverSet
Drivers
Manage Driver
Driver Set Statistics
Driver Set Statistics
Object Inspector
Object Data Syncronization Inspector
Data Flow
Data Flow(Table View)
Entitlement Recipients
Entitlement Recipients
Work Order Management
Work Order Management
Password Synchronization
Password Synchronization
Libraries
Library Management
Email Server Configuration
Email Server Configuration
Email Notification Templates
Email Notification Templates
Role-Based Entitlements
Role-Based Entitlements

Deleting Custom Forms

1. Click **Custom Forms Management**.

   The **Custom Forms Management** page appears.

2. Select the checkbox against the Form that needs to be deleted. Then click 🗑.
3. A **Delete Confirm** page appears. Click **OK** to delete.

   The **Form(s) Deleted Successfully** message appears.

Copying Custom Forms

1. Click **Custom Forms Management**.

   The **Custom Forms Management** page appears.

2. Select the checkbox against the Form that needs to be copied.
3. Click Copy Form .

   A **Custom Forms Builder** page with **Available Attributes (Class)** list and **Control Properties** will appear.

4. Edit **Available Attributes (Class)** list and **Control Properties** as required.
5. Edit the **Name, RAC Configuration, Module Name, and Role (Optional)** fields.

6 Click Create.

   The **Custom Form Created Successfully** message appears.

7 Click **OK.**

Importing Custom Forms

The following procedure explains importing a Custom Form onto the Identity Console server.

NOTE: While importing the form containing the custom Classes and Attributes, ensure to create related Object Classes and Attributes in your schema.

---

1 On the **Custom Form Management** page, click Import Form.

   The Import Forms page appears. Navigate to the folder where your file is present

2 Select the `CustomForms.json` file that you want to import.

3 Select the **RAC Collection** into which you want to import the Custom Form.

4 Click **OK**.

Exporting Custom Forms

The following procedure explains how to export a Custom Form, making them deployable to other Identity Console servers.

1 On the **Custom Form Management** page, select the check-box of Custom Form(s) that needs to be exported.

2 Click Export Form.

Managing Render Forms

To create a new Tile of the rendered Form on the Identity Console home page, you must render a required Form, and Create a Role in RAC, and then Associate a Task to that Role.

The following procedure explains how to Render a Form.

1 On the Identity Console home page click **Roles and Access Control** > Select the required Collection.

2 On the **Roles** tab Create a Role for that Custom Form.

For more information see the section: Creating a New Role from Roles and Access Control.

After completing the above procedure, the Rendered Form tile will be visible on the Identity Console home page.

Tasks to Modify

This feature helps the user in simplifying the modification of forms. The following procedure explains how to modify a form.

1. Click **Custom Forms Management**.
2. On the **Customs Forms Management** page, click +.

   The **Custom Forms Builder** page opens.
3. Select the **Task Type** as **Tasks to Modify**.
4. Select the required class from the **Available Classes**.
5. (Optional) Add a description in the **Description** field.
6. If you want to specify any additional attribute, select **Add Aux Class** checkbox.

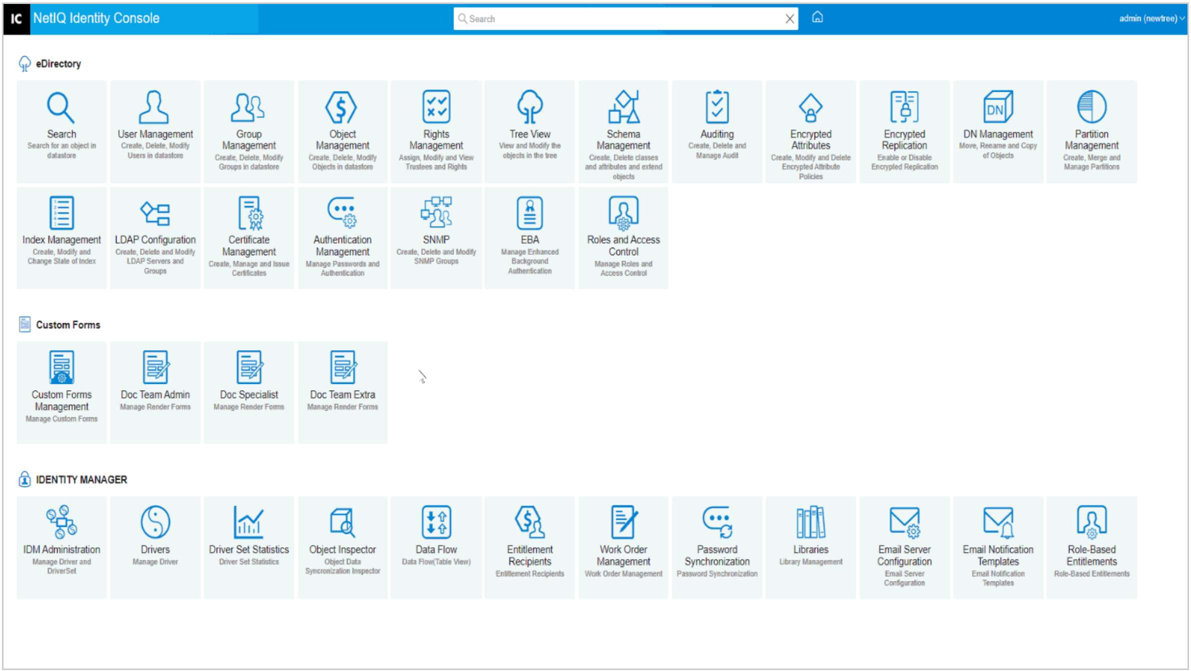
   The available Aux Classes lists appears.

   6a Select the required Aux Class that provides the required attributes.
7. Click **Next**.

   A **Custom Forms Builder** page with **Available Attributes (Class)** list will appear.
8. At the **Name** field provide a modified name.
9. Select the required **RAC Configuration**.
10. Select the **Available Attributes (Class)**.
11. Select a **Module Name**.
12. (Optional) Select a **Role**.
13. Click Create.

    The modified Form is listed in the **Custom Forms Management** page.

Figure 36-4 Task to Modify


IC
NetIQ Identity Console
Search
admin (newtree)
eDirectory
Search
Search for an object in datastore
User Management
Create, Delete, Modify Users in datastore
Group Management
Create, Delete, Modify Groups in datastore
Object Management
Create, Delete, Modify Objects in datastore
Rights Management
Assign, Modify and View Trustees and Rights
Tree View
View and Modify the objects in the tree
Schema Management
Create, Delete classes and attributes and extend objects
Auditing
Create, Delete and Manage Audit
Encrypted Attributes
Create, Modify and Delete Encrypted Attribute Policies
Encrypted Replication
Enable or Disable Encrypted Replication
DN Management
Move, Rename and Copy of Objects
Partition Management
Create, Merge and Manage Partitions
Index Management
Create, Modify and Change State of Index
LDAP Configuration
Create, Delete and Modify LDAP Servers and Groups
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
Roles and Access Control
Manage Roles and Access Control
Custom Forms
Custom Forms Management
Manage Custom Forms
Doc Team Admin
Manage Render Forms
Doc Specialist
Manage Render Forms
Doc Team Extra
Manage Render Forms
IDENTITY MANAGER
IDM Administration
Manage Driver and DriverSet
Drivers
Manage Driver
Driver Set Statistics
Driver Set Statistics
Object Inspector
Object Data Syncronization Inspector
Data Flow
Data Flow(Table View)
Entitlement Recipients
Entitlement Recipients
Work Order Management
Work Order Management
Password Synchronization
Password Synchronization
Libraries
Library Management
Email Server Configuration
Email Server Configuration
Email Notification Templates
Email Notification Templates
Role-Based Entitlements
Role-Based Entitlements

Tasks to Delete

This feature helps the user in deleting the forms. The following procedure explains how to delete a form

1. Click **Custom Forms Management**.
2. On the **Customs Forms Management** page, click +.

   The **Custom Forms Builder** page opens.
3. Select the **Task Type** as **Tasks to Delete**.
4. Select the required class from the **Available Classes**.
5. (Optional) Add a description in the **Description** field.
6. Provide a name in the **Name** field.
7. Select the **RAC Configuration**.
8. Select a **Module Name**.
   - **8a** If a new module is required, click +.
9. (Optional) Select a **Role**.
10. Click Create.

    The **Custom Form Created Successfully** message appears.

37 Managing External Application

External Application is a new feature that helps Administrators or Role Associated members to launch an externally configured application (that is configured with OSP). The functionalities can be accessed by the users directly from the home page of the Identity Console. The External Application helps administrators to create configurations that are assigned as Tasks to the Users through Roles. When an end user login, only those specific tiles that are configured by the Administrator will be visible to the User as a Tiles. The User can log in to his workspace without entering any credentials, which makes the login process smooth and seamless. Identity Console acts as a Home page to all other applications of Identity Manager, such as User Apps, Identity Reporting, and so on.

NOTE: Before configuring the External Applications, ensure:

- The RAC Configuration exists in the tree.
- Configure a whitelist of trusted URLs in the Identity Console. For more information see: Configure a Whitelist of Target URLs

---

- “Configure External Applications” on page 241

Configure External Applications

- “Modify External Applications” on page 242
- “Delete External Applications” on page 242

The following procedure explains how to configure External application Tiles.

1. Login to Identity Console as Administrator.
2. On the Home Screen of the Identity Console, click **External Applications**.
3. Click **Create** +.

   Create External Application page appears.
4. Give a **Name** to the tile.
5. Choose an **External Application Icon** 🗎 > click **OK**.
6. Give a description.
7. Select the required **RAC Configuration**.

   For more information see: “Configuration of RAC” on page 221
8. Click **Module Name** > Add a New Module > Select an Icon for the Module (Optional) > click **OK**.
9. Select a **Role**.
10. Select an **External Application URL** where the application should redirect to.

    For more information see: Configuring a Whitelist of Target URLs.

11 Click **Create** Create.

The **Configuration Created Successfully** message appears.

NOTE: The administrator must ensure that all the Clients are directed to the same Open Service Platform (OSP). The credentials must be saved in the same OSP. If not, the application is redirected to the Login page of the Identity Console.

Modify External Applications

The following procedure explains how to modify External application Tiles. The Administrator can modify only the Description and External Application URL.

1. On the **Manage External Applications** page select the Tile that needs to be modified and then click ✎ icon.
2. On the **Modify External Application** window, modify the description, and modify the URL.
3. Click **Save**.

Delete External Applications

The following procedure explains how to delete External application Tiles. The Administrator can delete only the Description and External Application URL.

1. On the **Manage External Applications** page select the Tile that needs to be deleted and then click 🗑 icon.
2. Click **OK**.

38 Best Practices and Common Questions

This section includes some tips and best practices while using Identity Console. If you find something that works well for you, please share it at Cool Solutions (http://www.novell.com/coolsolutions).

- "How to Overcome Identity Console Slowdown, when RAC is Configured" on page 243
- "Configuring Identity Console as Reverse Proxy" on page 243
- "RAC Configuration for Administrator" on page 244

For the Identity Console to perform at its best, use latest supported browser, and clear the browser cache and cookies at regular intervals.

How to Overcome Identity Console Slowdown, when RAC is Configured

When you experience slowness in loading of the Identity Console application, create the following indexes to improve the performance.

- Value index on `rbsparameter`.
- Substring index on `rbsxmlinfo`.
- Value Index on object class.

To create Index refer: https://www.netiq.com/documentation/identity-console/identity_console-admin/data/createindex.html (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/createindex.html)

Configuring Identity Console as Reverse Proxy

The following procedure explain how to configure the Reverse Proxy.

1. Open the `edirapi` configuration file. Default path: `/etc/opt/novell/eDirAPI/conf/edirapi.conf`.
2. Change the existing osp-redirect URL: `https://<dnsname:port>/eDirAPI/v1/idmdc1_tree/authcoderedirect` to Reverse Proxy URL: `https://<Published DNS Name>/eDirAPI/v1/idmdc1_tree/authcoderedirect`

   Example:

   Default osp-redirect URL: `https://idconsoledc1.extremelyfocused.intra:9000/eDirAPI/v1/idmdc1_tree/authcoderedirect`.

   Changed osp-redirect URL: `https://idc.extremelyfocused.solutions/eDirAPI/v1/idmdc1_tree/authcoderedirect`.
3. Restart Identity Console.

For more information see: Reverse Proxy Based Single Sign-On (https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin/data/reverse-proxy-based-single-sign-on.html).

RAC Configuration for Administrator

For the administrator to access all the modules, it is advisable to create a separate RAC Configuration for the administrator with all the Modules selected.