Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

Copyright (C) 2019 NetIQ Corporation. All rights reserved.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this Book and the Library</td>
<td>9</td>
</tr>
<tr>
<td>About NetIQ Corporation</td>
<td>11</td>
</tr>
<tr>
<td>Part I Overview of Identity Manager Environment</td>
<td>13</td>
</tr>
<tr>
<td>1 Brief Introduction of Identity Manager Components</td>
<td>15</td>
</tr>
<tr>
<td>Identity Manager Server Components</td>
<td>16</td>
</tr>
<tr>
<td>Identity Manager Server</td>
<td>17</td>
</tr>
<tr>
<td>Remote Loader</td>
<td>17</td>
</tr>
<tr>
<td>Fanout Agent</td>
<td>18</td>
</tr>
<tr>
<td>iManager</td>
<td>18</td>
</tr>
<tr>
<td>Identity Applications Components</td>
<td>19</td>
</tr>
<tr>
<td>User Application</td>
<td>19</td>
</tr>
<tr>
<td>Authentication Service</td>
<td>19</td>
</tr>
<tr>
<td>Self-Service Password Reset</td>
<td>19</td>
</tr>
<tr>
<td>Web Application Server</td>
<td>20</td>
</tr>
<tr>
<td>Identity Applications Database</td>
<td>20</td>
</tr>
<tr>
<td>Drivers for Identity Applications</td>
<td>21</td>
</tr>
<tr>
<td>Identity Reporting Components</td>
<td>21</td>
</tr>
<tr>
<td>Identity Reporting</td>
<td>21</td>
</tr>
<tr>
<td>Authentication Service</td>
<td>22</td>
</tr>
<tr>
<td>Self-Service Password Reset</td>
<td>22</td>
</tr>
<tr>
<td>Identity Reporting Database</td>
<td>22</td>
</tr>
<tr>
<td>Web Application Server</td>
<td>22</td>
</tr>
<tr>
<td>Drivers for Identity Reporting</td>
<td>23</td>
</tr>
<tr>
<td>Sentinel Log Management for Identity Governance and Administration</td>
<td>23</td>
</tr>
<tr>
<td>Identity Manager Tools</td>
<td>24</td>
</tr>
<tr>
<td>Designer for Identity Manager</td>
<td>24</td>
</tr>
<tr>
<td>Analyzer for Identity Manager</td>
<td>24</td>
</tr>
<tr>
<td>Functional Architecture</td>
<td>25</td>
</tr>
<tr>
<td>Deployment Options for Identity Manager</td>
<td>26</td>
</tr>
<tr>
<td>Sample Identity Manager Deployments</td>
<td>27</td>
</tr>
<tr>
<td>Sample Advanced Edition Deployment</td>
<td>29</td>
</tr>
<tr>
<td>Sample Standard Edition Deployment</td>
<td>30</td>
</tr>
<tr>
<td>Part II Planning to Install Identity Manager</td>
<td>33</td>
</tr>
<tr>
<td>2 Planning Your Installation</td>
<td>35</td>
</tr>
<tr>
<td>Determine Hardware Requirements</td>
<td>35</td>
</tr>
<tr>
<td>Deployment Planning Worksheet</td>
<td>36</td>
</tr>
<tr>
<td>Sizing Worksheet</td>
<td>36</td>
</tr>
<tr>
<td>Architecture Worksheet</td>
<td>37</td>
</tr>
<tr>
<td>System Requirements Worksheet</td>
<td>37</td>
</tr>
<tr>
<td>Reviewing the Ports Used by the Identity Manager Components</td>
<td>38</td>
</tr>
</tbody>
</table>
Part III Installing and Configuring Identity Manager Components

3 Installation and Configuration Process Overview

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Order</td>
<td>43</td>
</tr>
<tr>
<td>Understanding the Installation and Configuration Process for Identity Manager Server, Identity Applications, and Identity Reporting Components</td>
<td>43</td>
</tr>
<tr>
<td>Types of Installation Methods</td>
<td>44</td>
</tr>
<tr>
<td>Installation Options</td>
<td>44</td>
</tr>
<tr>
<td>Types of Configuration Modes</td>
<td>44</td>
</tr>
<tr>
<td>Using Non-Intuitive Passwords During Configuration</td>
<td>45</td>
</tr>
<tr>
<td>Understanding the Installation Process for Designer and Analyzer</td>
<td>45</td>
</tr>
<tr>
<td>Installation Procedures</td>
<td>45</td>
</tr>
<tr>
<td>Installation Procedures for Identity Manager Server, Identity Applications, and Identity Reporting</td>
<td>45</td>
</tr>
<tr>
<td>Installing Remote Loader</td>
<td>47</td>
</tr>
<tr>
<td>Installing Java Remote Loader</td>
<td>48</td>
</tr>
<tr>
<td>Installing .NET Remote Loader</td>
<td>50</td>
</tr>
<tr>
<td>Installing SSPR</td>
<td>50</td>
</tr>
<tr>
<td>Types of Configuration Settings</td>
<td>51</td>
</tr>
<tr>
<td>Configuration Worksheet for Identity Manager Engine</td>
<td>51</td>
</tr>
<tr>
<td>Configuration Worksheet for Identity Applications</td>
<td>53</td>
</tr>
<tr>
<td>Configuration Worksheet for Identity Reporting</td>
<td>55</td>
</tr>
<tr>
<td>Configuration Worksheet for Self-Service Password Reset</td>
<td>57</td>
</tr>
<tr>
<td>Post-Installation Steps</td>
<td>58</td>
</tr>
<tr>
<td>Passing the preferIPv4Stack Property to JVM</td>
<td>58</td>
</tr>
<tr>
<td>Checking the Health of the Server</td>
<td>59</td>
</tr>
<tr>
<td>Monitoring the Health Statistics</td>
<td>59</td>
</tr>
<tr>
<td>Creating Compound Indexes</td>
<td>60</td>
</tr>
<tr>
<td>Configuring Identity Application to Reject Client-initiated SSL Renegotiation</td>
<td>60</td>
</tr>
</tbody>
</table>

4 Final Steps for Completing the Installation

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the Identity Vault</td>
<td>63</td>
</tr>
<tr>
<td>Manually Importing Identity Applications and Identity Reporting Certificates into Identity Vault</td>
<td>63</td>
</tr>
<tr>
<td>Configuring the Remote Loader and Drivers</td>
<td>64</td>
</tr>
<tr>
<td>Configuring Forgotten Password Management</td>
<td>64</td>
</tr>
<tr>
<td>Using Self Service Password Reset for Forgotten Password Management</td>
<td>64</td>
</tr>
<tr>
<td>Using an External System for Forgotten Password Management</td>
<td>66</td>
</tr>
<tr>
<td>Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment</td>
<td>68</td>
</tr>
<tr>
<td>Configuring the Database for the Identity Applications</td>
<td>68</td>
</tr>
<tr>
<td>Configuring an Oracle Database</td>
<td>69</td>
</tr>
<tr>
<td>Configuring a SQL Server Database</td>
<td>70</td>
</tr>
<tr>
<td>Configuring Identity Applications</td>
<td>71</td>
</tr>
<tr>
<td>Configuring the Settings for the Identity Applications</td>
<td>71</td>
</tr>
<tr>
<td>Deploying REST APIs for Identity Applications</td>
<td>93</td>
</tr>
<tr>
<td>Accessing the Oracle Database Using Oracle Service Name</td>
<td>93</td>
</tr>
<tr>
<td>Manually Creating the Database Schema</td>
<td>94</td>
</tr>
<tr>
<td>Configuring Single Sign-On Settings for the Identity Applications</td>
<td>95</td>
</tr>
<tr>
<td>Starting the Identity Applications</td>
<td>96</td>
</tr>
<tr>
<td>Configuration and Usage Considerations for the Identity Applications</td>
<td>96</td>
</tr>
<tr>
<td>Configuring the Runtime Environment for Data Collection</td>
<td>96</td>
</tr>
</tbody>
</table>
Part VI Upgrading Identity Manager 133

10 Preparing to Upgrade Identity Manager 135

Checklist for Upgrading Identity Manager .......................................................... 135
Understanding Upgrade and Migration ............................................................... 137
Upgrade Order ................................................................................................. 138
Supported Upgrade Paths .................................................................................. 138
   Upgrading from Identity Manager 4.7.x Versions ......................................... 138
   Upgrading from Identity Manager 4.6.x Versions ......................................... 140
Backing Up the Current Configuration .............................................................. 142
   Exporting the Designer Project .................................................................. 142
   Exporting the Configuration of the Drivers .................................................. 143

11 Upgrading Identity Manager Components 145

Upgrading Designer ................................................................. 145
Upgrading the Identity Manager Engine Components ......................................... 146
   Upgrading the Identity Vault .................................................................... 146
   Upgrading the Identity Manager Engine .................................................... 147
   Upgrading the Remote Loader .................................................................. 149
   Upgrading the Java Remote Loader ............................................................ 150
   Upgrading iManager ................................................................................... 150
Upgrading Identity Applications ................................................................. 152
   Understanding the Upgrade Program ......................................................... 153
   Prerequisite for Upgrade .......................................................................... 153
   System Requirements ................................................................................ 154
Upgrading the PostgreSQL Database ............................................................... 154
Upgrading the Identity Manager Engine Components ......................................... 146
Upgrading Identity Reporting ........................................................................... 160
   Prerequisite for Upgrade .......................................................................... 160
   Upgrading Identity Reporting .................................................................. 160
   Post-upgrade Steps for Reporting ............................................................... 161
   Changing the References to reportRunner in the Database ....................... 161
   Verifying the Upgrade for Identity Reporting ............................................ 162
Upgrading Analyzer ......................................................................................... 162
Stopping and Starting Identity Manager Drivers ................................................. 162
   Stopping the Drivers ................................................................................ 162
   Starting the Drivers .................................................................................. 163
Upgrading the Identity Manager Drivers ........................................................... 165
   Creating a New Driver .............................................................................. 165
   Replacing Existing Content with Content from Packages ......................... 165
   Keeping the Current Content and Adding New Content with Packages .... 166
Adding New Servers to the Driver Set .............................................................. 166
   Adding the New Server to the Driver Set .................................................... 167
   Removing the Old Server from the Driver Set .......................................... 167
Restoring Custom Policies and Rules to the Driver ............................................ 168
   Using Designer to Restore Custom Policies and Rules to the Driver .......... 168
   Using iManager to Restore Custom Policies and Rules to the Driver ......... 169
Part VII  Migrating Identity Manager Data to a New Installation

13 Preparing to Migrate Identity Manager 175

Checklist for Performing a Migration 175

14 Migrating Identity Manager to a New Server 177

Checklist for Migrating Identity Manager 177

Preparing Your Designer Project for Migration 178

Copying Server-specific Information for the Driver Set
   Copying the Server-specific Information in Designer 179
   Changing the Server-specific Information in iManager 180
   Changing the Server-specific Information for the User Application 180

Migrating the Identity Manager Engine to a New Server 180

Migrating the User Application Driver 181
   Importing a New Base Package 181
   Upgrading an Existing Base Package 181
   Deploying the Migrated Driver 182

Upgrading the Identity Applications 182

Migrating Identity Applications 182
   Migrating the Database to the New Server 183
   Installing Identity Applications on the New Server 184

Completing the Migration of the Identity Applications 184
   Preparing an Oracle Database for the SQL File 184
   Flushing the Browser Cache 185
   Updating the Maximum Timeout Setting for the SharedPagePortlet 185
   Disabling the Automatic Query Setting for Groups 186

Part VIII  Deploying Identity Manager on Microsoft Azure

15 Planning and Implementation of Identity Manager on Microsoft Azure 189

Prerequisites 189

Deployment Procedure 189
   Creating a Resource Group 191
   Creating a Virtual Network and Subnet 191
   Creating an Application Gateway 192
   Creating a Virtual Machine Instance 193
   Updating host entries in VM 194
   Setting Up Designer 196
   Configuring the Application Gateway 196

16 Example Scenarios of Hybrid Identity Manager

Using Multi-Server Driver Set Connection 199
Using eDirectory Driver Connection 200
17 Uninstalling Identity Manager Components ................................................. 201
  Uninstalling the Identity Vault ...................................................................... 201
  Removing Objects from the Identity Vault ..................................................... 202
  Uninstalling the Identity Manager Engine ................................................... 202
  Uninstalling the Remote Loader .................................................................. 202
  Uninstalling the Identity Applications ......................................................... 203
    Deleting the Drivers for the Roles Based Provisioning Module .................. 203
    Uninstalling the Identity Applications ..................................................... 203
  Uninstalling the Identity Reporting Components ....................................... 204
    Deleting the Reporting Drivers .................................................................. 204
    Uninstalling Identity Reporting ............................................................... 204
  Uninstalling Analyzer .................................................................................. 205
  Uninstalling iManager .................................................................................. 205
    Uninstalling iManager on Windows ......................................................... 205
    Uninstalling iManager Workstation ......................................................... 205
  Uninstalling Designer .................................................................................. 206

Part IX Deploying Identity Manager for High Availability ............................. 207

18 Preparing for Installing Identity Manager in a Cluster Environment .......... 209
  Prerequisites .................................................................................................. 209
    Identity Vault .............................................................................................. 209
    Identity Applications .................................................................................... 210
    Database for Identity Applications ............................................................ 210
  Preparing a Cluster for the Identity Applications ....................................... 211
    Understanding Cluster Groups in Tomcat Environments .......................... 211
    Setting System Properties for Workflow Engine IDs ............................... 211
    Using the Same Master Key for Each User Application in the Cluster ....... 211

19 Sample Identity Manager Cluster Deployment Solution .......................... 213
  Prerequisites .................................................................................................. 213
  Configuring NetIQ Identity Manager on eDirectory Cluster ....................... 213
  Clustering Remote Loader ............................................................................ 214

20 Sample Identity Applications Cluster Deployment Solution .................... 215
  Prerequisites .................................................................................................. 216
  Installation Procedure .................................................................................... 217
  Enabling the Permission Index for Clustering .............................................. 222

21 Troubleshooting ......................................................................................... 223
  Troubleshooting Identity Manager Engine .................................................. 223
  Troubleshooting the Identity Applications and RBPM Installation .............. 224
  Troubleshooting Installation and Uninstallation ......................................... 226
  Troubleshooting Login .................................................................................. 230
  Troubleshooting SSPR Page Request Error ................................................ 232
  Troubleshooting .NET Remote Loader Not Starting Issue on Windows 2016 233
  Troubleshooting 502 Bad gateway while loading the forms in Azure deployment 233
About this Book and the Library

The Setup Guide provides instructions for installing the NetIQ Identity Manager (Identity Manager) product. This guide describes the process for installing individual components in a distributed environment.

Intended Audience

This book provides information for identity architects and identity administrators responsible for installing the components necessary for building an identity management solution for their organization.

Other Information in the Library

For more information about the library for Identity Manager, see the Identity Manager documentation website.
About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new
In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

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

Our Philosophy

Selling intelligent solutions, not just software
In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

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

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management
Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

This guide focuses on the tasks that you must complete in order to install and configure Identity Manager. Before you start with the installation

If you are new to NetIQ Identity Manager, the information in the below sections will acquaint you with the solution and the components that it comprises. The components that you can download and install is determined by your Identity Manager Edition.

- Brief Introduction of Identity Manager Components
- Functional Architecture
Brief Introduction of Identity Manager Components

To cover the varying needs of customers, Identity Manager is available in Advanced and Standard Editions. Each edition comprises of a specific set of functionalities and each functionality is handled by multiple components. Therefore, your Identity Manager implementation can include one or all of the following components depending on your requirements:

- Identity Manager Server
- Identity Applications
- Identity Reporting
- Identity Manager Tools

Figure 1-1 lists the components deployed in an Identity Manager Advanced Edition environment.

*Figure 1-1  Components for Identity Manager Advanced Edition*
Figure 1-2 lists the components deployed in an Identity Manager Standard Edition environment.

Based on how the components interact with each other, some components are logically installed as a group of components. Some components are installed as standalone components to ease the installation experience. For information about how the components interact with each other, see the NetIQ Identity Manager Overview and Planning Guide.

Review the information from the subsequent sections to understand how the components are grouped and how each component or a group of components is installed.

**Identity Manager Server Components**

*Required for all installations*

An Identity Manager Server installation comprises of the following components.
Identity Manager Server

The Identity Manager Server executes tasks within Identity Manager. It comprises of Identity Vault, Identity Manager Engine, and Identity Manager drivers.

To support the Identity Manager Server operations, the installation program installs a supported version of Oracle Java Runtime Environment (JRE). To install the Identity Manager Server components, use the Identity Manager Engine installation option of the installation program.

Identity Vault

When you install Identity Manager Engine, the installation process creates and configures a connection to Identity Vault. Identity Manager uses Identity Vault as the default repository of all identity data. Identity data includes current state of managed identities, including user account and organizational data.

Identity Manager Engine

The Identity Manager engine processes all data changes that occur in the Identity Vault or a connected application. The server on which the Identity Manager engine runs is referred to as the Identity Manager server.

Identity Manager Drivers

The Identity Manager Server handles provisioning of users, and manages connected system accounts and groups through drivers. A driver is the software interface to a connected system.

Identity Manager Drivers run as part of the Identity Manager Server architecture. A driver acts as a gateway to a native endpoint type system technology. For example, computers running Active Directory Services can be managed only if the Active Directory driver is installed either on the Identity Manager server or the target application server with which the Identity Manager server can communicate. Drivers manage the objects that reside on the connected systems. Managed objects include accounts, groups, and optionally, endpoint-type specific objects.

A driver translates Identity Manager Engine actions into changes on the connected system, such as “Create a new email account on a Microsoft Exchange connected system.” Every driver that is configured in Identity Manager has an associated event cache file (TAO file). Events are cached in the cache file before a driver processes them. By default, the cache files are placed in Identity Vault’s DIB (Data Information Base) directory.

Identity Manager provides several in-built drivers (Java, native, .NET) to manage connections with different types of connected systems. Identity Manager also provides the ability to develop a custom driver to enable data synchronization to a variety of other systems such as a home-grown application or a repository that has no technology interface and cannot leverage out-of-box drivers.

Remote Loader

Drivers can be installed locally on the Identity Manager Server or with a Remote Loader. A Remote Loader loads drivers and communicates with the Identity Manager engine on behalf of drivers installed on remote servers. If the application runs on the same server as the Identity Manager engine, you can install the driver on that server. However, if the application does not run on the...
same server as the Identity Manager engine, you must install the driver on the application’s server. To help with the workload or configuration of your environment, you can install Remote Loader on a server separate from the servers that have Tomcat and the Identity Manager server. For more information about Remote Loader, see Determining When to Use the Remote Loader in the NetIQ Identity Manager Driver Administration Guide.

Use the Identity Manager Remote Loader Server installation option to install the Remote Loader service and the driver instances in the Remote Loader.

**Fanout Agent**

Identity Manager Fanout Agent is an installation component used by Java Database Connectivity (JDBC) Fanout driver to create multiple JDBC Fanout driver instances. The Fanout driver provisions users, groups, and password to multiple databases with minimal effort. This eliminates the need for the Identity Manager administrator to configure multiple JDBC drivers using the same policies to provision multiple databases of the same type. You can centrally manage user accounts and have them automatically created, configured, maintained, and removed when appropriate. For more information, see the NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide.

To install Fanout Agent, use the Identity Manager Fanout Agent installation option of the installation program.

**iManager**

NetIQ iManager is a browser-based tool that provides a single point of administration for many Novell and NetIQ products, including Identity Manager. You can use iManager to perform administrative tasks such as managing Identity Manager Server options or driver attributes, which you cannot manage in Identity Manager Identity Applications. For more information about iManager, see the NetIQ iManager Administration Guide. After you install the Identity Manager plug-ins for iManager, you can manage Identity Manager and receive real-time health and status information about your Identity Manager system.

With iManager, you can perform similar tasks as performed with Designer and also monitor the health of your system. NetIQ recommends that you use iManager for administrative tasks. Use Designer for configuration tasks that require changes to packages, modeling, and testing prior to deployment.

Identity Manager requires the installation of Identity Manager plug-ins with iManager. Identity Manager provides a single installer to install the iManager client and Identity Manager plug-ins. You can install iManager on the Identity Manager server or on a separate computer.

To install iManager, use the iManager Web Administration installation option of the installation program.

**TIP:** After learning about the components, you must develop a good understanding of how they are installed and configured for use in a production environment.
Identity Applications Components

Required for Advanced Edition installation

Identity Applications are an interconnected set of browser-based Web applications. They enable your organization to manage the user accounts and permissions associated with the wide variety of roles and resources available to users. You can configure the identity applications to provide self-service support for your users, such as requesting roles or changing their passwords. You can also set up workflows to improve the efficiency in managing and assigning roles and resources. Identity Applications consists of Administration Console (for administration tasks), User Console (Dashboard), and REST services that help you perform these tasks.

Note: You must have the Identity Manager Engine installed before installing Identity Applications.

To install Identity Applications components, use the Identity Applications installation option of the installation program.

An Identity Applications installation comprises of the following components:

User Application

The User Application is a browser-based web application that gives users the ability to perform a variety of identity self-service and roles provisioning tasks. Some of the tasks that were performed by using the User Application interface in the previous versions of the product have been moved to the new user interface that includes an Administration Console and a User Console. The User Application continues to provide some of the functionality that does not yet exist in the new user interface. For more information, see the NetIQ Identity Manager - Administrator’s Guide to the Identity Applications.

Authentication Service

The authentication service provides access to Identity Applications features. For more information about using Single Sign-on access in Identity Manager, see the NetIQ Identity Manager - Administrator’s Guide to the Identity Applications.

The authentication service is provided by the NetIQ One Single Sign-On Provider (OSP) component. Identity Applications requires a local installation of OSP. OSP is automatically installed with Identity Applications.

Self-Service Password Reset

The self-service password management service provides access to self-service password management. Identity Applications include NetIQ Self Service Password Reset (SSPR) to help users who have access to the identity applications to reset their passwords without administrative intervention.

The Identity Applications installation process enables SSPR by default. However you can choose to install SSPR on a separate computer if your deployment needs it or if you are installing Standard Edition. When installing SSPR on a separate computer in Advanced Edition, you must define
password management settings in the Identity Applications configuration file (ism-configuration.properties) after completing the installation of both components, either manually or by using the ConfigUpdate utility.

Web Application Server

The application server provides the runtime framework in which the identity applications components execute. The identity applications are packaged as WAR (Web Application Resource or Web application ARchive) files. The installation process enables you to deploy the WAR files to the application server. The application server runs a Java™ virtual machine, providing the runtime environment for the application code. The following WAR files apply to the URL for a component of the identity applications:

- IDMProv for the User Application interface
- idmdash for the Dashboard
- idmadmin for Identity Applications Administration interface

When a user interacts with idmdash or idmadmin applications, these applications query the underlying IDMProv.war file and fetch the information for the user. IDMProv.war exposes the REST and SOAP APIs where idmdash and idmadmin contain the information that provides the user interface.

The identity applications run on an Apache Tomcat application server, included in the installation kit. To support the Tomcat application server, the installation program installs supported versions of JRE and Apache ActiveMQ.

Identity Applications Database

The Identity Applications database maintains configuration data for the identity applications such as localized labels, entitlement values, and Email server configuration. It also stores workflow state data required by the Workflow Engine. The supported databases for Identity Applications are PostgreSQL, Oracle, and Microsoft SQL Server.

The Identity Applications installation program automatically installs a supported version of PostgreSQL database that acts as the default database for Identity Applications. If you do not want to use PostgreSQL as the database, you can configure a supported version of Oracle or MS SQL database with Identity Applications. Identity Applications require a Java Database Connectivity driver (JDBC type 4 driver) to communicate with the database. The installation program prompts for the location and name of the JDBC driver for the database. Therefore, you must obtain this JDBC driver from your database installation directory before starting the Identity Applications installation.

- For PostgreSQL database, the driver is bundled with the Identity Manager installation program.
- For Oracle database, you can download the driver from the Oracle web site.
- For Microsoft SQL Server database, download the driver from the Microsoft web site.

The database can reside locally on the Identity Applications server or a remote computer. When using a remote database, you must configure a connection to the database.
Drivers for Identity Applications

The Identity Applications components require the following drivers:

User Application Driver
Stores configuration information and notifies the Identity Applications whenever changes occur in the Identity Vault. You can configure the driver to allow events in the Identity Vault to trigger workflows. The driver can also report success or failure of a workflow’s provisioning activity to the User Application so that users can view the final status of their requests.

Role and Resource Service Driver
Manages all role assignments, starts workflows for role assignment requests that require approval, and maintains indirect role assignments according to group and container memberships. The driver grants and revokes entitlements for users based on their role memberships, and it performs cleanup procedures for requests that have been completed. The driver also maintains resource requests in addition to role requests.

The Identity Applications installation option of the installation program deploys the User Application driver and the Role and Resource Service driver to the Identity Vault.

Identity Reporting Components

(Optional) Install this component only if you plan to implement the reporting functionality

Identity Reporting gives you a complete view of your users’ entitlements, providing the knowledge you need to see the past and present state of authorizations and permissions granted to identities in your organization. Identity Manager provides predefined reports that you can use to monitor the status of an Identity Manager environment, including information collected from Identity Vaults and connected systems. To use the reports provided with Identity Manager, you install Identity Reporting, which is included with Identity Manager. Identity Reporting also includes a report packaging tool that facilitates the process of creating custom reports. The user interface for Identity Reporting makes it easy to schedule reports to run at off-peak times for optimized performance. For more information about Identity Reporting, see the Administrator Guide to NetIQ Identity Reporting.


An Identity Reporting installation comprises of the following components:

Identity Reporting
Browser-based application that generates reports by making calls to the reporting service. The reporting service retrieves the data needed to generate reports from the Identity Reporting repository (Identity Information Warehouse), which contains all report management information (such as report definitions and schedules), database views, and configuration information required for reporting.
Authentication Service

The authentication service is provided by the OSP component. For more information, see “Authentication Service” on page 19.

NOTE: OSP is automatically installed with Identity Reporting. However, in an Advanced Edition installation, Identity Reporting can use the same authentication service that is installed with Identity Applications. When using the same authentication service, you must specify the authentication settings during the Identity Reporting configuration.

Self-Service Password Reset

The self-service password management service provides access to self-service password management. For more information, see “Self-Service Password Reset” on page 19.

Identity Reporting Database

The Identity Reporting database (Identity Information Warehouse) stores information about the actual and desired states of the Identity Vault and the connected systems within your organization. You can generate reports from this information to view the relationship between objects, such as users and roles. The database can reside locally on the Identity Reporting server or on a remote computer. Identity Manager uses data sources to connect to the database. Identity Reporting requires a Java Database Connectivity driver (JDBC type 4 driver) to communicate with the database. A JDBC driver enables an Identity Reporting server to communicate with the data source. The supported databases for Identity Reporting are PostgreSQL, Oracle, and Microsoft SQL.

- For PostgreSQL database, this driver is bundled with the Identity Manager installation program.
- For Oracle database, you can download the driver from the Oracle web site.
- For Microsoft SQL Server database, download the driver from the Microsoft web site.

NOTE: You must have the Identity Manager Server installed before installing the Identity Reporting components.

Web Application Server

The application server provides the runtime framework in which the identity reporting components execute. The following WAR files apply to the URL for a component of identity reporting:

- **IDMRPT** for the Identity Reporting application/interface
- **idmdcs** for Identity Manager Data Collection Service

When a user interacts with **IDMRPT** or **idmdcs** applications, these applications query the reporting service and fetch the information for the user. The reporting service exposes the REST APIs where **IDMRPT** and **idmdcs** contains the information that provides the user interface.

For more information on Web Application Server, see “Web Application Server” on page 20.
Drivers for Identity Reporting

The Identity Reporting components require the following drivers:

Managed System Gateway Driver

Queries the Identity Vault to collect the following type of information from managed systems:

- List of all managed systems
- List of all accounts for the managed systems
- Entitlement types, values, and assignments, and user account profiles for the managed systems

Data Collection Service Driver

The Data Collection Service uses the Data Collection Services driver to capture changes to objects stored in an Identity Vault, such as accounts, roles, resources, groups, and team memberships. The driver registers itself with the service and pushes change events (such as data synchronization, add, modify, and delete events) to the service.

The service includes three subservices:

- **Report Data Collector**: Uses a pull design model to retrieve data from one or more Identity Vault data sources. The collection runs on a periodic basis, as determined by a set of configuration parameters. To retrieve the data, the collector calls the Managed System Gateway driver.

- **Event-Driven Data Collector**: Uses a push design model to gather event data captured by the Data Collection Service driver.

- **Non-Managed Application Data Collector**: Retrieves data from one or more non-managed applications by calling a REST end point written specifically for each application. Non-managed applications are applications within your enterprise that are not connected to the Identity Vault.

The Identity Reporting installation option of the installation process deploys the Managed System Gateway driver and the Data Collection Service driver to the Identity Vault.

Sentinel Log Management for Identity Governance and Administration

Sentinel Log Management for Identity Governance and Administration (IGA) is a Security Information and Event Management (SIEM) system that receives information from many sources throughout an enterprise, standardizes it, prioritizes it and presents it to you to make threat, risk and policy related decisions. Sentinel Log Management for (IGA) captures log events associated with actions performed in several NetIQ products, including Identity Reporting, Identity Applications, and the Identity Vault. These events are stored in the public schema within the Identity Reporting repository (Identity Information Warehouse).

Identity Manager provides a separate installation program (SentinelLogManagementForIGA8.2.2.0.tar.gz) for Sentinel Log Management for IGA.
Identity Manager Tools

**Required for all installations**

Identity Manager includes a set of management tools to facilitate the implementation, customization and maintenance of the solution. Some of these tools are installed with Identity Manager and some must be installed separately.

**Designer for Identity Manager**

**Designer for Identity Manager** (Designer) helps you design, test, document, and deploy Identity Manager solutions in a network or test environment. You can configure your Identity Manager project in an off-line environment, and then deploy to your live system. From a design perspective, Designer helps do the following:

- Graphically view all of the components that comprise your Identity Manager solution and observe how they interact.
- Modify and test your Identity Manager environment to ensure it performs as expected before you deploy part or all of your test solution to your production environment.

Designer keeps track of your design and layout information. With a click of a button, you can print that information in a format of your choice. Designer also enables teams to share work on enterprise-level projects.

Identity Manager provides a separate installation program for Designer.

**Analyzer for Identity Manager**

**Analyzer for Identity Manager** (Analyzer) provides data analysis, cleansing, reconciliation, and reporting to help you adhere to internal data quality policies. Analyzer lets you analyze, enhance, and control all data stores throughout the enterprise. Analyzer includes the following features:

- Analyzer’s schema map associates an application’s schema attributes to the corresponding schema attributes in Analyzer’s base schema. This lets you ensure that your data analysis and cleaning operations properly associate similar values between the disparate systems. To accomplish this, Analyzer leverages the schema mapping features in Designer.
- The Analysis Profile editor lets you configure a profile for analyzing one or more data set instances. Each analysis profile contains one or more metrics against which you can evaluate attribute values to see how the data conforms to your defined data format standards.
- The Matching Profile editor lets you compare values in one or more data sets. You can check for duplicate values within a specified data set and check for matching values between two data sets.

Identity Manager provides a separate installation program for Analyzer.

After understanding the purpose of different Identity Manager components and the way they are installed, see Figure 1-3 to understand how the components interact with each other.
**Functional Architecture**

The following illustration depicts the basic functional architecture for Identity Manager components. This illustration does not cover all possible integrations.
For information about the possible deployment scenarios, see Deployment Options for Identity Manager.

Deployment Options for Identity Manager

Consult the following table to plan the physical environment for your Identity Management solution. These deployment use cases provide an overview of the Identity Management physical architecture and how the component products are connected and communicate with each other and other products. For an introductory overview of the Identity Management functional architecture and the components, see “Functional Architecture” on page 25.

<table>
<thead>
<tr>
<th>Deployment Option</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-server configuration on one computer</td>
<td>The most basic deployment configuration includes Identity Manager server and other required applications on one computer. You must ensure that the computer has the required memory, speed, and available disk space to meet the workload. This is a basic deployment use case and mostly suited for Proof-of-Concept (POC) and demonstration purposes only. It might not be appropriate for a production environment.</td>
</tr>
</tbody>
</table>
Identity Manager allows you to control user identities and their access to applications and accounts on connected systems. Based on the functionality you need, select which Identity Manager Edition to install, which in turn determines the components to install. The following table lists the features provided by Identity Manager Advanced Edition and Identity Manager Standard Edition.

### Deployment Option Summary

<table>
<thead>
<tr>
<th>Deployment Option</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed server configuration</td>
<td>This deployment has Identity Manager server on one computer and all other required applications on one or more additional computers. For example, components such as identity applications, iManager, OSP, and SSPR can run on a separate computer. You can include an additional computer to host the components for reporting service to suffice the system requirements for running the Sentinel Log Management for IGA component.</td>
</tr>
<tr>
<td>High-availability deployment</td>
<td>High availability is a redundancy operation that automatically switches to a standby server if the primary server fails or is temporarily shut down for maintenance. Identity Manager supports installing the following components in a high-availability environment:</td>
</tr>
<tr>
<td></td>
<td>• Identity Vault</td>
</tr>
<tr>
<td></td>
<td>• Identity Manager engine</td>
</tr>
<tr>
<td></td>
<td>• Remote Loader</td>
</tr>
<tr>
<td></td>
<td>• Identity applications, except Identity Reporting</td>
</tr>
<tr>
<td></td>
<td>A typical cluster configuration contains Tomcat Application Server nodes hosting the Identity Applications for load balancing and fault tolerance. All the communication is routed through the load balancer. All nodes communicate to the same instance of the Identity Vault and the Identity Applications database. This configuration is scalable. You can easily increase the number of nodes to handle the load.</td>
</tr>
</tbody>
</table>

### Sample Identity Manager Deployments

Identity Manager allows you to control user identities and their access to applications and accounts on connected systems. Based on the functionality you need, select which Identity Manager Edition to install, which in turn determines the components to install. The following table lists the features provided by Identity Manager Advanced Edition and Identity Manager Standard Edition.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Advanced Edition</th>
<th>Standard Edition</th>
<th>Components to Install</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule-based automated user provisioning</td>
<td>✓</td>
<td>✓</td>
<td>Identity Manager Engine and Designer</td>
</tr>
<tr>
<td>Real-time identity synchronization</td>
<td>✓</td>
<td>✓</td>
<td>Identity Manager Engine and Designer</td>
</tr>
<tr>
<td>Password management and password self-service</td>
<td>✓</td>
<td>✓</td>
<td>Identity Manager Engine and SSPR</td>
</tr>
<tr>
<td>Uniform identity information tool (Analyzer)</td>
<td>✓</td>
<td>✓</td>
<td>Analyzer</td>
</tr>
<tr>
<td>REST APIs and single sign-on support</td>
<td>✓ (limited support only)</td>
<td>✓</td>
<td>Identity Manager Engine, OSP, and Identity Reporting</td>
</tr>
</tbody>
</table>
NOTE: In all Identity Manager installations, Identity Manager Server is the central component. Depending on the Identity Manager edition, only Identity Reporting or both Identity Reporting and Identity Applications are installed on a Tomcat application server. Use the Identity Manager component-specific installer to install other components as needed. For example, install Designer, Analyzer, or Sentinel Log Management for Identity Governance and Administration.

In addition, review the goals for your implementation and pay attention to the physical topology options, such as high availability and scalability before installing Identity Manager. This helps you identify the configuration that matches your organization's requirements.

High availability ensures efficient manageability of critical network resources including data, applications, and services. You can implement high availability by reducing any single points-of-failure and by using redundant components. Similarly, connecting multiple instances of identity management components with a load balancer can provide a highly available environment.

This section describes two examples to illustrate Advanced Edition and Standard Edition implementations at a high level. You can use them as a reference to come up with a deployment diagram for your implementation.
Sample Advanced Edition Deployment

Figure 1-4 shows a high-level deployment topology of an Identity Manager Advanced Edition installation.

- Identity Manager Server components and its underlying repository (Identity Vault) and Web-enabled components (Identity Applications and Identity Reporting) are installed in the intranet zone. The load balancer then routes the traffic to the Identity Applications components. This deployment provides enhanced security because these components are separated from Internet traffic by firewalls.

- The Identity Manager Server components are configured to use a two server (primary/secondary) configuration. A virtual logical IP address is active on the primary server, which acts as the primary (active) node and another server acts as the secondary node. If the primary server fails, the logical IP address is moved to the secondary server. All the processes are then started on the secondary server. The application processes accessing the secondary server may experience a temporary loss of service when the logical IP address is moved over, and all other processes are started. All the components use the same Identity Vault server at any point of time.
SSPR services are available inside and outside the firewall to address the password management needs of local and mobile users of the organization. The services installed inside the firewall address the local password management needs. In case of forgotten password, the mobile workforce cannot access VPN which will prevent them from accessing the internally placed SSPR services. They can directly access the SSPR services placed outside the firewall to manage their passwords.

User Application and authentication service (OSP) are deployed in a cluster to handle the load and support the failover process for Identity Applications. The cluster nodes are attached to the same Identity Applications database that is installed on a separate computer. This deployment provides increased scalability by allowing you to add more nodes to the cluster. The cluster configuration is immediately sent to the newly added nodes. The load balancer is typically part of the cluster. It understands the cluster configuration as well as failover policies. In this configuration, all the cluster nodes are active at any point of time. The load balancer distributes the load across the nodes to ensure that the nodes have roughly the same workload. If a node fails, it diverts the requests made to that node to the surviving nodes in the cluster. Because this installation is an intrasite, high availability solution, it provides protection from local hardware and software failures, using a two node hardware-based cluster to achieve high availability for Identity Applications components.

NetIQ has tested and recommends this configuration.

**NOTE:** Identity Manager does not support clustering the Identity Reporting components.

**Sample Standard Edition Deployment**

In production deployments, security policies might specify to not expose the authentication service that provides advanced authentication and protection for your environment to the public network. Figure 1-5 shows a high-level deployment topology of an Identity Manager Standard Edition installation.
Identity Manager Server components and its underlying repository (Identity Vault) and Identity Reporting components are installed in the intranet zone. Internet Web traffic is routed to the Identity Reporting components through the Web servers that are installed behind the firewall for added protection. This deployment provides enhanced security because these components are separated from Internet traffic by firewalls.

The Identity Manager Server components are configured to use a two-server (primary/secondary) configuration. A virtual logical IP address is active on the primary server, which acts as the active node while another server acts as the secondary node. If the primary server fails, the logical IP address is moved to the secondary server. All the processes are then started on the secondary server. The application processes accessing the secondary server may experience a temporary loss of service when the logical IP address is moved over, and all other processes are started. All the components use the same Identity Vault server at any point of time.

SSPR services are available inside and outside the firewall to address the password management needs of local and mobile users of the organization. The services installed inside the firewall address the local password management needs. In case of forgotten password, the mobile workforce cannot access VPN which will prevent them from accessing the internally placed SSPR services. They can directly access the SSPR services placed outside the firewall to manage their passwords.

NetIQ has tested and recommends this configuration.
NOTE: Identity Manager does not support clustering the Identity Reporting components.
Planning to Install Identity Manager

Planning your Identity Manager implementation depends on how you want Identity Manager to manage users and what functionality you need to accomplish your business goals. Consider the following points to help you make decisions:

- How do I manage identities.
- Do I need automated provisioning.
- Which business requirements should I implement using workflow.

The result of your decisions will determine the best way to implement Identity Manager for your requirements.

There are additional tasks that require planning before deploying Identity Manager in a large enterprise. For more information, refer to the Planning section of the NetIQ Identity Manager Overview and Planning Guide.
Planning Your Installation

The following table lists the components to install to support the functionality that you want to implement. For instructions on installing these components, see the Installation section.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Component to Install</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage user identities in a corporate directory</td>
<td>Identity Manager Server</td>
</tr>
<tr>
<td>Provision accounts in connected systems</td>
<td>Identity Manager Server</td>
</tr>
<tr>
<td></td>
<td>Identity Applications</td>
</tr>
<tr>
<td></td>
<td>User Application Driver</td>
</tr>
<tr>
<td></td>
<td>Role and Resource Service Driver</td>
</tr>
<tr>
<td></td>
<td>Designer</td>
</tr>
<tr>
<td><strong>NOTE:</strong> For instructions on installing Identity Manager drivers, see the driver implementation guide for the type of driver that you want to install on the Identity Manager Drivers Documentation Website.</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>Identity Manager Server</td>
</tr>
<tr>
<td>Password management</td>
<td>Identity Manager Server</td>
</tr>
<tr>
<td></td>
<td>One Single Sign-On Provider</td>
</tr>
<tr>
<td>Generate reports on Identity Manager activity</td>
<td>Identity Manager Server</td>
</tr>
<tr>
<td></td>
<td>Identity Reporting</td>
</tr>
<tr>
<td></td>
<td>One Single Sign-On Provider</td>
</tr>
</tbody>
</table>

Determine Hardware Requirements

The hardware that you need for your Identity Manager installation is governed by two factors:

- Functionality that you want to implement
- Size of your deployment

The following deployment types can help you estimate the size of the deployment.

<table>
<thead>
<tr>
<th>Type Of Deployment</th>
<th>Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proof of Concept (demonstration)</td>
<td>A single server deployment for use in demonstrations or basic testing in a development environment.</td>
</tr>
</tbody>
</table>
Table 2-1  Planning Worksheet

<table>
<thead>
<tr>
<th>Type Of Deployment</th>
<th>Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>A multi-server implementation that is suitable for small to medium size implementations. This type of implementation requires one server for running Identity Manager Server and its components and two additional servers for running the Identity Applications and Identity Reporting components.</td>
</tr>
<tr>
<td>Intermediate</td>
<td>A high availability implementation that is suitable for medium size implementations.</td>
</tr>
<tr>
<td>Large Enterprise</td>
<td>A high availability implementation that includes Identity Manager engine cluster to provide failover capabilities and another cluster of Identity Applications and authentication service to support single sign-on access (OSP on Windows) and load balancing and fault tolerance.</td>
</tr>
</tbody>
</table>

Deployment Planning Worksheet

Use the information in this topic to understand the details of a new implementation of Identity Manager.

Table 2-1  Planning Worksheet

<table>
<thead>
<tr>
<th>Planning Activity</th>
<th>Worksheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decide on your implementation type based on use cases and size the deployment</td>
<td>Sizing Worksheet</td>
</tr>
<tr>
<td>Design your deployment architecture. List down the number of physical computers/servers and other systems needed to support your environment</td>
<td>Architecture Worksheet</td>
</tr>
<tr>
<td>Ensure that your system meets the system requirements</td>
<td>System Requirements Worksheet</td>
</tr>
<tr>
<td>Review the network ports to determine whether the default ports will conflict with the ports in use</td>
<td>Reviewing the Ports Used by the Identity Manager Components</td>
</tr>
</tbody>
</table>

Sizing Worksheet

It is important to estimate the size of your deployment correctly because the steps to follow and the design elements vary depending on the size of the deployment. Review sizing and scalability considerations for each component to understand the capacity requirements.

Table 2-2  Sizing Worksheet

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Physical Computers/Servers</td>
<td></td>
</tr>
<tr>
<td>Number of Drivers Running on the primary Identity Manager Server</td>
<td></td>
</tr>
</tbody>
</table>
After sizing the deployment, select the appropriate deployment and record the number of physical computers/servers required to support the deployment.

### Architecture Worksheet

After sizing the deployment, select the appropriate deployment and record the number of physical computers/servers required to support the deployment.

#### Table 2-3  Architecture Worksheet

<table>
<thead>
<tr>
<th>Deployment use case</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Manager Server failover deployment with all drivers</td>
<td>Number of Drivers Running Identity Applications high availability deployment</td>
</tr>
</tbody>
</table>

### System Requirements Worksheet

For information about the recommended hardware, supported operating systems, and supported virtual environments, see the [System Requirements for Identity Manager 4.8](#).

For information about system requirements for a specific release, see the Release Notes accompanying the release at the [Identity Manager documentation website](#).

An Identity Manager implementation can vary based on the needs of your IT environment, so you should contact [NetIQ Consulting Services](#) or any of the NetIQ Identity Manager partners prior to finalizing the Identity Manager architecture for your environment.
Reviewing the Ports Used by the Identity Manager Components

Identity Manager components use different ports for proper communication among the Identity Manager components.

**NOTE:** If a default port is already in use, ensure that you specify a different port for the Identity Manager component.

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Component</th>
<th>Port Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>389</td>
<td>Identity Vault</td>
<td>Used for LDAP communication in clear text with Identity Manager components</td>
</tr>
<tr>
<td>465</td>
<td>Identity Reporting</td>
<td>Used for communication with the SMTP mail server</td>
</tr>
<tr>
<td>524</td>
<td>Identity Vault</td>
<td>Used for NetWare Core Protocol (NCP) communication</td>
</tr>
<tr>
<td>636</td>
<td>Identity Vault</td>
<td>Used for LDAP with TLS/SSL communication with Identity Manager components</td>
</tr>
<tr>
<td>5432</td>
<td>Identity Applications</td>
<td>Used for communication with the identity applications database</td>
</tr>
<tr>
<td>7707</td>
<td>Identity Reporting</td>
<td>Used by the Managed System Gateway driver to communicate with the Identity Vault</td>
</tr>
</tbody>
</table>
| 8000        | Remote Loader | Used by the driver instance for TCP/IP communication  
**NOTE:** Each instance of the Remote Loader should be assigned a unique port. |
| 8005        | Identity Applications | Used by Tomcat to listen for shutdown commands |
| 8009        | Identity Applications | Used by Tomcat for communication with a web connector using the AJP protocol instead of HTTP |
| 8028        | Identity Vault | Used for HTTP clear text communication with NCP communication |
| 8030        | Identity Vault | Used for HTTPS communication with NCP communication |
| 8080        | Identity Applications | Used by Tomcat for HTTP clear text communication |
| iManager    |           |          |
| 8090        | Remote Loader | Used by the Remote Loader to listen for TCP/IP connections from the remote interface shim  
**NOTE:** Each instance of the Remote Loader should be assigned a unique port. |
| 8109        | Identity Applications | Applies only when using the integrated installation process  
Used by Tomcat for communication with a web connector using the AJP protocol instead of HTTP |
<table>
<thead>
<tr>
<th>Port Number</th>
<th>Component</th>
<th>Port Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>8180</td>
<td>Identity Applications</td>
<td>Used for HTTP communications by the Tomcat application server on which the identity applications run</td>
</tr>
<tr>
<td>8443</td>
<td>Identity Applications, iManager</td>
<td>Used by Tomcat for HTTPS (SSL) communication or redirecting requests for SSL communication</td>
</tr>
</tbody>
</table>
| 8543        | Identity Applications | *Not listening, by default*  
Used by Tomcat to redirect requests that require SSL transport when you do not use TLS/SSL protocol |
| 9009        | iManager            | Used by Tomcat for MOD_JK                                                 |
| 5432        | Identity Reporting  | Used for the PostgreSQL database Sentinel                                 |
| 45654       | User Application    | Used by the server on which the database for the identity applications are installed to listen for communications, when running Tomcat with a cluster group |
Installing and Configuring Identity Manager Components

This section guides you through the process of installing and configuring Identity Manager components. For installation instructions, see “Installation Procedures” on page 45.

After Identity Manager components are installed and basic configuration has been completed, you must perform some additional configuration steps for the components to be fully functional. For more information, see Chapter 4, “Final Steps for Completing the Installation,” on page 63.
Installation and Configuration Process Overview

This section describes the process of installing and configuring Identity Manager components. You must review the configuration options for each component before beginning the configuration process. For more information, see Understanding the Configuration Settings.

Some components, such as Designer and Analyzer, might not require configuration.

Installation Order

The components must be installed in the following order because the installation programs for some components require information about previously installed components:

- Sentinel Log Management for Identity Governance and Administration (IGA) (installation supported only on Linux computers)
- Identity Manager Server components
- Identity Applications components (only for Advanced Edition)
- Identity Reporting components
- Designer for Identity Manager
- Analyzer for Identity Manager

You must review the installation prerequisites and considerations for each component before installing the component.

Understanding the Installation and Configuration Process for Identity Manager Server, Identity Applications, and Identity Reporting Components

Identity Manager provides a wizard-based installation method for installing and configuring the following Identity Manager components:

- Identity Manager Server
- Identity Applications
- Identity Reporting

The installer allows you to install and configure the components interactively or silently. The installation process allows you to specify the values for the installed components.

The installation process also creates a repository of dependent components such as JRE, Apache Tomcat, PostgreSQL, ActiveMQ, and OpenSSL on your filesystem. When you install multiple Identity Manager components on the same computer, the installation process refers to this repository.
instead of creating multiple copies of these components for each Identity Manager component that
requires them. For example, Identity Applications and Identity Reporting use the same Tomcat when
they are installed on the same computer.

Types of Installation Methods

Identity Manager supports interactive and silent installation methods. A silent (non-interactive)
installation does not display a user interface or ask the user any questions.

Interactive Method

- Requires you to select the components that you want to install. Based on your selection, the
  components are installed.

Silent Method

- You are required to specify the values for the components you want to install in the properties
  file. When the installation program is invoked, it reads these values from the properties file. You
can use the same properties file to run silent installation on different computers in your
environment.

Installation Options

The following table describes the components that are installed with the installation options
provided by the installation program.

<table>
<thead>
<tr>
<th>Installation Option</th>
<th>Components Installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Manager Engine</td>
<td>Installs the Identity Vault, Identity Manager Engine, Remote Loader Service, iManager Web Administrator and Identity plug-ins, Fanout Agent, and drivers.</td>
</tr>
</tbody>
</table>
| Identity Applications        | Installs Identity Applications, One SSO Provider (OSP), User Application driver, Roles and Resource Service Driver (RRSD), PostgreSQL, and Self Service Password Reset (SSPR).  

**NOTE:** If you want to install SSPR on a different server than Identity Applications, use the install.exe available at <iso mounted location>\common\sspr\ directory. |
| Identity Reporting           | Installs Identity Reporting, OSP, PostgreSQL, Data Collection Service Driver (DCS), and Managed System Gateway (MSG) driver. |

Types of Configuration Modes

You can configure the Identity Manager components in the following ways:

- Typical
- Custom
A typical configuration assumes default settings for most of the configuration options. In a custom configuration, you can specify custom values according to your requirement. You can configure most of the settings by using this option.

**Using Non-Intuitive Passwords During Configuration**

Many of the Identity Manager components require you to specify a password during the configuration phase. For faster configuration, you can instruct the process to apply the same password to all the configuration parameters.

The password must be a minimum of six characters. Do not use words that can be found in the dictionary. Dictionary words are vulnerable to freely available password-cracking tools that often come with dictionary lists. If you must use dictionary words, try combining them with numerals and punctuation.

**Understanding the Installation Process for Designer and Analyzer**

Identity Manager provides separate Windows installation programs for Designer and Analyzer. The installation programs for Designer and Analyzer are available on the product download site.

**Designer**

You can install Designer using the `Identity_Manager_4.8_Windows_Designer.tar.gz` file. For silent installation, specify the values for installation in the `designerInstaller.properties` file. Otherwise, the installer will assume the default parameter values for the installation.

Designer does not require any configuration.

**Analyzer**

You can install Analyzer using the `Identity_Manager_4.8_Windows_Analyzer.tar.gz` file. For silent installation, specify the values for installation in the `designerInstaller.properties` file. Otherwise, the installer will assume the default parameter values for the installation.

Analyzer does not require any configuration.

**Installation Procedures**

Use this topic to understand the installation methods for Identity Manager components.

**Installation Procedures for Identity Manager Server, Identity Applications, and Identity Reporting**

This section guides you through the process of installing the Identity Manager Server, Identity Applications, and Identity Reporting components through an interactive method or silent method. The Identity Manager Server option in the installation program allows you to install the 32-bit, 64-bit and .NET Remote loader.
NOTE: Before installing Identity Manager engine, ensure that your Windows server is updated with the latest Windows patch and the Windows server is restarted.

Interactive Installation

1. Download the Identity_Manager_4.8_Windows.iso from the download site.
2. Mount the downloaded iso.
3. Based on the component that you wish to install, run the install.exe available at the following locations:
   - Identity Manager Server: <iso mounted location>\IdentityManagerServer
   - Identity Applications: <iso mounted location>\IdentityApplications
   - Identity Reporting: <iso mounted location>\IdentityReporting
4. Select the language that you want to use for the installation and click OK. The Introduction screen displays the components available for installation.
5. Click Next.
6. Read and accept the license agreement.
7. Select the components you wish to install and click Next.
8. Specify the installation folder and then click Next.

   NOTE: The custom installation folder should not contain special characters such as . and _.

9. Select the installation type:
   - Typical Installation
   - Custom Installation
10. Based on the mode of installation that you have selected, the installation parameters will differ. Specify the required details. For information on the configuration parameters, see the following tables:
    - Identity Manager Engine Settings
    - Identity Applications Settings
    - Identity Reporting Settings
11. Review the details on the pre-install summary page and click Install.

Silent Installation

To run a silent installation of the Identity Manager components, use the properties files available in the .iso for the respective components. The Identity Manager media includes a sample properties file at <iso_downloaded_location>\<Identity Manager Component>\response-files location.

To install the component using silent installation, perform the following actions:

1. Download the Identity_Manager_4.8_Windows.iso from the NetIQ Downloads website.
2. Mount the downloaded .iso.
3 Based on the mode of installation that you want to use for installing the components, use the `typical_install.properties` or `custom_install.properties` files available at the following locations:

- **Identity Manager Server**: `<iso mounted location>\IdentityManagerServer\response-files`
- **Identity Applications**: `<iso mounted location>\IdentityApplications\response-files`
- **Identity Reporting**: `<iso mounted location>\IdentityReporting\response-files`

4 Modify the installation parameters according to your requirement. For information on the configuration parameters, see the following tables:

- **Identity Manager Engine Settings**
- **Identity Applications Settings**
- **Identity Reporting Settings**

5 To run the silent installation, run the following command from the directory of the component to be installed:

   ```
   .\install.exe -i silent -f <path to typical or custom install properties file>
   ```

   For example:

   ```
   .\install.exe -i silent -f C:\Users\Administrator\Desktop\typical_install_idmengine.properties
   ```

6 (Optional) For default installed locations, see the install log. For example, you can check the following files:

   ```
   C:\Program Files\NetIQ\IDM\Install\logs
   ```

### Installing Remote Loader

Identity Manager provides you an option to install Remote Loader on a standalone server. Use this option when you want to install Identity Manager Engine and Remote Loader on separate computers.

**NOTE**: You can install the 64-bit Remote Loader and .NET Remote Loader using this option. To install a 32-bit remote loader, see Installation Procedures for Identity Manager Server, Identity Applications, and Identity Reporting.

### Interactive Installation

1. Download the `Identity_Manager_4.8_RL_Windows.iso` from the NetIQ Downloads website.
2. Mount the downloaded `.iso`.
3. From the mounted location, run the `install.exe` file.
4. Select the language that you want to use for the installation and click **OK**.
5. Click **Next**.
6. Read and accept the license agreement.
7. Click Next.
8. Specify the installation folder and click Next.
9. Click Install.

**Silent Installation**

1. Download the Identity_Manager_4.8_RL_Windows.iso from the NetIQ Downloads website.
2. Mount the downloaded .iso.
3. Navigate to the <ISO mounted location>\response-files.
4. To perform a silent installation, run the following command from the directory of the properties file:

   install.exe -i silent -f install.properties

**Installing Java Remote Loader**

Identity Manager uses the Java Remote Loader to exchange data between the Identity Manager engine running on one server and the Identity Manager drivers running in another location, where rdxml does not run. You can install java remote loader - dirxml_jremote on any supported Windows platform that has a compatible JRE and Java Sockets.

1. On the server that hosts the Identity Manager engine, copy the application shim .iso or .jar files, in the default location. For example, C:\NetIQ\idm\NDS\lib directory.
2. Log in to the computer where you want to install the Java Remote Loader (the target computer).
3. Verify that the target computer has a supported version of JRE.
4. Download the Identity_Manager_4.8_Windows.iso from the NetIQ Downloads website.
5. Mount the downloaded .iso.
6. Navigate to the <iso mounted location>`IdentityManagerServer\products\IDM\java_remoteloader directory.
7. Copy the dirxml_jremote_dev.tar.gz file to the desired location on the target computer. For example, copy the file to C:\NetIQ\idm.
8. Copy one of the following files to the desired location on the target computer:

   - dirxml_jremote.tar.gz
   - dirxml_jremote_mvs.tar

   For information about mvs, untar the dirxml_jremote_mvs.tar file, then refer to the usage.html document.
9. On the target computer, unzip and extract the .tar.gz files.

   For example, use 7-Zip or supported software to unzip .tar.gz files.
10. Set the CLASSPATH environment variable to all jars that are present in lib folder. If you have dependent jars specific to any driver, copy those jar files to lib folder, then set the CLASSPATH environment variable to these jars also.

   For example, set:
CLASSPATH=E:\RL\JAVARL\lib\activation.jar;E:\RL\JAVARL\lib\commondrive
rshim.jar;E:\RL\JAVARL\lib\delimitedtextshim.jar;E:\RL\JAVARL\lib\deli
mitedtextutil.jar;E:\RL\JAVARL\lib\dirxml.jar;E:\RL\JAVARL\lib\dirxml_-
misc.jar;E:\RL\JAVARL\lib\dirxml_remote.jar;E:\RL\JAVARL\lib\jco3envir-
onment.jar;E:\RL\JAVARL\lib\mail.jar;E:\RL\JAVARL\lib\mapdb.jar;E:\RL\-
JAVARL\lib\nxsl.jar;E:\RL\JAVARL\lib\shimwrapper.jar;E:\RL\JAVARL\lib\-
xds.jar;E:\RL\JAVARL\lib\xp.jar

11 Set the **PATH** environment variable to bin folder of JDK or JRE for Java.exe.

12 You must specify the location of the jar files in the dirxml_jremote script from the lib
subdirectory of the untarred dirxml_jremote.tar.gz directory. For example,
\lib\*.jar.

13 Configure the sample configuration file config8000.txt for use with your application shim.
The dirxml_jremote.tar.gz jar file contains this file. For more information, see Configuring
the Remote Loader and Drivers in the NetIQ Identity Manager Driver Administration Guide.

14 Launch the Remote Loader using following commands:

14a To specify a Remote Loader password:

```bash
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config
file name> -sp <Remote Loader Password> <Object Driver Password>
```

For example,

```bash
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config<e:\RL\JAVARL\config8000.txt -sp novell novell
```

14b To start the Remote Loader:

```bash
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config
file name>
```

For example,

```bash
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config<e:\RL\JAVARL\config8000.txt
```

14c To stop the Remote Loader:

```bash
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config
file name> -unload
```

For example,

```bash
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config<e:\RL\JAVARL\config8000.txt -unload
```
Installing .NET Remote Loader

To install the .NET Remote Loader as an administrative user:

1. Log in as administrator on the computer where you want to install the .NET Remote Loader.
2. To access the installation program, complete one of the following steps:
   2a. (Conditional) If you have the .iso image file for the Identity Manager installation package, navigate to the directory containing the .NET Remote Loader installation files, located by default in the \products\idm\windows\setup\ directory.
   2b. (Conditional) If you downloaded the .NET Remote Loader installation files from the NetIQ Downloads website, complete the following steps:
       * Navigate to the .tgz file for the downloaded image.
       * Extract the contents of the file to a folder on the local computer.
3. Run the idm_install.exe program from the installation directory.
4. Accept the license agreement, and then click Next.
5. In the Select Components window, specify the .NET Remote Loader.
6. (Optional) To select specific drivers for the individual components, complete the following steps:
   6a. Click Customize the selected components, and then click Next.
   6b. Expand Drivers under the component that you want to install.
   6c. Select the drivers that you want to install.
7. Click Next.
8. In the Activation Notice window, click OK.
9. Select the .NET Remote Loader installation directory on your computer.
10. Review the Summary page, then click Install to complete the installation.

Installing SSPR

The installer provides you an option to install SSPR separately. Use this option when you want to install Identity Applications and SSPR on separate computers. This is the only option to install SSPR in a Standard Edition. SSPR is not automatically installed in a Standard Edition.

You can perform an interactive or a silent installation of SSPR.

Interactive Installation

1. Download the Identity_Manager_4.8_Windows.iso from the NetIQ Downloads website.
2. Mount the downloaded .iso.
3. Navigate to the <ISO mounted location>\common\sspr directory.
4. Run the install.exe file.
5. Select the language that you want to use for the installation and click OK.
6. Click Next.
7. Read and accept the license agreement.
8 Click Next.
9 Specify the installation folder and click Next.
10 Specify the configuration settings for SSPR. For more information, see “Configuration Worksheet for Self-Service Password Reset” on page 57.

11 Click Next.
12 Click Install.

**Silent Installation**

1 Download the `Identity_Manager_4.8_Windows.iso` from the NetIQ Downloads website.
2 Mount the downloaded `.iso`.
3 Navigate to the `<ISO mounted location>`\common\sspr directory.
4 To perform a silent installation, run the following command from the directory of the properties file:
   
   `install.exe -i silent -f sspr_silentinstall.properties`

**Understanding the Configuration Settings**

Use the following worksheets to help collect the information that you need to specify when configuring the Identity Manager components.

**Configuration Worksheet for Identity Manager Engine**

Use the following worksheet to help collect the information that you need to specify when configuring Identity Manager Engine.

**Table 3-2  Identity Manager Engine Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Vault DIB Location</td>
<td>Specify the Identity Vault DIB location.</td>
</tr>
<tr>
<td>Create a New Tree</td>
<td>Select this option if you want to create a new Identity Vault tree.</td>
</tr>
<tr>
<td>Tree Name</td>
<td>Applies only if you have selected the Create a New Tree option.</td>
</tr>
<tr>
<td></td>
<td>Specify the Identity Vault tree name.</td>
</tr>
<tr>
<td>Add to an Existing Tree</td>
<td>Select this option if you want to connect to an Identity Vault tree existing on a remote server. You must only specify an IP address; hostname or FQDN is not supported.</td>
</tr>
<tr>
<td>Host</td>
<td>Applies only if you have selected the Add to an Existing Tree option.</td>
</tr>
<tr>
<td></td>
<td>Specify the IP address for your Identity Vault.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secure LDAP Port</td>
<td>Applies only if you have selected the Add to an Existing Tree option. Specify the port on which the Identity Vault listens for LDAP requests using Secure Sockets Layer (SSL) protocol. The default value is 636. If a service already loaded on the server (before you install eDirectory) uses the default port, you must specify a different port.</td>
</tr>
<tr>
<td>Administrator DN</td>
<td>Specify the administrator name for Identity Manager engine. The default value is cn=admin,ou=sa,o=system.</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Specify the password for the Administrator object. For example, password.</td>
</tr>
<tr>
<td>Identity Vault Server Context (in LDAP format)</td>
<td>Specify the DN for the server container. The default value is ou=servers, o=system</td>
</tr>
<tr>
<td>Identity Vault Driver Set (in LDAP format)</td>
<td>Specify the context DN for the driver set. The default value is cn=DriverSet, o=system.</td>
</tr>
<tr>
<td>Clear Text LDAP Port</td>
<td>Specify the port on which the Identity Vault listens for LDAP requests in clear text. The default value is 389.</td>
</tr>
<tr>
<td>Secure LDAP Port</td>
<td>Specify the port on which the Identity Vault listens for LDAP requests using Secure Sockets Layer (SSL) protocol. The default value is 636. If a service already loaded on the server (before you install eDirectory) uses the default port, you must specify a different port.</td>
</tr>
<tr>
<td>Clear Text HTTP Port</td>
<td>Specify the port on which the HTTP stack operates in clear text. The default value is 8028.</td>
</tr>
<tr>
<td>Secure HTTP Port</td>
<td>Specify the port on which the HTTP stack operates using TLS/SSL protocol. The default value is 8030.</td>
</tr>
<tr>
<td>RSA Key Size</td>
<td>Applies only if you have selected the Create a New Tree option. Specify the key size for RSA certificates. Allowed values are 2048, 4096, and 8192 bits. The default value is 4096.</td>
</tr>
<tr>
<td>EC Curve</td>
<td>Applies only if you have selected the Create a New Tree option. Specify the elliptical curve (EC) limit for EC certificates. Allowed values are P256, P384, and P521. The default value is P384.</td>
</tr>
<tr>
<td>Certificate Lifetime</td>
<td>Applies only if you have selected the Create a New Tree option. Specify the certificate life in years.</td>
</tr>
</tbody>
</table>
Configuration Worksheet for Identity Applications

Use the following worksheet to help collect the information that you need to specify when configuring Identity Applications.

Table 3-3  Identity Applications Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Self-Service Password Reset</td>
<td>Specify whether you want to install the SSPR component.</td>
</tr>
<tr>
<td>Host</td>
<td>Specify the IP address of the server where Identity Vault is installed.</td>
</tr>
<tr>
<td>Secure LDAP Port</td>
<td>Specify the port on which the Identity Vault listens for LDAP requests using Secure Sockets Layer (SSL) protocol. The default value is 636. If a service already loaded on the server (before you install eDirectory) uses the default port, you must specify a different port.</td>
</tr>
<tr>
<td>Administrator DN</td>
<td>Specify the administrator name for Identity Manager engine. The default value is cn=admin,ou=sa,o=system.</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Applies only when installing a new authentication server. Specify the password for the administrator account of the LDAP authentication server.</td>
</tr>
<tr>
<td>Root Container DN</td>
<td>Specify the root container. The default value is o=data.</td>
</tr>
<tr>
<td>User Container DN</td>
<td>Applies only when installing a new authentication server. Specify the container in the LDAP authentication server where you store the user accounts that can log in to Access Review. For example, o=data.</td>
</tr>
<tr>
<td>Administrator Container DN</td>
<td>Applies only when installing a new authentication server. Specify the container in the LDAP authentication server where you store the administrator accounts.</td>
</tr>
<tr>
<td>Driver Set DN</td>
<td>Specify the driver set DN.</td>
</tr>
<tr>
<td>Deploy Identity Applications Drivers</td>
<td>Select this option if you want to deploy the User Application driver and the Roles and Resources Services driver.</td>
</tr>
<tr>
<td>Select the Database Platform for Identity Applications</td>
<td>Select the database that you want use with the Identity Applications. The options are PostgreSQL, Oracle, and Microsoft SQL Server.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>New PostgreSQL Server</td>
<td>Select this option if you want to install a new instance of the PostgreSQL database.</td>
</tr>
<tr>
<td>Existing PostgreSQL Server</td>
<td>Select this option if you want to connect to an existing PostgreSQL database server.</td>
</tr>
<tr>
<td>Database Host</td>
<td>Specify the name or IP address of the server.</td>
</tr>
<tr>
<td>Database Port</td>
<td>Specify the port that you want the server to use for communication with the User Application. By default, the value is set to 5432.</td>
</tr>
<tr>
<td>Identity Applications Database Name</td>
<td>Specify the name of the database for identity applications.</td>
</tr>
<tr>
<td>Workflow Engine Database Name</td>
<td>Specify the name of the database for workflow engine.</td>
</tr>
<tr>
<td>Database User</td>
<td>Specify the name of an account that allows the User Application to access and modify data in the databases.</td>
</tr>
<tr>
<td>Database User Password</td>
<td>Specify the database user password.</td>
</tr>
<tr>
<td>Database Driver Jar</td>
<td>Specify the JAR file for the database platform. The database vendor provides the driver JAR file, which represents the Thin Client JAR for the database server. For example, for PostgreSQL, you might specify postgresql-9.4-1212.jdbc42.jar, by default in the C:\NetIQ\idm\apps\Postgres folder. NetIQ does not support driver JAR files from third-party vendors.</td>
</tr>
<tr>
<td>When would you like the schema to be created</td>
<td>Specify when you want to create the database schema as part of the process. The available options are Now, At Application Startup, and Write SQL to a File.</td>
</tr>
<tr>
<td>Application Server Host</td>
<td>Specify the IP address where Tomcat is installed.</td>
</tr>
<tr>
<td>Application Server HTTPS Port</td>
<td>Specify the port where Tomcat is installed. By default the value is set to 8543.</td>
</tr>
<tr>
<td>Login Screen Name</td>
<td>Specify the custom name that you want to display on user login screen. The default value is Identity Access.</td>
</tr>
<tr>
<td>When you upgrade Identity Applications, the login screen name automatically changes to NetIQ Access.</td>
<td></td>
</tr>
<tr>
<td>Identity Applications Administrator</td>
<td>Specify the DN for an administrator account of the LDAP authentication server. For example, cn=uaadmin,ou=sa,o=data</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Specify the Identity Applications administrator password.</td>
</tr>
<tr>
<td>Set this password as a common password for other settings</td>
<td>Select this option if you want to set a common password.</td>
</tr>
<tr>
<td>NOTE: The default password for Tomcat keystore is changelt.</td>
<td></td>
</tr>
</tbody>
</table>
Installation and Configuration Process Overview

Configuration Worksheet for Identity Reporting

Use the following worksheet to help collect the information that you need to specify when configuring Identity Reporting.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAuth Keystore Password</td>
<td>Applies only if you have selected the Set this password as a common password for other settings check box. Specify the OAuth keystore password.</td>
</tr>
<tr>
<td>SSO Client Password</td>
<td>Applies only if you have selected the Set this password as a common password for other settings check box. Specify the SSO client password.</td>
</tr>
<tr>
<td>SSPR Configuration Password</td>
<td>Applies only if you have selected the Set this password as a common password for other settings check box. Specify the SSPR configuration password.</td>
</tr>
<tr>
<td>Form Renderer HTTPS Port</td>
<td>Specify the form renderer HTTPS port. By default the value is set to 8600.</td>
</tr>
<tr>
<td>Workflow Engine ID</td>
<td>Specify a unique value for the Workflow Engine ID.</td>
</tr>
</tbody>
</table>

**Table 3-4  Identity Reporting Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Specify the IP address of the server where Identity Vault is installed.</td>
</tr>
<tr>
<td>Secure LDAP Port</td>
<td>Specify the port on which the Identity Vault listens for LDAP requests using Secure Sockets Layer (SSL) protocol. The default value is 636. If a service already loaded on the server (before you install eDirectory) uses the default port, you must specify a different port.</td>
</tr>
<tr>
<td>Administrator DN</td>
<td>Specify the administrator name for Identity Manager engine. The default value is cn=admin,ou=sa,o=system.</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Specify the password for the administrator account of the LDAP authentication server.</td>
</tr>
<tr>
<td>User Container DN</td>
<td>Applies only when installing a new authentication server. Specify the container in the LDAP authentication server where you store the user accounts that can log in to Access Review. For example, o=data.</td>
</tr>
<tr>
<td>Administrator Container DN</td>
<td>Applies only when installing a new authentication server. Specify the container in the LDAP authentication server where you store the administrator accounts.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Driver Set DN</td>
<td>Specify the driver set DN.</td>
</tr>
<tr>
<td>Deploy Identity Reporting Drivers</td>
<td>Select this option if you want to deploy the Data Collection Services driver and the Managed System Gateway services driver.</td>
</tr>
<tr>
<td>Select the Database Platform for Identity Reporting</td>
<td>Select the database that you want to use with the Identity Reporting. The options are PostgreSQL, Oracle, and Microsoft SQL Server.</td>
</tr>
<tr>
<td>New PostgreSQL Server</td>
<td>Select this option if you want to install a new instance of the PostgreSQL database.</td>
</tr>
<tr>
<td>Existing PostgreSQL Server</td>
<td>Select this option if you want to connect to an existing PostgreSQL database server.</td>
</tr>
<tr>
<td>Database Host</td>
<td>Specify the name or IP address of the server.</td>
</tr>
<tr>
<td>Database Port</td>
<td>Specify the port that you want the server to use for communication with Identity Reporting. By default, the value is set to 5432.</td>
</tr>
<tr>
<td>Database Name</td>
<td>Specify the database name for Identity Reporting.</td>
</tr>
<tr>
<td>Database User Password</td>
<td>Specify the database user password.</td>
</tr>
<tr>
<td>Database Account Password</td>
<td>Specify the database account password for Identity Reporting.</td>
</tr>
<tr>
<td>Application Server Host</td>
<td>Specify the IP address where Tomcat is installed.</td>
</tr>
<tr>
<td>Application Server HTTPS Port</td>
<td>Specify the port where Tomcat is installed. By default the value is set to 8543.</td>
</tr>
<tr>
<td>External OSP Server</td>
<td>Select this option if you want to connect to an external OSP server. For example, use this option if you want to connect to a remote OSP which is used by Identity Applications.</td>
</tr>
<tr>
<td>OSP Server Host</td>
<td>Applies only if you have selected the External OSP Server option.</td>
</tr>
<tr>
<td>OSP Server Port</td>
<td>Applies only if you have selected the External OSP Server option.</td>
</tr>
<tr>
<td>OSP Keystore</td>
<td>Applies only if you have selected the External OSP Server option.</td>
</tr>
<tr>
<td>OSP Keystore Password</td>
<td>Applies only if you have selected the External OSP Server option.</td>
</tr>
<tr>
<td>OSP Keystore Password</td>
<td>Specify the location of the OSP keystore file.</td>
</tr>
<tr>
<td>OSP Keystore Password</td>
<td>Specify the OSP keystore password.</td>
</tr>
</tbody>
</table>
Table 3-5  SSPR Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSP Client Password</td>
<td>Applies only if you have selected the External OSP Server option.</td>
</tr>
<tr>
<td></td>
<td>Specify the OSP client password.</td>
</tr>
<tr>
<td>Identity Reporting Administrator</td>
<td>Specifies the administrator name for Identity Reporting. The default value is <code>cn=uaadmin,ou=sa,o=data</code>.</td>
</tr>
<tr>
<td>Identity Reporting Administrator password</td>
<td>Specifies the administrator password for Identity Reporting.</td>
</tr>
<tr>
<td>Set this password as a common password for other settings</td>
<td>Select this option if you want to set a common password.</td>
</tr>
</tbody>
</table>

**Configuration Worksheet for Self-Service Password Reset**

Use the following worksheet to help collect the information that you need to specify when configuring Self-Service Password Reset (SSPR).

This section applies only when you want to install Identity Applications and SSPR on separate computers.

Table 3-5  SSPR Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Specify the IP address of the server where Identity Vault is installed.</td>
</tr>
<tr>
<td>Secure LDAP Port</td>
<td>Specify the port on which the Identity Vault listens for LDAP requests using Secure Sockets Layer (SSL) protocol. The default value is 636. If a service already loaded on the server (before you install eDirectory) uses the default port, you must specify a different port.</td>
</tr>
<tr>
<td>Administrator DN</td>
<td>Specify the administrator name for Identity Manager engine. The default value is <code>cn=admin,ou=sa,o=system</code>.</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Specify the password for the administrator account of the LDAP authentication server.</td>
</tr>
<tr>
<td>User Container DN</td>
<td>Applies only when installing a new authentication server.</td>
</tr>
<tr>
<td></td>
<td>Specify the container in the LDAP authentication server where you store the user accounts that can log in to Access Review. For example, <code>c=data</code>.</td>
</tr>
<tr>
<td>Administrator Container DN</td>
<td>Applies only when installing a new authentication server.</td>
</tr>
<tr>
<td></td>
<td>Specify the container in the LDAP authentication server where you store the administrator accounts.</td>
</tr>
<tr>
<td>Application Server Host</td>
<td>Specify the IP address where Tomcat is installed.</td>
</tr>
</tbody>
</table>
Installation and Configuration Process Overview

Post-Installation Steps

This section provides information about updating your Tomcat environment after you install the identity applications.

- “Passing the preferIPv4Stack Property to JVM” on page 58
- “Checking the Health of the Server” on page 59
- “Monitoring the Health Statistics” on page 59
- “Creating Compound Indexes” on page 60
- “Configuring Identity Application to Reject Client-initiated SSL Renegotiation” on page 60

Passing the preferIPv4Stack Property to JVM

The identity applications use JGroups for the caching implementation. In some configurations, JGroups requires that the preferIPv4Stack property be set to true to ensure that the mcast_addr binding is successful.

Without this option, the following error might occur:

```
[10/1/09 16:11:22:147 EDT] 0000000d UDP    W org.jgroups.util.Util createMulticastSocket could not bind to /228.8.8.8 (IPv4 address); make sure your mcast_addr is of the same type as the IP stack (IPv4 or IPv6).
```

You might also see this error:

```
[3/21/12 10:04:32:470 EDT] 00000024 UDP    E org.jgroups.protocols.TP down failed sending message to null (131 bytes)
   java.lang.Exception: dest=/228.8.8.8:45654 (134 bytes) at org.jgroups.protocols.UDP._send(UDP.java:353)
```

The parameter `java.net.preferIPv4Stack=true` is a system property that can be set in the same manner as other system properties such as `extend.local.config.dir`.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server HTTPS Port</td>
<td>Specify the port where Tomcat is installed. By default the value is set to 8543.</td>
</tr>
<tr>
<td>Identity Applications Administrator</td>
<td>Specify the DN for an administrator account of the LDAP authentication server. For example, <code>cn=uaadmin,ou=sa,o=data</code></td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Specify the Identity Applications administrator password.</td>
</tr>
<tr>
<td>Authentication Server Host</td>
<td>Specify the IP address of the server where OSP is installed.</td>
</tr>
<tr>
<td>Authentication Server HTTPS Port</td>
<td>Specify the OSP server HTTPS port.</td>
</tr>
<tr>
<td>Authentication Server Client Password</td>
<td>Specify the OSP client password.</td>
</tr>
</tbody>
</table>
Checking the Health of the Server

Most loadbalancers provide a healthcheck feature for determining whether an HTTP server is up and listening. The User Application contains a URL that can be used for configuring HTTP healthchecks on your loadbalancer. The URL is:

http://<NodeIP>:port/IDMProv/jsps/healthcheck.jsp

Monitoring the Health Statistics

The REST API allows you to retrieve information about the health of the User Application. The API can access the system for the currently running threads, memory consumption, cache, and cluster information and returns the information using the GET operation.

- **Memory information (JVM and system memory):** Reads the memory related information such as system memory and memory consumed by the JVM.
  
  For example,
  
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/memoryinfo

- **Thread information:** Reads the information about the CPU-intensive threads and returns the list of top threads that cause heavy utilization of the CPU.
  
  For example,
  
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo
  
  To access the stack trace of threads in the JVM, set the stack parameter to True.
  
  For example,
  
  
  To specify the number of threads in the JVM, specify the value for the thread-count parameter.
  
  For example,
  

- **Cache information:** Reads the cache information for the User Application.
  
  For example,
  
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/cacheinfo

- **Cluster information:** Reads the cluster related information.
  
  For example,
  

**NOTE:** You need to be a Security Administrator to view the User Application health statistics by using the REST API.
Creating Compound Indexes

After installing or upgrading the identity applications, manually create the compound indexes for each attribute that you want to use to sort users in the Identity Manager Dashboard. You can create compound indexes using ndsindex utility which is located in the eDirectory installed path. You can specify multiple attributes separated using $ sign for compound indexing. Following are the basic attributes that require compound indexing:

- Surname, Given Name
- Given Name, Surname
- cn, Surname
- Title, Surname
- Telephone Number, Surname
- Internet Email Address, Surname
- L, Surname
- OU, Surname

The following command helps you to create compound indexes using ndsindex utility:

```
ndsindex add [-h <hostname>] [-p <port>] -D <admin DN> -W[-w <password>] -s <eDirectory Server DN> [<indexName1>, <indexName2>.....]
```

For example, to sort users based on Title, execute the following command:

```
ndsindex add -h <hostname> -p <ldap port> -D <admin DN> -w <admin passwd> -s <eDirectory Server DN> Title-SN;Title$Surname;value
```

You can also create compound indexes using Conversion Export Utility.

You must use an LDIF file to create indexes. After the LDIF file is imported, initiate the indexing activity by triggering Limber. Otherwise, indexing takes place when Limber triggers automatically.

Example LDIF file to create compound indexes to sort users on Title attribute:

```
dn: cn=osg-nw5-7, o=Novell
changetype: modify
add: indexDefinition
indexDefinition: 0$sntitleindex$0$0$0$1$Title$surname
```

For more information LDIF files, see LDIF Files in NetIQ eDirectory Administration Guide.

Configuring Identity Application to Reject Client-initiated SSL Renegotiation

By default, the identity applications installer configures a non-secure connection (http). Under certain circumstances, a non-secure connection can make Identity Manager susceptible to a denial-of-service attack caused by client initiated SSL renegotiation with the identity applications server. To prevent this issue, add the following flag to the CATALINA_OPTS entry in <tomcat-install-directory>\bin\setenv.bat file.
"-Djdk.tls.rejectClientInitiatedRenegotiation=true"
Final Steps for Completing the Installation

After completing the installation and configuration of Identity Manager components, you must perform certain tasks to make your solution work properly in your environment. For example, configure the drivers you installed to meet the policies and requirements defined by your business processes and configure Sentinel Log Management for IGA to gather audit events.

Post-installation tasks typically include the following items:

- “Configuring the Identity Vault” on page 63
- “Configuring the Remote Loader and Drivers” on page 64
- “Configuring Forgotten Password Management” on page 64
- “Configuring the Database for the Identity Applications” on page 68
- “Configuring Identity Applications” on page 71
- “Configuring the Runtime Environment for Data Collection” on page 96
- “Configuring Identity Reporting” on page 105
- “Activating Identity Manager” on page 110
- “Reviewing the Ports Used by Identity Manager Components” on page 110

Configuring the Identity Vault

- Manually Importing Identity Applications and Identity Reporting Certificates into Identity Vault

Manually Importing Identity Applications and Identity Reporting Certificates into Identity Vault

- If you have custom certificates for Identity Applications and Identity Reporting components, import those certificates into cacerts in the Identity Vault (C:\NetIQ\eDirectory\jre\lib\security\cacerts).

  For example, you can use the following keytool command to import certificates into the Identity Vault:

  ```
  keytool -import -trustcacerts -alias <User Application certificate alias name> -keystore <cacerts file> -file <User Application certificate file>
  ```

- If you install SSPR on a different server than the User Application server, import the SSPR application certificate into idm.jks in the User Application (C:\NetIQ\idm\apps\tomcat\conf\idm.jks).
For example, you can use the following keytool command to import certificates into User Application:

```bash
keytool -import -trustcacerts -alias <SSPR certificate alias name> -keystore <idm.jks> -file <SSPR certificate file>
```

### Configuring the Remote Loader and Drivers

Remote Loader allows Identity Manager drivers to access the connected application without requiring to install Identity Vault and Identity Manager engine on the same server as the application. Using Remote Loader requires you to configure the application shim so that it can securely connect with the Identity Manager engine. You must also configure both the Remote Loader and Identity Manager drivers. This information is provided in detail in Configuring the Remote Loader and Drivers in the NetIQ Identity Manager Driver Administration Guide.

### Configuring Forgotten Password Management

The Identity Manager installation includes Self Service Password Reset to help you manage the process for resetting forgotten passwords. Alternatively, you can use an external password management system.

- “Using Self Service Password Reset for Forgotten Password Management” on page 64
- “Using an External System for Forgotten Password Management” on page 66
- “Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment” on page 68

### Using Self Service Password Reset for Forgotten Password Management

In most cases, you can enable the forgotten password management feature when you install SSPR and the identity applications. However, you might not have specified the URL of the landing page for the identity applications to which SSPR forwards users after a password change. You might also need to enable forgotten password management. This section provides the following information:

- “Configuring Identity Manager to Use Self Service Password Reset” on page 64
- “Configuring Self Service Password Reset for Identity Manager” on page 65
- “Locking the SSPR Configuration” on page 65

### Configuring Identity Manager to Use Self Service Password Reset

This section provides information about configuring Identity Manager to use SSPR.

1. Log in to the server where you installed the identity applications.
2. Run the configuration update utility. For more information, see Section 3, “Installation and Configuration Process Overview,” on page 43.
3. In the utility, navigate to Authentication > Password Management.
4. For Password Management Provider, specify Self Service Password Reset (SSPR).
5 (Optional) To provide links for resetting the username or password, or activation of a new user account on the Identity Applications login page, select Other links from the User Interface drop-down list followed by selecting the required check box. Alternatively, you can provide a common link by selecting “Can’t sign in?” from the User Interface drop-down list. The following link will display on the Identity Applications login page: Click here if you’ve forgotten your username or password, or if you need to register.

6 Navigate to IDM SSO Clients > Self Service Password Reset.

7 For OAuth client ID, specify the name that you want to use to identify the single sign-on client for SSPR to the authentication server. The default value is sspr.

8 For OAuth client secret, specify the password for the single sign-on client for SSPR.

9 For OAuth redirect URL, specify the absolute URL to which the authentication server redirects a browser client when authentication is complete.

   Use the following format: protocol://server:port/path. For example, http://10.10.10.48:8180/sspr/public/oauth.

10 Save your changes and close the utility.

Configuring Self Service Password Reset for Identity Manager

This section provides information about configuring SSPR to work with Identity Manager. For example, you might want to modify the password policies and challenge response questions. When you installed SSPR with Identity Manager, you specified a password that an administrator can use to configure the application. NetIQ recommends that you modify the SSPR settings, then specify an administrator account or group can configure SSPR.

NOTE: If you install SSPR on a different server than user application server, ensure that SSPR application certificate is added to user application cacerts.

1 Log in to SSPR by using the configuration password that you specified during installation.

2 In the Settings page, modify the settings for the password policy and challenge response questions. For more information about configuring the default values for SSPR settings, see Configuring Self Service Password Reset in the NetIQ Self Service Password Reset Administration Guide.

3 Lock the SSPR configuration file (SSPRConfiguration.xml). For more information about locking the configuration file, see “Locking the SSPR Configuration” on page 65.

4 (Optional) To modify SSPR settings after you lock the configuration, you must set the configIsEditable setting to true in the SSPRConfiguration.xml file.

5 Log out of SSPR.

6 For the changes to take effect, restart Tomcat.

Locking the SSPR Configuration

1 Go to http://<IP/DNS name>[:<port>]/sspr. This link takes you to the SSPR portal.

2 Log in to the Identity Manager with an administrator account or log in with your existing login credentials.
3 Click **Configuration Manager** at the top of the page and specify the configuration password that you specified during installation.

4 Click **Configuration Editor** and navigate to **Settings > LDAP Settings**.

5 Lock the SSPR configuration file (**SSPRConfiguration.xml**).
   
   5a Under the Administrator Permission section, define a filter in LDAP format for a user or a group that has administrator rights to SSPR in the Identity Vault. By default, the filter is set to `groupMembership=cn=Admins,ou=Groups,o=example`.
   
   For example, set it to `uaadmin (cn=uaadmin)` for the User Application administrator.
   
   This prevents users from modifying the configuration in SSPR except the SSPR admin user who has full rights to modify the settings.

5b To ensure LDAP query returns results, click **View Matches**.

   If there is any error in the setting, you cannot proceed to the next configuration option. SSPR displays the error details to help you troubleshoot the issue.

5c Click **Save**.

5d In the confirmation window that pops up, click **OK**.

   When SSPR is locked, the admin user can see additional options in the Administration user interface such as Dashboard, User Activity, Data Analysis, and so on that were not available for him before SSPR lock down.

6 (Optional) To modify SSPR settings after you lock the configuration, you must set the `configIsEditable` setting to `true` in the **SSPRConfiguration.xml** file.

7 Log out of SSPR.

8 Log in to SSPR again as an admin user defined in **Step 3**.

9 Click **Close Configuration**, then click **OK** to confirm the changes.

10 For the changes to take effect, restart Tomcat.

### Using an External System for Forgotten Password Management

To use an external system, you must specify the location of a WAR file containing Forgot Password functionality. This process includes the following activities:

- “Specifying an External Forgotten Password Management WAR File” on page 67
- “Testing the External Forgot Password Configuration” on page 67
- “Configuring SSL Communication between Application Servers” on page 68
Specifying an External Forgotten Password Management WAR File

If you did not specify these values during installation and want to modify the settings, you can use either the RBPM Configuration utility or make the changes in the User Application as an administrator.

1 (Conditional) To modify the settings in the RBPM Configuration utility, complete the following steps:

1a Log in to the server where you installed the identity applications.
1b Run the RBPM configuration utility. For more information, see Section 3, “Installation and Configuration Process Overview,” on page 43.
1c In the utility, navigate to Authentication > Password Management.
1d For Password Management Provider, specify User Application (Legacy).

2 (Conditional) To modify the settings in the User Application, complete the following steps:

2a Log in as the User Application Administrator.
2b Navigate to Administration > Application Configuration > Password Module Setup > Login.

3 For Forgotten Password, specify External.

4 For Forgot Password Link, specify the link shown when the user clicks Forgot password on the login page. When the user clicks this link, the application directs the user to the external password management system. For example:

http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp

5 For Forgot Password Return Link, specify the link shown after the user finishes performing the forgot password procedure. When the user clicks this link, the user is redirected to the link specified. For example:

http://localhost/IDMProv

6 For Forgot Password Web Service URL, specify the URL for the web service that the external forward password WAR uses to call back to the identity applications. Use the following format:

https://idmhost:sslport/idm/pwdmgt/service

The return link must use SSL to ensure secure web service communication to the identity applications. For more information, see “Configuring SSL Communication between Application Servers” on page 68.

7 Manually copy ExternalPwd.war to the remote application server deploy directory that runs the external password WAR functionality.

Testing the External Forgot Password Configuration

If you have an external password WAR file and want to test the Forgot Password functionality by accessing it, you can access it in the following locations:

- On the User Application login page, click the link for Forgot password.
Configuring SSL Communication between Application Servers

If you use an external password management system, you must configure SSL communication between the Tomcat instances on which you deploy the identity applications and the External Forgotten Password Management WAR file. For more information, refer to the Tomcat documentation.

Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment

The installation process assumes that you deploy SSPR on the same application server as the identity applications and Identity Reporting. By default, the built-in links on the Applications page in the Dashboard use a relative URL format that points to SSPR on the local system. For example, \sspr\private\changepassword. If you install the applications in a distributed or clustered environment, you must update the URLs for the SSPR links.

For more information, see the Help for the Identity Applications.

1. Log in as an administrator to the Dashboard. For example, log in as uaadmin.
2. Click Edit.
3. In the Edit Home Items page, hover on the item that you want to update, and then click the edit icon. For example, select Change My Password.
4. For Link, specify the absolute URL. For example, http://10.10.10.48:8180/sspr/changepassword.
5. Click Save.
6. Repeat for each SSPR link that you want to update.
7. Upon completion, click I’m done.
8. Log out, and then log in as a regular user to test the changes.

Configuring the Database for the Identity Applications

The database for the Identity Applications supports tasks such as storing configuration data and data for workflow activities. Before you can install the applications, the database must be installed and configured. For more information about supported databases, see the NetIQ Identity Manager System requirements Page.

NOTE: If you are migrating to a new version of RBPM and the Identity Applications, you must use the same database that you used for the previous installation. That is, the installation from which you are migrating.

- “Configuring an Oracle Database” on page 69
- “Configuring a SQL Server Database” on page 70
Configuring an Oracle Database

This section provides configuration options for using an Oracle database for the User Application. For information about supported versions of Oracle, see the NetIQ Identity Manager Technical Information website.

Checking Compatibility Level of Databases

Databases from different releases of Oracle are compatible if they support the same features and those features perform the same way. If they are not compatible, certain features or operations might not work as expected. For example, creation of schema fails that does not allow you to deploy the identity applications.

To check the compatibility level of your database, perform the following steps:

1. Connect to the Database Engine.
2. After connecting to the appropriate instance of the SQL Server Database Engine, in Object Explorer, click the server name.
3. Expand Databases, and, depending on the database, either select a user database or expand System Databases and select a system database.
4. Right-click the database, and then click Properties.
   The Database Properties dialog box opens.
5. In the Select a page pane, click Options.
   The current compatibility level is displayed in the Compatibility level list box.
6. To check the Compatibility Level, enter the following in the query window and click Execute.
   SQL> SELECT name, value FROM v$parameter
   WHERE name = 'compatible';
   The expected output is: 12.2.0.1

Configuring the Character Set

Your User Application database must use a Unicode-encoded character set. When creating the database, use AL32UTF8 to specify this character set.

To confirm that an Oracle 12c database is set for UTF-8, issue the following command:

```
select * from nls_database_parameters;
```

If the database is not configured for UTF-8, the system responds with the following information:

NLS_CHARACTERSET
WE8MSWIN1252

Otherwise, the system responds with the following information that confirms the database is configured for UTF-8:

NLS_CHARACTERSET
AL32UTF8
NOTE: It is recommended to use JDBC JAR version ojdbc6.jar.

For more information about configuring a character set, see “Choosing an Oracle Database Character Set”.

Configuring the Admin User Account

The User Application requires that the Oracle database user account have specific privileges. In the SQL Plus utility, enter the following commands:

```
CREATE USER idmuser IDENTIFIED BY password
GRANT CONNECT, RESOURCE to idmuser
ALTER USER idmuser quota 100M on USERS;
```

where `idmuser` represents the user account.

Configuring a SQL Server Database

This section provides configuration options for using an SQL Server database for the User Application. For information about supported versions of SQL Server, see the NetIQ Identity Manager Technical Information website.

Configuring the Character Set

SQL Server does not allow you to specify the character set for databases. The User Application stores SQL Server character data in a NCHAR column type, which supports UTF-8.

NOTE: The only supported collation for SQL is SQL_Latin1_General_CP1_CI_AS.

Configuring the Admin User Account

After installing a supported version of Microsoft SQL Server, create a database and database user using an application such as SQL Server Management Studio. The database user account must have the following privileges:

- CREATE TABLE
- DELETE
- INSERT
- SELECT
- UPDATE

NOTE: It is recommended to use JDBC JAR version sqljdbc4.jar with Microsoft SQL Server 2014 and sqljdbc42.jar with Microsoft SQL Server 2016.
Configuring Identity Applications

- “Configuring the Settings for the Identity Applications” on page 71
- “Deploying REST APIs for Identity Applications” on page 93
- “Accessing the Oracle Database Using Oracle Service Name” on page 93
- “Manually Creating the Database Schema” on page 94
- “Configuring Single Sign-On Settings for the Identity Applications” on page 95
- “Starting the Identity Applications” on page 96
- “Configuration and Usage Considerations for the Identity Applications” on page 96

Configuring the Settings for the Identity Applications

The Identity Applications Configuration utility helps you manage the settings for the User Application drivers and the identity applications. The installation program for the identity applications invokes a version of this utility so that you can more quickly configure the applications. You can also modify most of these settings after installation.

The file to run the Configuration utility (configupdate.bat) is located by default in an installation subdirectory for the identity applications (C:\NetIQ\idm\apps\UserApplication).

NOTE: In a cluster, the configuration settings must be identical for all members of the cluster.

This section explains the settings in the configuration utility. The settings are organized by tabs. If you install Identity Reporting, the process adds parameters for Reporting to the utility.

- “Running the Identity Applications Configuration Utility” on page 71
- “User Application Parameters” on page 72
- “Reporting Parameters” on page 82
- “Authentication Parameters” on page 84
- “SSO Clients Parameters” on page 88
- “CEF Auditing Parameters” on page 92

Running the Identity Applications Configuration Utility

1 Open the configupdate.properties file in a text editor and verify that the following options are configured:

   edit_admin="true"

   use_console="false"

2 At the command prompt, run the configuration utility (configupdate.bat).

   NOTE: You might need to wait a few minutes for the utility to start up.
User Application Parameters

When configuring the identity applications, this tab defines the values that the applications use when communicating with the Identity Vault. Some settings are required for completing the installation process.

By default, the tab displays the basic options. To see all settings, click Show Advanced Options. This tab includes the following groups of settings:

- “Identity Vault Settings” on page 72
- “Identity Vault DN” on page 73
- “Identity Vault User Identity” on page 76
- “Identity Vault User Groups” on page 77
- “Identity Vault Certificates” on page 78
- “Email Server Configuration” on page 78
- “Trusted Key Store” on page 80
- “NetIQ Sentinel Digital Signature Certificate & Key” on page 80
- “Miscellaneous” on page 81
- “Container Object” on page 82

Identity Vault Settings

This section defines the settings that enable the identity applications to access the user identities and roles in the Identity Vault. Some settings are required for completing the installation process.

Identity Vault Server

Required

Specifies the hostname or IP address for your LDAP server. For example: myLDAPHost.

LDAP port

Specifies the port on which the Identity Vault listens for LDAP requests in clear text. The default value is 389.

LDAP secure port

Specifies the port on which the Identity Vault listens for LDAP requests using Secure Sockets Layer (SSL) protocol. The default value is 636.

If a service already loaded on the server (before you install eDirectory) uses the default port, you must specify a different port.

Identity Vault Administrator

Required

Specifies the credentials for the LDAP Administrator. For example, cn=admin. This user must already exist in the Identity Vault.

The identity applications use this account to make an administrative connection to the Identity Vault. This value is encrypted, based on the master key.
Identity Vault Administrator Password

Required

Specifies the password associated the LDAP Administrator. This password is encrypted, based on the master key.

Use Public Anonymous Account

Specifies whether users who are not logged in can access the LDAP Public Anonymous Account.

Secure Administrator Connection

Specifies whether RBPM uses SSL protocol for all communication related to the admin account. This setting allows other operations that do not require SSL to operate without SSL.

**NOTE:** This option might have adverse performance implications.

Secure User Connection

Specifies whether RBPM uses TLS/SSL protocol for all communication related to the logged-in user's account. This setting allows other operations that do not require TLS/SSL to operate without the protocol.

**NOTE:** This option might have adverse performance implications.

Identity Vault DNs

This section defines the distinguished names for containers and user accounts that enable communication between the identity applications and other Identity Manager components. Some settings are required for completing the installation process.

Root Container DN

Required

Specifies the LDAP distinguished name of the root container. This is used as the default entity definition search root when no search root is specified in the directory abstraction layer. For example, o=mycompany.

User Container DN

Required

When showing the advanced options, the utility displays this parameter under Identity Vault User Identity.

Specifies the LDAP distinguished name (DN) or fully qualified LDAP name of the user container. The following considerations apply to this setting:

- Users in this container (and below) are allowed to log in to the identity applications.
- If you have started Tomcat hosting the identity applications, you cannot change this setting with the configupdate.bat file.
- This container must include the User Application Administrator that you specified as you set up the User Application driver. Otherwise, the specified account cannot execute workflows.
Group Container DN

*Required*

When showing the advanced options, the utility displays this parameter under Identity Vault User Groups.

Specifies the LDAP distinguished name (DN) or fully qualified LDAP name of the group container. The following considerations apply to this setting:

- Entity definitions within the directory abstraction layer use this DN.
- If you have started Tomcat hosting the identity applications, you cannot change this setting with the `configupdate.bat` file.

User Application Driver

*Required*

Specifies the distinguished name of the User Application driver.

For example, if your driver is `UserApplicationDriver` and your driver set is called `myDriverSet`, and the driver set is in a context of `o=myCompany`, specify `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`.

User Application Administrator

*Required*

Specifies an existing user account in the Identity Vault that has the rights to perform administrative tasks for the specified user container for User Application. The following considerations apply to this setting:

- If you have started Tomcat hosting the User Application, you cannot change this setting with the `configupdate.bat` file.
- To change this assignment after you deploy the User Application, use the Administration > Security pages in the User Application.
- This user account has the right to use the Administration tab of the User Application to administer the portal.
- If the User Application Administrator participates in workflow administration tasks exposed in iManager, Designer, or the User Application (Requests & Approvals tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. For more information, see the User Application Administration Guide for details.

Provisioning Administrator

Specifies an existing user account in the Identity Vault that will manage Provisioning Workflow functions available throughout the User Application.

To change this assignment after you deploy the User Application, use the Administration > Administrator Assignments page in the User Application.
Compliance Administrator
Specifications an existing account in the Identity Vault that performs a system role to allow members to perform all functions on the Compliance tab. The following considerations apply to this setting:

- To change this assignment after you deploy the identity applications, use the Administration > Administrator Assignments page in the User Application.
- During a configuration update, changes to this value take effect only if you do not have a valid Compliance Administrator assigned. If a valid Compliance Administrator exists, then your changes are not saved.

Roles Administrator
Specifications the role that allows members to create, remove, or modify all roles, and grant or revoke any role assignment to any user, group, or container. It also allows its role members to run any report for any user. The following considerations apply to this setting:

- By default, the User Application Admin is assigned this role.
- To change this assignment after you deploy the identity applications, use the Administration > Administrator Assignments page in the User Application.
- During a configuration update, changes to this value take effect only if you do not have a valid Roles Administrator assigned. If a valid Roles Administrator exists, then your changes are not saved.

Security Administrator
Specifications the role that gives members the full range of capabilities within the Security domain. The following considerations apply to this setting:

- The Security Administrator can perform all possible actions for all objects within the Security domain. The Security domain allows the Security Administrator to configure access permissions for all objects in all domains within RBPM. The Security Administrator can configure teams, and also assign domain administrators, delegated administrators, and other Security Administrators.
- To change this assignment after you deploy the identity applications, use the Administration > Administrator Assignments page in the User Application.

Resources Administrator
Specifications the role that gives members the full range of capabilities within the Resource domain. The following considerations apply to this setting:

- The Resources Administrator can perform all possible actions for all objects within the Resource domain.
- To change this assignment after you deploy the identity applications, use the Administration > Administrator Assignments page in the User Application.
RBPM Configuration Administrator

Specifies the role that gives members the full range of capabilities within the Configuration domain. The following considerations apply to this setting:

- The RBPM Configuration Administrator can perform all possible actions on all objects within the Configuration domain. The RBPM Configuration Administrator controls access to navigation items within RBPM. In addition, the RBPM Configuration Administrator configures the delegation and proxy service, the provisioning user interface, and the workflow engine.
- To change this assignment after you deploy the identity applications, use the Administration > Administrator Assignments page in the User Application.

RBPM Reporting Administrator

Specifies the Reporting Administrator. By default, the installation program lists this value as the same user as the other security fields.

Identity Vault User Identity

This section defines the values that enable the identity applications to communicate with a user container in the Identity Vault. Some settings are required for completing the installation process.

The utility displays these settings only when you select Show Advanced Options.

User Container DN

*Required*

*When not showing the advanced options, the utility displays this parameter under Identity Vault DNs.*

Specifies the LDAP distinguished name (DN) or fully qualified LDAP name of the user container. The following considerations apply to this setting:

- Users in this container (and below) are allowed to log in to the identity applications.
- If you have started Tomcat hosting the identity applications, you cannot change this setting with the configupdate.bat file.
- This container must include the User Application Administrator that you specified as you set up the User Application driver. Otherwise, the specified account cannot execute workflows.

User Search Scope

Specifies the depth of scope that Identity Vault users can search the container.

User Object Class

Specifies the object class of the LDAP user. Usually the class is *inetOrgPerson*.

Login Attribute

Specifies the LDAP attribute that represents the user’s login name. For example, *cn*.

Naming Attribute

Specifies the LDAP attribute used as the identifier when looking up users or groups. This is not the same as the login attribute, which is used only during login. For example, *cn*.
User Membership Attribute
(Optional) Specifies the LDAP attribute that represents the user’s group membership. Do not use spaces when specifying the name.

Identity Vault User Groups
This section defines the values that enable the identity applications to communicate with a group container in the Identity Vault. Some settings are required for completing the installation process.

The utility displays these settings only when you select Show Advanced Options.

Group Container DN
Required
When not showing the advanced options, the utility displays this parameter under Identity Vault DNs.
Specifies the LDAP distinguished name (DN) or fully qualified LDAP name of the group container. The following considerations apply to this setting:
• Entity definitions within the directory abstraction layer use this DN.
• If you have started Tomcat hosting the identity applications, you cannot change this setting with the configupdate.bat file.

Group Container Scope
Specifies the depth of scope that Identity Vault users can search for the group container.

Group Object Class
Specifies the object class of the LDAP group. Usually the class is groupOfNames.

Group Membership Attribute
(Optional) Specifies the user’s group membership. Do not use spaces in this name.

Use Dynamic Groups
Specifies whether you want to use dynamic groups.
You must also specify a value for Dynamic Group Object Class.

Dynamic Group Object Class
Applies only when you select Use Dynamic Groups.
Specifies the object class of the LDAP dynamic group. Usually the class is dynamicGroup.
Identity Vault Certificates

This section defines the path and password for the JRE keystore. Some settings are required for completing the installation process.

Keystore Path

  *Required*

  Specifies the full path to your keystore (cacerts) file of the JRE that Tomcat uses to run. You can manually enter the path or browse to the cacerts file. The following considerations apply to this setting:
  
  - In environments, you must specify the installation directory of RBPM. The default value is set to the correct location.
  - The installation program for the identity applications modifies the keystore file.

Keystore Password

  *Required*

  Specifies the password for the keystore file. The default is changeit.

Email Server Configuration

This section defines the values that enable email notifications, which you can use for email-based approvals. For more information, see the NetIQ Identity Manager - Administrator’s Guide to the Identity Applications.

Notification Template Host

  Specifies the name or IP address of Tomcat that hosts the identity applications. For example, myapplication_serverServer.

  This value replaces the $HOST$ token in e-mail templates. The installation program uses this information to create a URL to provisioning request tasks and approval notifications.

Notification Template Port

  Specifies the port number of Tomcat that hosts the identity applications.

  This value replaces the $PORT$ token in e-mail templates that are used in provisioning request tasks and approval notifications.

Notification Template Secure Port

  Specifies the secure port number of Tomcat that hosts the identity applications.

  This value replaces the $SECURE_PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.

Notification Template Protocol

  Specifies a non-secure protocol included in the URL when sending user email. For example, http.

  This value replaces the $PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications.
Notification Template Secure Protocol

Specifies the secure protocol included in the URL when sending user email. For example, https.
This value replaces the $SECURE_PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications.

Notification SMTP Email From

Specifies the email account that the identity applications use to send email notifications.

SMTP Server Name

Specifies the IP address or DNS name of the SMTP email host that the identity applications use for provisioning emails. Do not use localhost.

Server requires authentication

Specifies whether you want the server to require authentication.
You must also specify the credentials for the email server.

User name

*Applies only when you enable Server requires authentication.*
Specifies the name of a login account for the email server.

Password

*Applies only when you enable Server requires authentication.*
Specifies the password of a login account for the mail server.

Use SMTP TLS

Specifies whether you want to secure the contents of email messages during transmission between the mail servers.

Email Notification Image Location

Specifies the path to the image that you want to include in email notifications.
When the Identity Applications server and the email server are both set to use secure connection, make sure that the following conditions are met:

- The certificate used to establish a secure connection between the Identity Applications server and the email server is a trusted CA certificate
- Use https in the image path. For example, https://localhost:8543/IDMProv/images

If Identity Applications is operating on a server that use http for plain text communication, replace https with http in the image path. An example of the image path: http://localhost:8080/IDMProv/images

Sign email

Specifies whether you want to add a digital signature to outgoing messages.
If you enable this option, you must also specify settings for the keystore and signature key.

Keystore Path

*Applies only when you enable Sign email.*
Specifies the full path to the keystore (cacerts) file that you want to use for digitally signing an email. You can manually enter the path or browse to the cacerts file. For example, `C:\NetIQ\idm\apps\jre\lib\security\cacerts`.

**Keystore Password**

*Aplies only when you enable* Sign email.

Specifies the password for the keystore file. For example, `changeit`.

**Alias of signature key**

*Aplies only when you enable* Sign email.

Specifies the alias of the signing key in the keystore. For example, `idmapptest`.

**Signature key password**

*Aplies only when you enable* Sign email.

Specifies the password that protects the file containing the signature key. For example, `changeit`.

**Trusted Key Store**

This section defines the values for the trusted keystore for the identity applications. The utility displays these settings only when you select *Show Advanced Options*.

**Trusted Store Path**

Specifies the path to the Trusted Key Store that contains all trusted signers’ certificates. If this path is empty, the identity applications get the path from System property `javax.net.ssl.trustStore`. If the System property cannot provide the path, the installation program defaults to `jre\lib\security\cacerts`.

**Trusted Store Password**

Specifies the password for the Trusted Key Store. If you leave this field is empty, the identity applications gets the password from System property `javax.net.ssl.trustStorePassword`. If the System property cannot provide the path, the installation program defaults to `changeit`.

This password is encrypted, based on the master key.

**Trusted Store Type**

Specifies whether the trusted store path uses a Java keystore (JKS) or PKCS12 for digital signing.

**NetIQ Sentinel Digital Signature Certificate & Key**

This section defines the values that allows Identity Manager to communicate with Sentinel for auditing events. The utility displays these settings only when you select *Show Advanced Options*.

**Sentinel Digital Signature Certificate**

Lists the custom public key certificate that you want the OAuth server to use to authenticate audit messages sent to Sentinel.

**Sentinel Digital Signature Private Key**

Specifies the path to the custom private key file that you want the OAuth server to use to authenticate audit messages sent to Sentinel.
Miscellaneous

The utility displays these settings only when you select Show Advanced Options.

OCSP URI

Specifies the Uniform Resource Identifier (URI) to use when the client installation uses the On-Line Certificate Status Protocol (OCSP). For example, http://host:port/ocspLocal.

The OCSP URI updates the status of trusted certificates online.

Authorization Config Path

Specifies the fully qualified name of the authorization configuration file.

Identity Vault Indexes

During installation, specifies whether you want the installation program to create indexes on the manager, ismanager, and srvprvUUID attributes. After installation, you can modify the settings to point to a new location of the indexes. The following considerations apply to this setting:

- Without indexes on these attributes, identity applications users can experience impeded performance of the identity applications.
- You can create these indexes manually by using iManager after you install the identity applications.
- For best performance, you should create the index during installation.
- The indexes must be in Online mode before you make the identity applications available to users.
- To create or delete an index, you must also specify a value for Server DN.

Server DN

Applies only when you want to create or delete an Identity Vault index.

Specifies the eDirectory server where you want the indexes to be created or removed.

You can specify only one server at a time. To configure indexes on multiple eDirectory servers, you must run the RBPM Configuration utility multiple times.

Reinitialize RBPM Security

Specifies whether you want to reset RBPM security when the installation process completes. You must also redeploy the identity applications.

IDMReport URL

Specifies the URL of the Identity Manager Reporting Module. For example, http://hostname:port/IDMRPT.

Custom Themes Context Name

Specifies the name of the customized theme that you want to use for displaying the identity applications in the browser.

Log Message Identifier Prefix

Specifies the value that you want to use in the layout pattern for the CONSOLE and FILE appenders in the idmuserapp_logging.xml file. The default value is RBPM.
Change RBPM Context Name
   Specifies whether you want to change the context name for RBPM.
   You must also specify the new name and DN of the Roles and Resource driver.

RBPM Context Name
   Applies only when you select Change RBPM Context Name.
   Specifies the new context name for RBPM.

Role Driver DN
   Applies only when you select Change RBPM Context Name.
   Specifies the DN of the Roles and Resource driver.

Container Object
   These parameters apply only during installation.
   This section helps you to define the values for container objects or create new container objects.

Selected
   Specifies the Container Object Types that you want to use.

Container Object Type
   Specifies the container: locality, country, organizationalUnit, organization, or domain.
   You can also define your own containers in iManager and add them under Add a new Container Object.

Container Attribute Name
   Specifies the name of the Attribute Type associated with the specified Container Object Type.

Add a New Container Object: Container Object Type
   Specifies the LDAP name of an object class from the Identity Vault that can serve as a new container.

Add a New Container Object: Container Attribute Name
   Specifies the name of the Attribute Type associated with the new Container Object Type.

Reporting Parameters

When configuring the identity applications, this tab defines the values for managing Identity Reporting. The utility adds this tab when you install Identity Reporting.

By default, the tab displays the basic options. To see all settings, click Show Advanced Options. This tab includes the following groups of settings:

- “Email Delivery Configuration” on page 83
- “Report Retention Values” on page 83
- “Modify Locale” on page 84
- “Role Configuration” on page 84
- “Outbound Proxy” on page 84
Email Delivery Configuration

This section defines the values for sending notifications.

SMTP Server Hostname
 Specifies the DNS name or IP address of the email server than you want Identity Reporting to use when sending notification. Do not use localhost.

SMTP Server Port
 Specifies the port number for the SMTP server.

SMTP Use SSL
 Specifies whether you want to use TLS/SSL protocol for communication with the email server.

Server Needs Authentication
 Specifies whether you want to use authentication for communications with the email server.

SMTP User Name
 Specifies the email address that you want to use for authentication.
 You must specify a value. If the server does not require authentication, you can specify an invalid address.

SMTP User Password
 Applies only when you specify that the server requires authentication.
 Specifies the password for the SMTP user account.

Default Email Address
 Specifies the email address that you want Identity Reporting to use as the origination for email notifications.

Report Retention Values

This section defines the values for storing completed reports.

Report Unit, Report Lifetime
 Specifies the amount of time that Identity Reporting keeps completed reports before deleting them. For example, to specify six months, enter 6 in the Report Lifetime field and then select Month in the Report Unit field.

Location of Reports
 Specifies a path where you want to store the report definitions. For example, C:\NetIQ\idm\apps\IdentityReporting.
Modify Locale
This section defines the values for the language that you want Identity Reporting to use. Identity Reporting uses the specific locales in searches. For more information, see the Administrator Guide to NetIQ Identity Reporting.

Role Configuration
This section defines the values for the authentication sources that Identity Reporting uses to generate reports.

Add Authentication Source
Specifies the type of authentication source that you want to add for reporting. Authentication sources can be
- Default
- LDAP Directory
- File

Outbound Proxy
Applies only when you use Identity Manager 4.8.1 or later versions.
This section defines the values to use reverse proxy server that Identity Reporting uses to download reports.

Use Proxy
Specifies the option to use Reverse Proxy server for reporting.
- Hostname or IP address
- Port
- Use TLS
  Applies only when you want to use TCP as your network protocol.

Authentication Parameters
When configuring the identity applications, this tab defines the values that Tomcat uses to direct users to the identity application and password management pages.

By default, the tab displays the basic options. To see all settings, click Show Advanced Options. This tab includes the following groups of settings:
- “Authentication Server” on page 85
- “Authentication Configuration” on page 85
- “Authentication Method” on page 86
- “Password Management” on page 86
- “Sentinel Digital Signature Certificate and Key” on page 88
Authentication Server

This section defines settings for the identity applications to connect to the authentication server.

**OAuth server host identifier**

*Required*

Specifies the relative URL of the authentication server that issues tokens to OSP. For example, 192.168.0.1.

**OAuth server TCP port**

Specifies the port for the authentication server.

**Access Manager is the OAuth provider**

Converting from OSP to NAM for OAuth is not supported from Authentication tab of configuration update utility. To hide this option, set the `no_nam_oauth` value to “true” in `configupdate.sh.properties` file.

**OAuth server is using TLS/SSL**

Specifies whether the authentication server uses TLS/SSL protocol for communication.

**Optional TLS/SSL truststore file**

*Applies only when you select OAuth server is using TLS/SSL and the utility is showing the advanced options.*

**Optional TLS/SSL truststore password**

*Applies only when you select OAuth server is using TLS/SSL and the utility is showing the advanced options.*

Specifies the password used to load the keystore file for the TLS/SSL authentication server.

**NOTE:** If you do not specify the keystore path and password, and the trust certificate for the authentication server is not in the JRE trust store (cacerts), the identity applications fail to connect to the authentication service that uses TLS/SSL protocol.

Authentication Configuration

This section defines settings for the authentication server.

**LDAP DN of Admins Container**

*Required*

Specifies the distinguished name of the container in the Identity Vault that contains any administrator User objects that OSP must authenticate. For example, `ou=sa,o=data`.

**Duplicate resolution naming attribute**

Specifies the name of the LDAP attribute used to differentiate between multiple eDirectory User objects with the same `cn` value. The default value is `mail`.

**Restrict authentication sources to contexts**

Specifies whether searches in the user and administrator containers in the Identity Vault are restricted to only User objects in those containers or searches should also include subcontainers.
Final Steps for Completing the Installation

**Session Timeout (minutes)**
Specifies the number of minutes of inactivity in a session before the server times out the user’s session. The default value is 20 minutes.

**Access token lifetime (seconds)**
Specifies the number of seconds an OSP access token remains valid. The default value is 60 seconds.

**Refresh token lifetime (hours)**
Specifies the number of seconds an OSP refresh token remains valid. The refresh token is used internally by OSP. The default value is 48 hours.

**Authentication Method**
This section defines the values that enable OSP to authenticate users who log in to the browser-based components of Identity Manager.

**Method**
Specifies the type of authentication that you want Identity Manager to use when a user logs on.

- **Name and Password**: OSP verifies authentication with the identity vault.
- **Kerberos**: OSP accepts authentication from both a Kerberos ticket server and the identity vault. You must also specify a value for **Mapping attribute name**.
- **SAML 2.0**: OSP accepts authentication from both a SAML identity provider and the identity vault. You must also specify values for **Mapping attribute name** and **Metadata URL**.

**Mapping attribute name**
*Applies only when you specify** Kerberos or SAML.**

Specifies the name of the attribute that maps to the Kerberos ticket server or SAML representations at the identity provider.

**Metadata URL**
*Applies only when you specify** SAML.

Specifies the URL that OSP uses to redirect the authentication request to SAML.

**Password Management**
This section defines the values that enable users to modify their passwords as a self-service operation.

**Password Management Provider**
Specifies the type of password management system that you want to use.

- **User Application (Legacy)**: Uses the password management program that Identity Manager traditionally has used. This option also allows you to use an external password management program.
Self Service Password Reset (SSPR): Use the NetIQ Self Service Password Reset service included with the Identity Applications that helps users to reset their password without administrative intervention. You can select the links that will display on the Identity Applications Dashboard login page, allowing users to select the appropriate action for resetting the login access based on their requirement. For more information, see “User Interface” on page 87.

SSPR is the default selection for the Password Management Provider field.

Forgotten Password

This menu list applies only when you select User Application (Legacy).

Specifies whether you want to use the password management system integrated with the User Application or an external system.

- **Internal:** Use the default internal Password Management functionality, /jsps/pwdmgt/ForgotPassword.jsp (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR.

- **External:** Use an external Forgot Password WAR to call back the User Application through a web service. You must also specify the settings for the external system.

Forgotten Password Link

Applies only when you want to use an external password management system.

Specifies the URL that points to the Forgot Password functionality page. Specify a ForgotPassword.jsp file in an external or internal password management WAR.

Forgotten Password Return Link

Applies only when you want to use an external password management system.

Specifies the URL for the Forgot Password Return Link that the user can click after performing a forgot password operation.

Forgotten Password Web Service URL

Applies only when you want to use an external password management system.

Specifies the URL that the External Forgot Password WAR will use to call back to the User Application to perform core forgot password functionalities. Use the following format:

https://<idmhost>:<sslport>/<idm>/pwdmgt/service

User Interface

This menu list applies only when you select Self Service Password Reset (SSPR).

Specifies the links that you want to display on the login page of Identity Applications Dashboard. The default selection, “Can't sign in?” displays a common link for resetting the username or password, or to register for the access permission on the login page. If you select None, the user will have no option to reset the password on their own.

When you select “Other links”, the following options are available for selection:

- **Forgot password:** Provides a link that an existing user can click to reset their password in case they have forgotten.
- **Forgot Username**: Provides a link that an existing user can click to reset their username and password in case they have forgotten.
- **Activate account**: Provides a link that the user can click to create a new user account for accessing Identity Applications.

**Sentinel Digital Signature Certificate and Key**

This section defines the values that allows Identity Manager to communicate with Sentinel for auditing events.

**Sentinel Digital Signature Certificate**

Specifies a custom public key certificate that you want the OSP server to use to authenticate audit messages sent to the audit system.

For information about configuring certificates for Novell Audit, see “Managing Certificates” in the *Novell Audit Administration Guide*.

**Sentinel Digital Signature Private Key**

Specifies the path to the custom private key file that you want the OSP server to use to authenticate audit messages sent to the audit system.

**SSO Clients Parameters**

When configuring the identity applications, this tab defines the values for managing single sign-on access to the applications.

By default, the tab displays the basic options. To see all settings, click *Show Advanced Options*. This tab includes the following groups of settings:

- “IDM Dashboard” on page 88
- “IDM Administrator” on page 89
- “RBPM” on page 89
- “Reporting” on page 90
- “IDM Data Collection Service” on page 91
- “DCS Driver” on page 91
- “Self Service Password Reset” on page 92

**IDM Dashboard**

This section defines the values for the URL that users need to access the Identity Manager Dashboard, which is the primary login location for the identity applications.

<table>
<thead>
<tr>
<th>IDM Dashboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAuth client ID</td>
</tr>
<tr>
<td>OAuth client secret</td>
</tr>
</tbody>
</table>
OAuth client ID

Required

Specifies the name that you want to use to identify the single sign-on client for the Dashboard to the authentication server. The default value is idmdash.

OAuth client secret

Required

Specifies the password for the single sign-on client for the Dashboard.

OSP OAuth redirect URL

Required

Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

Use the following format: protocol://server:port/path. For example, https://192.168.0.1:8543/idmdash/oauth.html.

IDM Administrator

This section defines the values for the URL that users need to access the Identity Manager Administrator page.

OAuth client ID

Required

Specifies the name that you want to use to identify the single sign-on client for the Identity Manager Administrator to the authentication server. The default value is idmadmin.

OAuth client secret

Required

Specifies the password for the single sign-on client for the Identity Manager Administrator.

OSP OAuth redirect URL

Required

Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

Use the following format: protocol://server:port/path. For example, https://192.168.0.1:8543/idmadmin/oauth.html.

RBPM

This section defines the values for the URL that users need to access the User Application.
OAuth client ID

*Required*

Specifies the name that you want to use to identify the single sign-on client for the User Application to the authentication server. The default value is `rbpm`.

OAuth client secret

*Required*

Specifies the password for the single sign-on client for the User Application.

URL link to landing page

*Required*

Specifies the relative URL to use to access the Dashboard from the User Application. The default value is `/landing`.

OSP OAuth redirect URL

*Required*

Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

Use the following format: `protocol://server:port/path`. For example, `https://192.168.0.1:8543/IDMProv/oauth`.

RBPM to eDirectory SAML configuration

*Required*

Specifies the RBPM to eDirectory SAML settings required for SSO authentication.

**Reporting**

This section defines the values for the URL that users need to access Identity Reporting. The utility display these values only if you add Identity Reporting to your Identity Manager solution.

<table>
<thead>
<tr>
<th>Reporting</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>OAuth client ID</td>
<td>rpt</td>
</tr>
<tr>
<td>OAuth client secret</td>
<td>...</td>
</tr>
<tr>
<td>URL link to landing page</td>
<td>/admdash/*landing</td>
</tr>
<tr>
<td>URL link to Identity Governance</td>
<td></td>
</tr>
</tbody>
</table>

OAuth client ID

*Required*

Specifies the name that you want to use to identify the single sign-on client for the Identity Reporting to the authentication server. The default value is `rpt`.

OAuth client secret

*Required*

Specifies the password for the single sign-on client for Identity Reporting.
Final Steps for Completing the Installation

URL link to landing page

*Required*

Specifies the relative URL to use to access the Dashboard from Identity Reporting. The default value is /idmdash/#/landing.

If you installed Identity Reporting and the identity applications in separate servers, then specify an absolute URL. Use the following format: `protocol://server:port/path`. For example, `https://192.168.0.1:8543/IDMRPT/oauth`.

OSP OAuth redirect url

*Required*

Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

Use the following format: `protocol://server:port/path`. For example, `https://192.168.0.1:8543/IDMRPT/oauth`.

IDM Data Collection Service

This section defines the values for the URL that users need to access the Identity Manager Data Collection Service.

OAuth client ID

*Required*

Specifies the name that you want to use to identify the single sign-on client for Identity Manager Data Collection Service to the authentication server. The default value is `idmdcs`.

OAuth client secret

*Required*

Specifies the password for the single sign-on client for the Identity Manager Data Collection Service.

OSP OAuth redirect URL

*Required*

Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

Use the following format: `protocol://server:port/path`. For example, `https://192.168.0.1:8543/idmdcs/oauth.html`.

DCS Driver

This section defines the values for managing the Data Collection Services driver.

*Figure 4-1*

<table>
<thead>
<tr>
<th>DCS Driver</th>
<th>OAuth client ID</th>
<th>OAuth client secret</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCS Driver</td>
<td>dev/</td>
<td>........</td>
</tr>
</tbody>
</table>
OAuth client ID
Specifies the name that you want to use to identify the single sign-on client for the Data Collection Service driver to the authentication server. The default value for this parameter is dcdrv.

OAuth client secret
Specifies the password for the single sign-on client for the Data Collection Service driver.

Self Service Password Reset
This section defines the values for the URL that users need to access SSPR.

OAuth client ID
*Required*
Specifies the name that you want to use to identify the single sign-on client for SSPR to the authentication server. The default value is sspr.

OAuth client secret
*Required*
Specifies the password for the single sign-on client for SSPR.

OAuth redirect URL
*Required*
Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.


CEF Auditing Parameters
This section defines the values for managing the CEF Auditing parameters.

Send audit events
Specifies whether you want to use CEF for auditing events in Identity Applications.

Destination host
Specifies the DNS name or the IP address of the auditing server.

Destination port
Specifies the port of the auditing server.

Network Protocol
Specifies the network protocol used by the auditing server to receive CEF events.

Use TLS
*Applies only when you want to use TCP as your network protocol.*
Specifies if the auditing server is configured to use TLS with TCP.
Intermediate event store directory

Specifies the location of the cache directory before the CEF events are sent to the auditing server.

NOTE: Ensure that the novlua permissions are set for the Intermediate event store directory. Otherwise, you cannot access the IDMDash and IDMProv applications. Also, none of the OSP events will be logged in the Intermediate event store directory. For example, you can change the permission and ownership of the directory using the `chown novlua:novlua <directorypath>` command, where `<directorypath>` is the Intermediate event store directory.

Deploying REST APIs for Identity Applications

The identity applications components incorporate several REST APIs that enable different features within Identity Applications. The REST services use OAUTH2 protocol to provide authentication. You can invoke these APIs using a browser or curl command in scripts to automate the administrative tasks. The REST APIs and the corresponding documentation are available in the `idmappsdoc.war` file. The war is automatically deployed when Identity Applications are installed. For more information, see the REST API documentation.

To access the REST API documentation on the server where identity applications are installed, specify `https://<identity applications servername>:<Port>/idmappsdoc`, in the address bar of your browser. For example: `https://192.168.0.1:8543/idmappsdoc`.

Accessing the Oracle Database Using Oracle Service Name

You can connect to the Oracle database by using Oracle System ID (SID) or Oracle Service Name. The identity applications installer accepts only SID. If you want to access the database by using a service name, complete the identity applications installation to one database instance by connecting through SID. After the installation is completed, perform the following actions:

1. Create a service name in the Oracle database by running the following command:

   ```
   alter system set service_names='SERVICE1' scope=both sid='*';
   ```

   where `SERVICE 1` is the name of the Oracle service.

   NOTE: You can specify the service name in uppercase or lowercase. It is not case-sensitive.

2. Define the service name in Tomcat’s `server.xml` file by modifying the Oracle data source details in the file:

   ```
   url="jdbc:oracle:thin:@IP:PORT/service1"
   ```

3. Restart Tomcat.

4. Verify that the service name is included in the `catalina.out` log file.

5. Verify that the identity applications are properly connected to the database.
Manually Creating the Database Schema

When you install the identity applications, you can postpone connecting to the database or creating tables in the database. If you do not have permissions to the database, you might need to choose this option. The installation program creates a SQL file that you can use to create the database schema. You can also recreate the database tables after installation without having to reinstall. To do so, you delete the database for the identity applications and create a new database with the same name.

Using the SQL File to Generate the Database Schema

This section assumes that the installation program created a SQL file that you can execute to generate the database schema. If you do not have the SQL file, see “Manually Creating the SQL File to Generate the Database Schema” on page 95.

**NOTE:** Do not use SQL*Plus to execute the SQL file. The line lengths in the file exceed 4000 characters.

1. Stop the Application Server.
2. Login to the Database Server.
3. Delete the database that is used by the identity applications.
4. Create a new database with the same name as the one that was deleted in Step 3.
5. Navigate to the SQL script that the installation process created, by default in the /installation_path/userapp/sql directory.
6. (Conditional) For an Oracle database, insert a backslash (/) after the definition of the function CONCAT_BLOB. For example:

   ```sql
   -- Changeset icfg-data-load.xml::700::IDMRBPM
   CREATE OR REPLACE FUNCTION CONCAT_BLOB(A IN BLOB, B IN BLOB) RETURN BLOB AS
   C BLOB;
   BEGIN
       DBMS_LOB.CREATETEMPORARY(C, TRUE);
       DBMS_LOB.APPEND(C, A);
       DBMS_LOB.APPEND(C, B);
       RETURN C;
   END;
   /
   ```
7. Have the database administrator run the SQL script to create and configure the User Application database.
8. Restart Tomcat.
Manually Creating the SQL File to Generate the Database Schema

You can recreate the database tables after installation without having to reinstall and without having the SQL file. This section helps you create the database schema in the event that you do not have the SQL file.

1. Stop Tomcat.
2. Log in to the server that hosts your identity applications database.
3. Delete the existing database.
4. Create a new database with the same name as the one that you deleted in Step 3.
5. In a text editor, open the `NetIQ-Custom-Install.log` file, located by default at the root of the installation directory for the identity applications. For example:
   ```
   C:\NetIQ\idm\apps\UserApplication
   ``
6. Search and copy the below command from the `NetIQ-Custom-Install.log` file:
   ```
   C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m -Dwar.context.name=IDMProv
   -Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" -
   Duser.container="o=data" -jar C:\NetIQ\idm\jre\liquibase.jar --
   databaseClass=liquibase.database.core.PostgresDatabase --
   driver=org.postgresql.Driver --
   classpath=C:\NetIQ\idm\apps\postgresql\postgresql-9.4.1212jdbc42.jar
   C:\NetIQ\idm\apps\UserApplication\IDMProv.war --
   changeLogFile=DatabaseChangeLog.xml --url="jdbc:postgresql://
   localhost:5432/ idmuserappdb" --contexts="prov,newdb" --logLevel=info -
   --logFile=C:\NetIQ\idm\apps\UserApplication\db.out --username=******
   -- password=****** update
   
   C:\\NetIQ\\idm\\apps\\postgresql\\postgresql-9.4.1212jdbc42.jar
   ``
7. Log in to the server where you installed the database for the identity applications.
8. In a terminal, paste the command string that you copied.

   **NOTE:** The command should be `updateSQL`. If it is `update`, change the command to `updateSQL`.

9. In the command, replace the asterisks (*) that represent the database username and password with the actual values required to authenticate. Also, ensure the name of the SQL file is unique.
10. Execute the command.
11. (Conditional) If the process generates a SQL file instead of populating the database, provide the file to your database administrator to import into the database server. For more information, see “Using the SQL File to Generate the Database Schema” on page 94.
12. After the database administrator imports the SQL file, start Tomcat.

Configuring Single Sign-On Settings for the Identity Applications

The installation process installs an authentication service (OSP) for single sign-on access in Identity Manager. However, you can also configure the OSP authentication server to accept authentication from the Kerberos ticket server or SAML. To configure the single sign-on settings for the identity applications after installation, Configuring Single Sign-on Access in Identity Manager in the NetIQ Identity Manager - Administrator’s Guide to the Identity Applications.
Starting the Identity Applications

Ensure that you restart the Tomcat service and ActiveMQ service after you configure the identity applications.

```bash
systemctl restart netiq-tomcat
systemctl restart netiq-activemq
```

Configuration and Usage Considerations for the Identity Applications

The following considerations apply to the configurations and initial usage of the identity applications.

- During the installation process, the installation program writes log files to the installation directory. These files contain information about your configuration. After you configure your Identity Applications environment, you should consider deleting these log files or storing them in a secure location. During the installation process, you might choose to write the database schema to a file. Since this file contains descriptive information about your database, you should move the file to a secure location after the installation process is complete.

- (Conditional) To audit the identity applications, you must have Identity Reporting and an auditing service installed in your environment and configured to capture the events. You must also configure the identity applications for auditing.

- Before users can access the identity applications, you must complete the following activities:
  - Ensure that all necessary Identity Manager drivers are installed.
  - Enable cookies on all browsers. The applications do not work when cookies are disabled.
  - If you have installed Identity Applications and SSPR on different servers, then you must import the SSPR trusted certificate with the CN as Identity Applications to the cacerts of Identity Applications server.

Configuring the Runtime Environment for Data Collection

This section provides information about additional configuration steps you should perform to ensure that the runtime environment is operating correctly. It also provides troubleshooting techniques, as well as some information about database tables that are of particular interest.

This process includes the following activities:

- “Configuring the Data Collection Services Driver to Collect Data from the Identity Applications” on page 97
- “Migrating the Data Collection Service Driver” on page 98
- “Adding Support for Custom Attributes and Objects” on page 100
- “Adding Support for Multiple Driver Sets” on page 102
- “Configuring the Drivers to Run in Remote Mode with SSL” on page 104

If you have problems with one or more of the drivers that are difficult to understand, see “Troubleshooting the Drivers” in the NetIQ Identity Reporting Module Guide.
Configuring the Data Collection Services Driver to Collect Data from the Identity Applications

For the identity applications to function properly with Identity Reporting, you must configure the DCS driver to support the OAuth protocol.

**NOTE:**
- You only need to install and configure the DCS driver if you use Identity Reporting in your environment.
- If you have multiple DCS drivers configured in your environment, you must complete the following steps for each driver.

1. Log in to Designer.
2. Open your project in Designer.
3. (Conditional) If you have not already upgraded your DCS driver to the supported patch version, complete the following steps:
   3a. Download the latest DCS driver patch file.
   3b. Extract the patch file to a location on your server.
   3c. In a terminal, navigate to the location of the extracted patch RPM for your environment and run the following command:
      ```
      rpm -Uvh novell-DXMLdcs.rpm
      ```
   3d. Restart the Identity Vault.
   3e. In Designer, ensure that you have installed a supported version of the Data Collection Service Base package. If necessary, install the latest version before continuing.
   3f. Redeploy and restart the DCS driver in Designer.
4. In the **Outline** view, right-click the DCS driver, then select **Properties**.
5. Click **Driver Configuration**.
6. Click the **Driver Parameters** tab.
7. Click **Show connection parameters**, then select **show**.
8. Click **SSO Service Support**, then select **Yes**.
9. Specify the IP address and port for Identity Reporting.
10. Specify a password for the SSO Service Client. The default password is **driver**.
11. Click **Apply**, then click **OK**.
12. In the **Modeler** view, right-click the DCS driver, then select **Driver > Deploy**.
13. Click **Deploy**.
14. If prompted to restart the DCS driver, click **Yes**.
15. Click **OK**.
Migrating the Data Collection Service Driver

For the objects to synchronize into the Identity Information Warehouse, you must migrate the Data Collection Service driver.

1. Log in to iManager.
2. In the Overview panel for the Data Collection Service Driver, select Migrate From Identity Vault.
3. Select the organizations that contain relevant data, and click Start.

**NOTE:** Depending on the amount of data that you have, the migration process could take several minutes. Be sure to wait until the migration process is complete before you proceed.

4. Wait for the migration process to complete.
5. In the idmrpt_identity and idmrpt_acct tables, which provide information about the identities and accounts in the Identity Vault, ensure they contain the following type of information:

<table>
<thead>
<tr>
<th>ID</th>
<th>idmrpt_identity</th>
<th>idmrpt_acct</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>John Doe</td>
<td>Jane</td>
</tr>
<tr>
<td>2</td>
<td>David Smith</td>
<td>Sarah</td>
</tr>
<tr>
<td>3</td>
<td>Emily Johnson</td>
<td>Michael</td>
</tr>
<tr>
<td>4</td>
<td>Richard Brown</td>
<td>Elizabeth</td>
</tr>
</tbody>
</table>

6. In the LDAP browser, verify that the migration process adds the following references for DirXML-Associations:
   - For each user, verify the following type of information:
For each group, verify the following type of information:

- Ensure that the data in the `idmrpt_group` table appears similar to the following information:

<table>
<thead>
<tr>
<th>group_name</th>
<th>group_desc</th>
<th>character_var</th>
<th>boolean</th>
<th>dynamic_role</th>
<th>nested_group</th>
<th>idmrpt_valid_from</th>
<th>idmrpt_deleted</th>
<th>idmrpt_syn_state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pharmacy</td>
<td>Pharmacy</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>2016-08-07 21:20:11</td>
<td>FALSE</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>2016-08-07 21:20:11</td>
<td>FALSE</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>2016-08-07 21:20:11</td>
<td>FALSE</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Physician</td>
<td>Physician</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>2016-08-07 21:20:11</td>
<td>FALSE</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td>Operations</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>2016-08-07 21:20:11</td>
<td>FALSE</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Medical Ops</td>
<td>Medical Operations</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>2016-08-07 21:20:11</td>
<td>FALSE</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Nursing</td>
<td>Nursing</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>2016-08-07 21:20:11</td>
<td>FALSE</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

This table shows the name for each group, as well as flags indicating whether the group is dynamic or nested. It also shows whether the group has been migrated. The synchronization status (`idmrpt_syn_state`) could possibly be set to 0 if an object had been modified in the User Application but not yet migrated. For example, if a user were added to a group, and the driver had not been migrated yet, this value might be set to 0.

8 (Optional) Verify the data in the following tables:

- `idmrpt_approver`
- `idmrpt_association`
- `idmrpt_category`
- `idmrpt_container`
- `idmrpt_idv_drivers`
- `idmrpt_idv_prd`
- `idmrpt_role`
- `idmrpt_resource`
- `idmrpt_sod`

9 (Optional) Verify that the `idmrpt_ms_collect_state` table, which shows information about the data collection state for the Managed System Gateway Driver, contains now rows.

This table includes data about which REST endpoints for managed systems have been executed. At this point, the table has no rows because you have not started the collection process for this driver.
Adding Support for Custom Attributes and Objects

You can configure the Data Collection Service driver to gather and persist data for custom attributes and objects that are not part of the default data collection scheme. To do this, you need to modify the Data Collection Service driver filter. Modifying the filter does not trigger object synchronization immediately. Instead, the newly added attributes and objects are sent to the data collection services when add, modify, or delete events occur in the Identity Vault.

When you add support for custom attributes and objects, you need to modify the reports in order to include the extended attribute and object information. The following views provide current and historic data on the extended objects and attributes:

- idm_rpt_cfg.idmrpt_ext_idv_item_v
- idm_rpt_cfg.idmrpt_ext_item_attr_v

This process includes the following activities:

- “Configuring the Driver to Use Extended Objects” on page 100
- “Including a Name and Description in the Database” on page 101
- “Adding Extended Attributes to Known Object Types” on page 101

Configuring the Driver to Use Extended Objects

You can add any object or attribute to the Data Collection Service filter policy. When you add a new object or attribute, you need to make sure you map the GUID (with subscriber sync) and the Object Class (with subscriber notify), as shown in the following example:

```xml
<filter-class class-name="Device" publisher="ignore" publisher-create-homedir="true" publisher-track-template-member="false" subscriber="sync">
  <filter-attr attr-name="CN" merge-authority="default" publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
  <filter-attr attr-name="Description" merge-authority="default" publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
  <filter-attr attr-name="GUID" merge-authority="default" publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
  <filter-attr attr-name="Object Class" merge-authority="default" publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
  <filter-attr attr-name="Owner" merge-authority="default" publisher="ignore" publisher-optimize-modify="true" subscriber="notify"/>
  <filter-attr attr-name="Serial Number" merge-authority="default" publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
  <filter-attr attr-name="sampleDeviceModel" from-all-classes="true" merge-authority="default" publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
  <filter-attr attr-name="sampleDeviceType" from-all-classes="true" merge-authority="default" publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
</filter-class>
```
Including a Name and Description in the Database

If you want the object to have a name and description in the database, you need to add a schema mapping policy for _dcsName and _dcsDescription. The schema mapping policy maps the attribute values on the object instance to the columns idmrpt_ext_idv_item.item_name and idmrpt_ext_idv_item.item_desc, respectively. If you do not add a schema mapping policy, the attributes will be populated in the child table idmrpt_ext_item_attr.

For example:

```html
<attr-name class-name="Device">
    <nds-name>CN</nds-name>
    <app-name>_dcsName</app-name>
</attr-name>
<attr-name class-name="Device">
    <nds-name>Description</nds-name>
    <app-name>_dcsDescription</app-name>
</attr-name>
```

The following example of SQL allows you to show these object and attribute values in the database:

```sql
SELECT
    item.item_dn,
    item.item_name,
    item.item_desc,
    attr.attribute_name,
    itemAttr.attribute_value,
    item.idmrpt_deleted as item_deleted,
    itemAttr.idmrpt_deleted as attr_deleted,
    item.item_desc,
    obj.object_class
FROM
    idm_rpt_data.idmrpt_ext_idv_item as item,
    idm_rpt_data.idmrpt_ext_item_attr itemAttr, idm_rpt_data.idmrpt_ext_attr
    as attr, idm_rpt_data.idmrpt_ext_obj as obj
WHERE
    item.object_id = obj.object_id and itemAttr.attribute_id =
    attr.attribute_id and itemAttr.cat_item_id = item.item_id
ORDER BY
    item.item_dn, item.item_name
```

Adding Extended Attributes to Known Object Types

If an attribute is added to the filter policy on the Data Collection Service driver and not explicitly mapped to the reporting database in the XML reference file (IdmrptIdentity.xml), the value is populated and maintained in the idmrpt_ext_item_attr table, with an attribute reference in the idmrpt_ext_attr table.

The following example of SQL shows these extended attributes:
SELECT
  acct.idv_acct_dn,
  attrDef.attribute_name,
  attribute_value,
  attrVal.idmrpt_valid_from,
  cat_item_attr_id,
  attrVal.idmrpt_deleted,
  attrVal.idmrpt_syn_state
FROM
  idm_rpt_data.idmrpt_ext_item_attr as attrVal,
  idm_rpt_data.idmrpt_ext_attr as attrDef, idm_rpt_data.idmrpt_identity as idd, idm_rpt_data.idmrpt_idv_acct as acct
WHERE attrVal.attribute_id = attrDef.attribute_id and idd.identity_id = acct.identity_id and attrVal.cat_item_id = acct.identity_id and cat_item_type_id = 'IDENTITY'

In addition to the User object, you can add extended attributes to the filter policy on the following objects and populate the database with these attributes:

- nrfRole
- nrfResource
- Containers

**NOTE:** The installed product provides support for organizationUnit, Organization, and Domain. The container types are maintained in the idmrpt_container_types table.

- Group
- nrfSod

You can see the association of the extended attributes to the parent table or object by looking at the idmrpt_cat_item_types.idmrpt_table_name column. This column describes how to join the idm_rpt_data.idmrpt_ext_item_attr.cat_item_id column to the primary key of the parent table.

### Adding Support for Multiple Driver Sets

The Data Collection Service Scoping package (NOVLDCSSCPNG) provides static and dynamic scoping capabilities for enterprise environments with multiple driversets and multiple pairs of Data Collection Service Drivers and Managed System Gateway Drivers.

During or after installation, you need to determine the role for the Data Collection Service Driver that the package is being installed on. You need to select one of the following roles:

- **Primary** The driver synchronizes everything except subtrees of other driver sets. A primary Data Collection Service Driver may well service a whole Identity Vault or it may work in conjunction with one or multiple secondary drivers.

- **Secondary** The driver synchronizes only its own driver set, but nothing else. A secondary Data Collection Service Driver usually requires a primary driver to run in a different driverset or no data outside the local driver set is sent to the Data Collection Service.

- **Custom** Allows the administrator to define custom scoping rules. The only implicit scope is the local driver set, everything else is considered out-of-scope, unless it is explicitly added to the list of custom scopes. A custom scope is the distinguished name in slash format of a container in the Identity Vault whose subordinates or subtree should be synchronized.
The scoping package is only required in some configuration scenarios, as described below:

- **Single server with a single driver set Identity Vault:** For this scenario, you do not need scoping, and, therefore, you do not need to install the scoping package.

- **Multiple servers with a single driver set Identity Vault:** For this scenario, you need to follow these guidelines:
  - Make sure the Identity Manager server holds replicas of all partitions from which data should be collected.
  - For this scenario, no scoping is required, so do not install the scoping package

- **Multiple servers with a multiple driver set Identity Vault:** In this scenario, there are two basic configurations:
  - All servers hold a replica of all partitions from which data should be collected.
    For this configuration, you need to follow these guidelines:
    - Scoping is required to avoid the same change being processed by multiple DCS drivers.
    - You need to install the scoping package on all DCS drivers.
    - You need to select one DCS driver to be the Primary driver.
    - You need to configure all other DCS drivers to be Secondary drivers.
  
  - All servers do not hold a replica of all partitions from which data should be collected.
    Within this configuration, there are two possible situations:
    - All partitions from which data should be collected are being held by **only one** Identity Manager server
      In this case, you need to follow these guidelines:
      - Scoping is required to avoid the same change being processed by multiple DCS drivers.
      - You need to install the scoping package on all DCS drivers.
      - You need to configure all DCS drivers to be Primary drivers.
    
    - All partitions from which data should be collected are **not being held by only one** Identity Manager server (some partitions are held by more than one Identity Manager server).
      In this case, you need to follow these guidelines:
      - Scoping is required to avoid the same change being processed by multiple DCS drivers.
      - You need to install the scoping package on all DCS drivers.
      - You need to configure all DCS drivers to be Custom drivers.
      
      You need to define custom scoping rules for each driver and be sure not to create any overlapping scopes.
Configuring the Drivers to Run in Remote Mode with SSL

When running in remote mode, you can configure the Data Collection Service and Managed System Gateway drivers to use SSL. This section provides steps for configuring the drivers to run in remote mode with SSL.

To configure SSL using a Keystore for the Managed System Gateway Driver:

1. Create a server certificate in iManager.
   - 1a In the Roles and Tasks view, click NetIQ Certificate Server > Create Server Certificate.
   - 1b Browse to and select the server object where the Managed System Gateway Driver is installed.
   - 1c Specify a certificate nickname.
   - 1d Select Standard as the creation method, then click Next.
   - 1e Click Finish, then click Close.

2. Export the server certificate using iManager.
   - 2a In the Roles and Tasks view, click NetIQ Certificate Access > Server Certificates.
   - 2b Select the certificate created in Step 1 and click Export.
   - 2c In the Certificates menu, select the name of your certificate.
   - 2d Ensure that Export private key is checked.
   - 2e Enter a password and click Next.
   - 2f Click Save the exported certificate, and save the exported pfx certificate.

3. Import the pfx certificate exported in Step 2 into the java key-store.
   - 3a Use the keytool available with Java. You must use JDK 6 or later.
   - 3b Enter the following command at a command prompt:
     ```
     keytool -importkeystore -srckeystore pfx certificate -srcstoretype PKCS12 -destkeystore Keystore Name
     
     For example:
     ```
     keytool -importkeystore -srckeystore cert.pfx -srcstoretype PKCS12 -destkeystore msgw.jks
   - 3c Enter the password when prompted to do so.

4. Modify the Managed System Gateway Driver configuration to use the keystore using iManager.
   - 4a From Identity Manager Overview, click the driverset containing the Managed System Gateway Driver.
   - 4b Click on the driver state icon and select Edit properties > Driver configuration.
   - 4c Set Show Connection Parameters to true and set the Driver configuration mode to remote.
   - 4d Enter the complete path of the keystore file and the password.
   - 4e Save and restart the driver.
5 Modify the Data Collection Service Driver configuration to use the keystore using iManager.

5a From Identity Manager Overview, click the driverset containing the Managed System Gateway Driver.

5b Click on the driver state icon and select Edit properties > Driver configuration.

5c Under the Managed System Gateway Registration header, set Managed System Gateway Driver Configuration Mode to remote.

5d Enter the complete path of the keystore, password and the alias enter in Step 1c.

5e Save and restart the driver.

Configuring Identity Reporting

After installing Identity Reporting, you can still modify many of the installation properties. To make changes, run the configuration update utility (configupdate.sh) file.

If you change any setting for Identity Reporting with the configuration tool, you must restart Tomcat for the changes to take effect. However, you do not need to restart the server after making changes in the web user interface for Identity Reporting.

- “Manually Adding the DataSource in the Identity Data Collection Services Page” on page 105
- “Running Reports on an Oracle Database” on page 106
- “Manually Generating the Database Schema” on page 106
- “Deploying REST APIs for Identity Reporting” on page 109
- “Connecting to a Remote PostgreSQL Database” on page 109

Manually Adding the DataSource in the Identity Data Collection Services Page

1. Log in to Identity Reporting application.
2. Click Data Sources.
3. Click Add.
4. In the Add Data Source dialog box, click the Select from predefined list radio button.
5. Select IDMDCSDatasource.
6. Click Save.
Running Reports on an Oracle Database

Identity Reporting provides the ability to run reports against remote Oracle databases. Ensure that you have the ojdbc8.jar file on the server where you are running the Oracle Database.

Manually Generating the Database Schema

To manually generate the database schema after installation, perform one of the following procedures for your database:

- “Configuring Create_rpt_roles_and_schemas.sql Schema against PostgreSQL Database” on page 106
- “Configuring Create_rpt_roles_and_schemas.sql Schema against Oracle Database” on page 107
- “Configuring Create_rpt_roles_and_schemas.sql Schema against MS SQL Database” on page 108
- “Clearing the Database Checksums” on page 108

Configuring Create_rpt_roles_and_schemas.sql Schema against PostgreSQL Database

1. Add the required roles to the database using the `create_dcs_roles_and_schemas.sql` and `create_rpt_roles_and_schemas.sql` SQLs located in `C:\NetIQ\idm\apps\IdentityReporting\sql`.

2. Log in to PGAdmin as a postgres user.

3. Run the Query tool.

4. To create `Create_rpt_roles_and_schemas` and `Create_dcs_roles_and_schemas` procedures, copy the content from these SQLs to the Query tool and execute against the connected database.

5. To create `IDM_RPT_DATA`, `IDM_RPT_CFG`, and `IDMRPTUSER` roles, execute the following commands in the given order:

   ```sql
   Select CREATE_DCS_ROLES_AND_SCHEMAS('Set pwd for IDM_RPT_DATA', 'Set pwd for IDMRPTUSER');
   Select CREATE_RPT_ROLES_AND_SCHEMAS('Set pwd for IDM_RPT_CFG');
   ```

   For example, if the password for `IDM_RPT_DATA`, `IDMRPTUSER`, and `IDM_RPT_CFG` are `password`, `password1`, and `password2` respectively, then you must execute the following commands:

   ```sql
   Select CREATE_DCS_ROLES_AND_SCHEMAS('password', 'password1');
   Select CREATE_RPT_ROLES_AND_SCHEMAS('password2');
   ```

6. Copy the content of `get_formatted_user_dn.sql` from `C:\NetIQ\idm\apps\IdentityReporting\sql` to the Query tool and execute against the connected database.
NOTE: The get_formatted_user_dn.sql function must be added manually when you select database schema creation option as File. If you select the database schema creation option as Now or Startup, the installer will add this function to the database.

Configuring Create_rpt_roles_and_schemas.sql Schema against Oracle Database

1. Add the required roles to the database using create_dcs_roles_and_schemas-oracle.sql and create_rpt_roles_and_schemas-oracle.sql from C:\NetIQ\idm\apps\IdentityReporting\sql.

2. Log in to SQL Developer as a database admin user.

3. To create Create_rpt_roles_and_schemas and Create_dcs_roles_and_schemas procedures, copy the content from these SQLs to SQL Developer and execute against the connected database.

4. To create IDM_RPT_DATA, IDM_RPT_CFG, and IDMRPTUSER roles, execute the following commands in the given order:

   ```sql
   begin
   CREATE_DCS_ROLES_AND_SCHEMAS('Set pwd for IDM_RPT_DATA', 'Set pwd for IDMRPTUSER');
   end;

   begin
   CREATE_RPT_ROLES_AND_SCHEMAS('Set pwd for IDM_RPT_CFG');
   end;
   
   For example, if the password for IDM_RPT_DATA, IDMRPTUSER, and IDM_RPT_CFG are password, password1, and password2 respectively, then you must execute the following commands:

   ```sql
   begin
   CREATE_DCS_ROLES_AND_SCHEMAS('password', 'password1');
   end;

   begin
   CREATE_RPT_ROLES_AND_SCHEMAS('password2');
   end;
   
5. Copy the content of get_formatted_user_dn-oracle.sql to SQL Developer from C:\NetIQ\idm\apps\IdentityReporting\sql and execute against the connected database.

NOTE: The get_formatted_user_dn-oracle.sql function must be manually added to the database when you select database schema creation option as File. If you select the database schema creation option as Now or Startup, the installer will add this function to the database.
Configuring Create_rpt_roles_and_schemas.sql Schema against MS SQL Database

1. Execute delete_create_dcs_roles_and_schemas-mssql.sql and delete_get_formatted_user_dn-mssql.sql.

2. Add the required roles to the database using create_dcs_roles_and_schemas.mssql and create_rpt_roles_and_schemas.mssql from C:\NetIQ\idm\apps\IdentityReporting\sql.

3. Log in to SQL Developer as a database admin user.

4. To create Create_rpt_roles_and_schemas and Create_dcs_roles_and_schemas procedures, copy the content from create_dcs_roles_and_schemas.mssql and create_rpt_roles_and_schemas.mssql to SQL Developer and execute against the connected database.

5. To create IDM_RPT_DATA, IDM_RPT_CFG, and IDMRPTUSER roles, execute the following commands in the given order:
   
   ```
   execute CREATE_DCS_ROLES_AND_SCHEMAS '<Set pwd for IDM_RPT_DATA>', '<Set pwd for IDMRPTUSER>'
   execute CREATE_DCS_ROLES_AND_SCHEMAS '<Set pwd for IDM_RPT_DATA>', '<Set pwd for IDMRPTUSER>'
   ```

6. Copy the content of get_formatted_user_dn.sql to SQL Developer from C:\NetIQ\idm\apps\IdentityReporting\sql and execute against the connected database.

Clearing the Database Checksums

1. Locate the following .sql files in C:\NetIQ\idm\apps\IdentityReporting\sql.
   - DbUpdate-01-run-as-idm_rpt_cfg.sql
   - DbUpdate-02-run-as-idm_rpt_cfg.sql
   - DbUpdate-03-run-as-idm_rpt_data.sql
   - DbUpdate-04-run-as-idm_rpt_data.sql
   - DbUpdate-05-run-as-idm_rpt_data.sql
   - DbUpdate-06-run-as-idm_rpt_cfg.sql

2. Clear the database checksums
   
   2a. To run the clearchsum command with each .sql, append the following line at the beginning of each file:

   ```
   update DATABASECHANGELOG set MD5SUM = NULL;
   ```

   The modified content should look similar to the following:
Final Steps for Completing the Installation

2b Run each .sql with the corresponding user.

Commit the changes to the database.

Deploying REST APIs for Identity Reporting

Identity Reporting incorporates several REST APIs that enable different features within the reporting functionality. These REST API uses the OAuth2 protocol for authentication.

On Tomcat, the rptdoc war and the dcsdoc war are automatically deployed when Identity Reporting is installed.

Connecting to a Remote PostgreSQL Database

If your PostgreSQL database is installed on a separate server, you need to change the default settings in the postgresql.conf and pg_hba.conf files in the remote database.

1 Change the listening address in the postgresql.conf file.
   By default, PostgreSQL allows to listen for the localhost connection. It does not allow a remote TCP/IP connection. To allow a remote TCP/IP connection, add the following entry to the
   C:\NetIQ\IDM\apps\postgres\data\postgresql.conf file:
   
   listen_addresses = '*'
   
   If you have multiple interfaces on the server, you can specify a specific interface to be listened.

2 Add a client authentication entry to the pg_hba.conf file.
   By default, PostgreSQL accepts connections only from the localhost. It refuses remote connections. This is controlled by applying an access control rule that allows a user to log in from an IP address after providing a valid password (the md5 keyword). To accept a remote connection, add the following entry to the
   C:\NetIQ\IDM\apps\postgres\data\pg_hba.conf file.
   
   host all all 0.0.0.0/0 md5
   
   For example, 192.168.104.24/26 trust
   This works only for IPv4 addresses. For IPv6 addresses, add the following entry:
host all all ::0/0 md5

If you want to allow connection from multiple client computers on a specific network, specify
the network address in the CIDR-address format in this entry.

The pg_hba.conf file supports the following client authentication formats.

- local database user authentication-method [authentication-option]
- host database user CIDR-address authentication-method [authentication-option]
- hostssl database user CIDR-address authentication-method [authentication-option]
- hostnossl database user CIDR-address authentication-method [authentication-option]

Instead of CIDR-address format, you can specify the IP address and the network mask in
separate fields using the following format:

- host database user IP-address IP-mask authentication-method [authentication-option]
- hostssl database user IP-address IP-mask authentication-method [authentication-option]
- hostnossl database user IP-address IP-mask authentication-method [authentication-option]

3 Test the remote connection.
   3a Restart the remote PostgreSQL server.
   3b Log in to the server remotely using the username and password.

Activating Identity Manager

You do not need an activation code to install or initially run Identity Manager. However, without an
activation code, Identity Manager stops functioning 90 days after installation. You can activate
Identity Manager at any time during the 90 days or afterward. For more information, see Activating
Identity Manager in NetIQ Identity Manager Overview and Planning Guide.

Reviewing the Ports Used by Identity Manager Components

Identity Manager components use various ports for communicating with one another. The ports are
opened on the firewall by default. To review the ports used by Identity Manager components, see
Understanding Identity Manager Communication in NetIQ Identity Manager Security Guide.
kind: PersistentVolume
apiVersion: v1
metadata:
  name: task-pv-volume
labels:
  type: nfs
spec:
  storageClassName: manual
  capacity:
    storage: 3Gi
  accessModes:
  - ReadWriteMany
  hostPath:
    path: '/mnt'
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: task-pv-claim1
spec:
  storageClassName: manual
  accessModes:
  - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
---
apiVersion: v1
kind: Pod
metadata:
  labels:
    name: identity-engine
spec:
  nodeSelector:
    kubernetes.io/hostname:
  hostNetwork: true
  containers:
  - image: <image name>
    name: identity-engine-container
    resources:
      limits:
        cpu: "2"
        memory: 4Gi
      requests:
        cpu: "1"
        memory: 1Gi
    volumeMounts:
    - name: data
      mountPath: /config
    env:
    - name: UPGRADE_IDM
      value:
    - name: IS_ADVANCED_EDITION
value:
  - name: INSTALL_ENGINE
    value:
  - name: INSTALL_IDVAULT
    value:
  - name: IS_COMMON_PASSWORD
    value:
  - name: COMMON_PASSWORD
    value:
  - name: TREE_CONFIG
    value:
  - name: ID_VAULT_PASSWORD
    value:
  - name: ID_VAULT_EXISTING_SERVER
    value:
  - name: ID_VAULT_EXISTING_NCP_PORT
    value:
  - name: ID_VAULT_EXISTING_LDAPS_PORT
    value:
  - name: ID_VAULT_EXISTING_CONTEXTDN
    value:
  - name: ID_VAULT_TREENAME
    value:
  - name: ID_VAULT_ADMIN_LDAP
    value:
  - name: ID_VAULT_ADMIN
    value:
  - name: ID_VAULT_PASSWORD
    value:
  - name: ID_VAULT_VARDIR
    value:
  - name: ID_VAULT_DIB
    value: '
  - name: ID_VAULT_NCP_PORT
    value:
  - name: ID_VAULT_LDAP_PORT
    value:
  - name: ID_VAULT_LDAPS_PORT
    value:
  - name: ID_VAULT_HTTP_PORT
    value:
  - name: ID_VAULT_HTTPS_PORT
    value:
  - name: ID_VAULT_CONF
    value:
  - name: ID_VAULT_DRIVER_SET
    value:
  - name: ID_VAULT_DEPLOY_CTX
    value:
  - name: ID_VAULT_SERVER_CONTEXT
    value:

volumes:
  - name: data
    persistentVolumeClaim:
      claimName: task-pv-claim1
Installing Designer

This section guides you through the process of installing Designer for Identity Manager. By default, the installation program installs the components in C:\NetIQ.

**IMPORTANT:** Ensure that the directory name containing the Designer installation program does not include a space. For example, do not name it Designer Install. Instead, it can be DesignerInstall.

NetIQ recommends that you review the installation process before beginning. For more information, see Chapter 5, “Planning to Install Designer,” on page 115.
Planning to Install Designer

This section provides the prerequisites, considerations, and system setup needed to install Designer. First, consult the checklist to understand the installation process.

- “Checklist for Installing Designer” on page 115

Checklist for Installing Designer

Before beginning the installation, NetIQ recommends that you review the following steps:

<table>
<thead>
<tr>
<th>Checklist Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Review the planning information. For more information, see Part II, “Planning to Install Identity Manager,” on page 33.</td>
</tr>
<tr>
<td>2. Review the considerations for installing Designer to ensure that the computer meets the prerequisites.</td>
</tr>
<tr>
<td>3. To install Designer, see one of the following sections:</td>
</tr>
<tr>
<td>- “Running the Windows Executable File” on page 117</td>
</tr>
<tr>
<td>- “Using the Silent Installation Process” on page 117</td>
</tr>
<tr>
<td>4. Install the rest of the Identity Manager components.</td>
</tr>
<tr>
<td>5. (Optional) To start a project for your Identity Manager solution, see the NetIQ Designer for Identity Manager Administration Guide.</td>
</tr>
</tbody>
</table>
Installing Designer

You can install Identity Manager Designer using an executable file, binary file, or in text mode, depending on the target computer. You can also perform a silent installation.

Several components of Identity Manager require packages in Designer. When you install Designer, the installation program automatically adds several packages to your new project.

- “Running the Windows Executable File” on page 117
- “Using the Silent Installation Process” on page 117
- “Installing Designer in a Locale Other Than the System Locale” on page 118
- “Modifying an Installation Path that Includes a Space Character” on page 119

Running the Windows Executable File

1. Log in with an administrator account to the computer on which you want to install Designer.
2. Download the Identity_Manager_4.8_Designer_Windows.zip from the NetIQ Downloads Website.
3. Extract the Identity_Manager_4.8_Designer_Windows.zip file.
4. Navigate to the designer_install folder.
5. Run the install.exe file.
6. Follow the steps in the wizard until the installation process completes.

Using the Silent Installation Process

You can use scripts to silently install Designer without user interaction. The -i silent option uses default parameter values for the installation unless you edit the designerInstaller.properties file.

1. Log in with an administrator account to the computer where you want to install Designer.
2. Navigate to the directory containing the installation program.
3. (Optional) To configure the installation directory and the language for Designer, complete the following steps.
   3a. Open the designerInstaller.properties file, located by default in the Path_to_unzipped_Designer_file\designer_install directory.
   3b. In the properties file, modify the values for the following parameters:

   USER_INSTALL_DIR
   
   Specifies the path to the location where you want to install Designer. For example:
USER_INSTALL_DIR=C:\designer

If you specify a path that does not end with the designer directory, the Designer installation program automatically appends a designer directory.

SELECTED_DESIGNER_LOCALE

Specifies one of the following languages that you want Designer to launch after installation:

- zh_CN - Chinese Simplified
- zh_TW - Chinese Traditional
- nl - Dutch
- en - English
- fr - French
- de - German
- it - Italian
- ja - Japanese
- pt_BR - Portuguese Brazil
- es - Spanish

3c Save and close the properties file.

4 Run the following command from the directory of the properties file:

```
install -i silent -f designerInstaller.properties
```

Installing Designer in a Locale Other Than the System Locale

You can use additional prompts with the Windows executable file to install Designer in a language other than the system locale. Consider the following scenario: the system locale on your computer is set to German, but you want to install Designer in English.

To install:

1 Download and extract the Identity_Manager_4.8_Designer_Windows.zip file.
2 Navigate to the designer_install folder in your computer’s Downloads folder.
   For example, C:\Users\<username>\Downloads\Identity_Manager_4.8_Designer_Windows\designer_install
3 Open a command prompt and run the following command:

```
install.exe -i silent -l en_us
```

This command silently installs Designer in the English (United States) locale. For other locale designation supported by Designer, see Step 3b in the “Using the Silent Installation Process” on page 117.
Modifying an Installation Path that Includes a Space Character

You can install Designer to a location that includes spaces in the directory names. However, after you install Designer, you must modify the StartDesigner.bat and Designer.ini files to ensure that Designer functions properly. Manually replace the space with an escape character ("\”). For example:

Change

C:\designer installation

to

C:\designer\ installation
Installing Analyzer

This section guides you through the process of installing Analyzer for Identity Manager. Analyzer is a thick client component that you install on a workstation. You can use Analyzer to examine and clean the data in the connected systems that you want to add to your Identity Manager solution. By using Analyzer during the planning phase, you can see what changes need to be made and how best to make those changes.

By default, the installation program installs the components in C:\NetIQ\Analyzer.

NetIQ recommends that you review the installation process before beginning. For more information, see “Checklist for Installing Analyzer” on page 123.
Planning to Install Analyzer

This section provides guidance for preparing to install Analyzer for Identity Manager. NetIQ recommends that you review the installation process before beginning.

- “Checklist for Installing Analyzer” on page 123

Checklist for Installing Analyzer

Before beginning the installation process, NetIQ recommends that you review the following steps:

<table>
<thead>
<tr>
<th>Checklist Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Review the planning information. For more information, see Part II, “Planning to Install Identity Manager,” on page 33.</td>
</tr>
<tr>
<td>2. Review the considerations for installing Analyzer to ensure that the computer meets the prerequisites.</td>
</tr>
<tr>
<td>3. To install Analyzer, see the following sections:</td>
</tr>
<tr>
<td>- To use the installation wizard, see “Running the Windows Executable File” on page 125.</td>
</tr>
<tr>
<td>- For a silent installation, see “Using the Silent Installation Process” on page 125</td>
</tr>
<tr>
<td>4. To activate Analyzer, see Activating Analyzer in the NetIQ Identity Manager Overview and Planning Guide.</td>
</tr>
</tbody>
</table>
Installing Analyzer

This section guides you through the process of installing Analyzer and configuring your environment for Analyzer.

- “Running the Windows Executable File” on page 125
- “Using the Silent Installation Process” on page 125

Running the Windows Executable File

1. Log in with an administrator account to the computer on which you want to install Analyzer.
2. Download the Identity_Manager_4.8_Analyzer_Windows.zip from the NetIQ Downloads Website.
3. Extract the Identity_Manager_4.8_Analyzer_Windows.zip file.
4. Navigate to the analyzer_install folder.
5. Run the install.exe file.
6. Follow the steps in the wizard until the installation process completes.

Using the Silent Installation Process

You can use scripts to silently install Analyzer without user interaction. The -i silent option uses default parameter values for the installation unless you edit the analyzerInstaller.properties file.

1. Log in with an administrator account to the computer where you want to install Analyzer.
2. Navigate to the directory containing the installation program.
3. (Optional) To configure the installation directory and the language for Analyzer, complete the following steps.
   3a. Open the analyzerInstaller.properties file, located by default in the Path_to_unzipped_Analyzer_file\analyzerInstall directory.
   3b. In the properties file, modify the values for the following parameters:
      USER_INSTALL_DIR
      Specifies the path to the location where you want to install Analyzer. For example:

      USER_INSTALL_DIR=C:\analyzer

      If you specify a path that does not end with the analyzer directory, the Analyzer installation program automatically appends a analyzer directory.
**SELECTED_ANALYZER_LOCALE**

Specifies one of the following languages that you want Analyzer to launch after installation:

- `zh_CN` - Chinese Simplified
- `zh_TW` - Chinese Traditional
- `nl` - Dutch
- `en` - English
- `fr` - French
- `de` - German
- `it` - Italian
- `ja` - Japanese
- `pt_BR` - Portuguese Brazil
- `es` - Spanish

3c  Save and close the properties file.

4  Run the following command from the directory of the properties file:

    install -i silent -f analyzerInstaller.properties
9 Post-Installation Tasks

After Identity Manager installs, you should configure the drivers you installed to meet the policies and requirements defined by your business processes. You also need to configure Sentinel Log Management for IGA to gather audit events. Post-installation tasks typically include the following items:

- “Configuring a Connected System” on page 127
- “Creating and Configuring a Driver Set” on page 127
- “Creating a Driver” on page 130
- “Defining Policies” on page 130
- “Managing Driver Activities” on page 131
- “Activating Identity Manager” on page 131

Configuring a Connected System

Identity Manager enables applications, directories, and databases to share information. For driver-specific configuration instructions, see the Identity Manager Driver Documentation.

Creating and Configuring a Driver Set

A driver set is a container that holds Identity Manager drivers. Only one driver set can be associated with any server at a time. You can use the Designer tool to create a driver set. If a server is already associated to a driver set and then you assign the server to a new driver set, the server will be removed from the original driver set.

To support password synchronization to the Identity Vault, Identity Manager requires that driver sets have a password policy. You can use the Default Universal Password Policy package in Identity Manager or create a password policy based on your existing organizational requirement. However, the password policy must include the DirMXL-PasswordPolicy object. If the policy object does not exist in the Identity Vault, you can create the object.

- “Creating Driver Set” on page 128
- “Assigning the Default Password Policy to Driver Sets” on page 128
- “Creating the Password Policy Object in the Identity Vault” on page 128
- “Creating a Custom Password Policy” on page 129
- “Creating the Default Notification Collection Object in the Identity Vault” on page 129
Creating Driver Set

Designer for Identity Manager provides many settings to create and configure a driver set. These settings allow you to specify Global Configurations Values, driver set packages, driver set named passwords, log levels, trace levels, and Java Environment Parameters. For more information, see “Configuring Driver Sets” in the NetIQ Designer for Identity Manager Administration Guide.

Assigning the Default Password Policy to Driver Sets

You must assign the DirMXL-PasswordPolicy object to each driver set in the Identity Vault. The Identity Manager Default Universal Password Policy package includes this policy object. The default policy installs and assigns a universal password policy to control how the Identity Manager engine automatically generates random passwords for drivers. Alternatively, to use a custom password policy, you must create the password policy object and the policy. For more information, see “Creating the Password Policy Object in the Identity Vault” on page 128 and “Creating a Custom Password Policy” on page 129.

1. Open your project in Designer.
2. In the Outline pane, expand your project.
3. Expand Package Catalog > Common to verify whether the Default Universal Password Policy package exists.
4. (Conditional) If the password policy package is not already listed in Designer, complete the following steps:
   4a. Right-click Package Catalog.
   4b. Select Import Package.
   4c. Select Identity Manager Default Universal Password Policy, and then click OK.
      To ensure that the table displays all available packages, you might need to deselect Show Base Packages Only.
5. Select each driver set and assign the password policy.

Creating the Password Policy Object in the Identity Vault

If the DirMXL-PasswordPolicy object does not exist in the Identity Vault, you can use Designer or the ldapmodify utility to create the object. For more information about how to do this in Designer, see “Configuring Driver Sets” in NetIQ Designer for Identity Manager Administration Guide. To use the ldapmodify utility, use the following procedure:

1. In a text editor, create an LDAP Data Interchange Format (LDIF) file with the following attributes:
Creating a Custom Password Policy

Rather than using the default password policy in Identity Manager, you can create a new policy based on your organizational requirements. You can assign a password policy to the entire tree structure, a partition root container, a container, or a specific user. To simplify management, NetIQ recommends that you assign password policies as high in the tree as possible. For more information, see Creating Password Policies in the Password Management 3.3.2 Administration Guide.

Creating the Default Notification Collection Object in the Identity Vault

The Default Notification Collection is an Identity Vault object that contains a set of e-mail notification templates and an SMTP server that is used when sending e-mails generated from the templates. If the Default Notification Collection object does not exist in the Identity Vault, use Designer to create the object.

1. Open your project in Designer.
2. In the Outline pane, expand your project.
Right-click the Identity Vault, then click Identity Vault Properties.

Click Packages, then click the Add Packages icon.

Select all the notification templates packages, and then click OK.

Click Apply to install the packages with the Install operation.

Deploy the notification templates to the Identity Vault.

Creating a Driver

To create drivers, use the package management feature provided in Designer. For each Identity Manager driver you plan to use, create a driver object and import a driver configuration. The driver object contains configuration parameters and policies for that driver. As part of creating a driver object, install the driver packages and then modify the driver configuration to suit your environment.

The driver packages contain a default set of policies. These policies are intended to give you a good start as you implement your data sharing model. Most of the time, you will set up a driver using the shipping default configuration, and then modify the driver configuration according to the requirements of your environment. After you create and configure the driver, deploy it to the Identity Vault and start it. In general, the driver creation process involves the following actions:

1. Importing the Driver Packages
2. Installing the Driver Packages
3. Configuring the Driver Object
4. Deploying the Driver Object
5. Starting the Driver Object

For additional and driver-specific information, refer to the relevant driver implementation guide from the Identity Manager Drivers Web site.

Defining Policies

Policies enable you to customize the flow of information into and out of the Identity Vault, for a particular environment. For example, one company might use the inetorgperson as the main user class, and another company might use User. To handle this, a policy is created that tells the Identity Manager engine what a user is called in each system. Whenever operations affecting users are passed between connected systems, Identity Manager applies the policy that makes this change.

Policies also create new objects, update attribute values, make schema transformations, define matching criteria, maintain Identity Manager associations, and many other things.

NetIQ recommends that you use Designer to define policies for drivers to meet your business needs. For a detailed guide to Policies, see NetIQ Identity Manager - Using Designer to Create Policies guide and NetIQ Identity Manager Understanding Policies Guide. For information about the document type definitions (DTD) that Identity Manager uses, see Identity Manager DTD Reference. These resources contain:

- A detailed description of each available policy.
• An in-depth Policy Builder user guide and reference, including examples and syntax for each condition, action, noun, and verb.
• A discussion on creating policies using XSLT style sheets.

Managing Driver Activities

To perform administration and configuration functions of Identity Manager drivers, use Designer or iManager. These functions are described in detail in NetIQ Identity Manager Driver Administration Guide.

Activating Identity Manager

You do not need an activation code to install or initially run Identity Manager. However, without an activation code, Identity Manager stops functioning 90 days after installation. You can activate Identity Manager at any time during the 90 days or afterward. For more information, see Understanding Licensing and Activation in the NetIQ Identity Manager Overview and Planning Guide.
Upgrading Identity Manager

This section provides information for upgrading Identity Manager components. To migrate existing data to a new server, see Part VII, “Migrating Identity Manager Data to a New Installation,” on page 173. For more information about the difference between upgrade and migration, see “Understanding Upgrade and Migration” on page 137.
Preparing to Upgrade Identity Manager

This section provides information to help you prepare for upgrading your Identity Manager solution to the latest version. You can upgrade most components of Identity Manager using an executable file, binary file, or in text mode, depending on the target computer. To perform the upgrade, you must download and unzip or unpack the Identity Manager installation kit.

**WARNING:** You must always rely on Identity Manager patch channels to update the components that are installed with Identity Manager 4.8. Otherwise, you can encounter severe conflicts during regular Identity Manager patch updates

- “Checklist for Upgrading Identity Manager” on page 135
- “Understanding Upgrade and Migration” on page 137
- “Upgrade Order” on page 138
- “Supported Upgrade Paths” on page 138
- “Back Up the Current Configuration” on page 142

Checklist for Upgrading Identity Manager

To perform the upgrade, NetIQ recommends that you complete the steps in the following checklist:

<table>
<thead>
<tr>
<th>Checklist Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Review the differences between an upgrade and a migration. For more information, see “Understanding Upgrade and Migration” on page 137.</td>
</tr>
<tr>
<td>2. Upgrade to Identity Manager 4.6.4. You cannot upgrade or migrate to version 4.8 from versions before 4.6.4. For more information, see the NetIQ Identity Manager 4.5 Setup Guide.</td>
</tr>
<tr>
<td>3. Ensure that you have the latest installation kit to upgrade Identity Manager. For more information, see Where to Get Identity Manager in the NetIQ Identity Manager Overview and Planning Guide.</td>
</tr>
<tr>
<td>4. Ensure that your computers meet the hardware and software prerequisites for a newer version of Identity Manager.</td>
</tr>
<tr>
<td>5. Back up the current project, driver configuration, and databases. For more information, see “Backing Up the Current Configuration” on page 142.</td>
</tr>
<tr>
<td>6. Upgrade Designer to the latest version. For more information, see “Upgrading Designer” on page 145.</td>
</tr>
</tbody>
</table>
Preparing to Upgrade Identity Manager

<table>
<thead>
<tr>
<th>Checklist Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Install or upgrade iManager to the latest version for Identity Manager. For more information, see one of the following sections:</td>
</tr>
<tr>
<td>- <strong>Installation</strong>: “Installation Procedures” on page 45</td>
</tr>
<tr>
<td>- <strong>Upgrade</strong>: “Upgrading iManager” on page 150</td>
</tr>
<tr>
<td>8. On the server running Identity Manager, upgrade eDirectory to the latest version and patch.</td>
</tr>
<tr>
<td>9. Update the iManager plug-ins to match the version of iManager. For more information, see “Updating iManager Plug-ins after an Upgrade or Re-installation” on page 152.</td>
</tr>
<tr>
<td>10. Stop the drivers that are associated with the server where you installed the Identity Manager engine. For more information, see “Stopping and Starting Identity Manager Drivers” on page 162.</td>
</tr>
<tr>
<td>11. Upgrade the Identity Manager engine. For more information, see “Upgrading the Identity Manager Engine” on page 147.</td>
</tr>
<tr>
<td><strong>NOTE</strong>: If you are migrating the Identity Manager engine to a new server, you can use the same the eDirectory replicas that are on the current Identity Manager server. For more information, see “Migrating the Identity Manager Engine to a New Server” on page 180.</td>
</tr>
<tr>
<td>12. (Conditional) If any of the drivers in the driver set for the Identity Manager Engine are Remote Loader drivers, upgrade the Remote Loader servers for each driver. For more information, see “Upgrading the Remote Loader” on page 149.</td>
</tr>
<tr>
<td>13. (Conditional) If you are using packages, upgrade the packages on the existing drivers to get new policies. For more information, see “Upgrading the Identity Manager Drivers” on page 165. This is only required if a newer version of a package is available and there is a new functionality included in the policies for a driver that you want to add to your existing driver.</td>
</tr>
<tr>
<td>14. (Conditional) If SSPR is not installed, install SSPR. For more information, see “Installing SSPR” on page 50.</td>
</tr>
<tr>
<td>15. Upgrade the Identity Applications. For more information, see “Upgrading Identity Applications” on page 152.</td>
</tr>
<tr>
<td>16. Upgrade Identity Reporting. For more information, see “Upgrading Identity Reporting” on page 160.</td>
</tr>
<tr>
<td>17. Start the drivers associated with the Identity Applications and the Identity Manager engine. For more information, see “Stopping and Starting Identity Manager Drivers” on page 162.</td>
</tr>
<tr>
<td>18. (Conditional) If you migrated the Identity Manager engine or the identity applications to a new server, add the new server to the driver set. For more information, see “Adding New Servers to the Driver Set” on page 166.</td>
</tr>
<tr>
<td>19. (Conditional) If you have custom policies and rules, restore your customized settings. For more information, see “Restoring Custom Policies and Rules to the Driver” on page 168.</td>
</tr>
<tr>
<td>20. Activate your upgraded Identity Manager solution. For more information, see “Activating Identity Manager” on page 131.</td>
</tr>
</tbody>
</table>
Understanding Upgrade and Migration

When you want to install a newer version of an existing Identity Manager installation, you usually perform an upgrade. However, when the new version of Identity Manager does not provide an upgrade path from your existing version, you need to upgrade to a version from which upgrade to 4.8 is possible. Alternatively you can also do a migration to a new machine. NetIQ defines migration as the process for installing Identity Manager on a new server, then migrating the existing data to this new server.


Upgrade

In general, you can upgrade Identity Manager 4.7 Standard and Advanced Editions.

* **Identity Manager 4.7 Standard Edition:** If you currently have Identity Manager 4.7 Standard Edition, you can directly upgrade it to Identity Manager 4.8 Standard Edition. For more information, see Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.8 Standard Edition.

To upgrade Identity Manager 4.7 Standard Edition to Identity Manager 4.8 Advanced Edition, choose one of the following approaches to complete the upgrade:


* **Identity Manager 4.7 Advanced Edition:** If you currently have Identity Manager 4.7 Advanced Edition, you can directly upgrade it to Identity Manager 4.8 Advanced Edition. For more information, see “Checklist for Upgrading Identity Manager” on page 135.

When you upgrade Identity Manager 4.7.4 that has latest version of NICI to 4.8, the Upgrade.log displays exit code 1603 as the latest version of NICI is already installed. This code can be ignored.

Migration

In some cases you cannot perform a direct upgrade. In such scenarios, migration is preferred. For example, if you previously installed Identity Manager on a server running an operating system that is no longer supported, you must perform a migration instead of an upgrade.

If you have multiple servers associated with a driver set, you can perform an upgrade or a migration on one server at a time. If you do not have time to upgrade the servers at the same time, the drivers continue to work with the different versions of Identity Manager until the upgrades for each server can be completed.

**IMPORTANT:** If you enable features for drivers that are supported only on Identity Manager 4.8 or later, the drivers stop working on the servers with mixed versions. The older engines cannot handle the new functionality. This breaks the drivers until all servers are upgraded to Identity Manager 4.8 or later.
Preparing to Upgrade Identity Manager

Switch From Advanced Edition to Standard Edition

Identity Manager allows you to switch from Advanced Edition to Standard Edition during the product evaluation period or after activating Advanced Edition.


Upgrade Order

You must upgrade the Identity Manager components in the following sequence:

1. Designer
2. iManager
3. Sentinel Log Management for IGA (can be installed only on Linux computers)
4. Identity Vault
5. Identity Manager Engine
6. Remote Loader
7. iManager Plug-Ins
8. Identity Applications (for Advanced Edition)
9. Identity Reporting
10. Analyzer
11. Self Service Password Reset

Supported Upgrade Paths

Identity Manager 4.8 support upgrade from 4.7.x and 4.6.x versions. Before starting the upgrade, NetIQ recommends that you review the information from the release notes for your current version.

**NOTE:** Upgrading Identity Manager to 4.8 version requires you to apply the Identity Manager 4.8 Upgrade Enablement Patch. Conditions for applying this patch depends on your current version of Identity Manager. For more information, see NetIQ Identity Manager 4.8 Upgrade Enablement Patch Release Notes.

- “Upgrading from Identity Manager 4.7.x Versions” on page 138
- “Upgrading from Identity Manager 4.6.x Versions” on page 140

Upgrading from Identity Manager 4.7.x Versions

The following table lists the component-wise upgrade paths for Identity Manager 4.7.x versions:
<table>
<thead>
<tr>
<th>Component</th>
<th>Base Version</th>
<th>Upgraded Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Manager Engine</td>
<td>4.7.x</td>
<td>1. Upgrade the operating system to a supported version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Upgrade Identity Vault to 9.2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Upgrade Identity Manager Engine to 4.8.</td>
</tr>
<tr>
<td>Remote Loader/Fanout Agent</td>
<td>4.7.x</td>
<td>Install 4.8 Remote Loader/Fanout Agent</td>
</tr>
<tr>
<td>Designer</td>
<td>4.7.x</td>
<td>Install Designer 4.8.</td>
</tr>
<tr>
<td>Identity Applications</td>
<td>4.7.x</td>
<td>Before you upgrade Identity Applications, ensure that the Identity Vault and Identity Manager engine are upgraded to 9.2 and 4.8 respectively.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Upgrade the operating system to a supported version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Upgrade the database to a supported version. For the supported database versions, see the NetIQ Identity Manager Technical Information website (<a href="https://www.netiq.com/products/identity-manager/advanced/technical-information/">https://www.netiq.com/products/identity-manager/advanced/technical-information/</a>).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. (Conditional) If SSPR is installed on a separate server, upgrade the component to 4.8 version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Update the User Application driver and Roles and Resources driver packages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Upgrade Identity Applications to 4.8.</td>
</tr>
</tbody>
</table>
Before starting the upgrade, NetIQ recommends that you review the information from the release notes for your version from the Identity Manager documentation page.

### Upgrading from Identity Manager 4.6.x Versions

The following table lists component-wise upgrade paths for Identity Manager 4.6.x versions:

<table>
<thead>
<tr>
<th>Component</th>
<th>Base Version</th>
<th>Intermediate Step</th>
<th>Upgraded Version</th>
</tr>
</thead>
</table>
| Identity Reporting         | 4.7.x                         |                   | 1. Upgrade the operating system to a supported version.  
2. Upgrade the database to a supported version. For more information about the supported database versions, see the NetIQ Identity Manager Technical Information website.  
3. Upgrade SLM for IGA to a supported version (installation supported only on Linux computers).  
4. Update the Data Collection Services and Managed Services Gateway driver packages.  
5. Upgrade Identity Reporting 4.8.  
6. (Conditional) Create a data synchronization policy from the Identity Manager Data Collection Services page. |
| Remote Loader/Fanout Agent | 4.6.x, where x is 0 to 3      | Apply the 4.6.4 patch | Install 4.8 Remote Loader/Fanout Agent.                                                                                                                                 |
| Designer                   | 4.6.x, where x is 0 to 3      |                   | Install Designer 4.8.                                                                                                                                 |
Before starting the upgrade, NetIQ recommends that you review the information from the release notes for your version from the Identity Manager documentation page.

<table>
<thead>
<tr>
<th>Component</th>
<th>Base Version</th>
<th>Intermediate Step</th>
<th>Upgraded Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Applications</td>
<td>4.6.x, where x is 0 to 3</td>
<td>Apply the 4.6.4 patch</td>
<td>Before you upgrade Identity Applications, ensure that Identity Vault and Identity Manager engine are upgraded to 9.2 and 4.8 versions respectively.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. Upgrade the operating system to a supported version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Update the User Application driver and Roles and Resources driver packages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Upgrade the database to a supported version. For the supported database versions, see the NetIQ Identity Manager Technical Information website.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4. (Conditional) If SSPR is installed on a separate server, upgrade the component to 4.8 version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5. Upgrade Identity Applications to 4.8.</td>
</tr>
<tr>
<td>Identity Reporting</td>
<td>4.6.x, where x is 0 to 3</td>
<td>Apply the 4.6.4 patch</td>
<td>1. Upgrade the operating system to a supported version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Upgrade the database to a supported version. For more information about the supported database versions, see the NetIQ Identity Manager Technical Information website.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Upgrade SLM for IGA to a supported version (installation supported only on Linux computers).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4. Update the Data Collection Services and Managed Services Gateway driver packages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5. Migrate Identity Reporting to 4.8.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6. (Conditional) Create a data synchronization policy from the Identity Manager Data Collection Services page.</td>
</tr>
</tbody>
</table>
Preparing to Upgrade Identity Manager

Back Up the Current Configuration

Before upgrading, NetIQ recommends that you back up the current configuration of your Identity Manager solution. There are no additional steps required to back up the User Application. All User Application configuration is stored in the User Application driver. You can create the backup in the following ways:

- “Exporting the Designer Project” on page 142
- “Exporting the Configuration of the Drivers” on page 143

Exporting the Designer Project

A Designer project contains the schema and all driver configuration information. Creating a project of your Identity Manager solution allows you to export all of the drivers in one step instead of creating a separate export file for each driver.

- “Exporting the Current Project” on page 142
- “Creating a New Project from the Identity Vault” on page 142

Exporting the Current Project

If you already have a Designer project, verify that the information in the project is synchronized with what is in the Identity Vault:

1. In Designer, open your project.
2. In the Modeler, right-click the Identity Vault, then select Live > Compare.
3. Evaluate the project and reconcile any differences, then click OK.
   For more information, see “Using the Compare Feature When Deploying” in the NetIQ Designer for Identity Manager Administration Guide.
4. On the toolbar, select Project > Export.
5. Click Select All to select all resources to export.
6. Select where to save the project and in what format, then click Finish.
   Save the project in any location, other than the current workspace. When you upgrade to Designer, you must create a new workspace location. For more information, see “Exporting a Project” in the NetIQ Designer for Identity Manager Administration Guide.

Creating a New Project from the Identity Vault

If you do not have a Designer project of your current Identity Manager solution, you must create a project to back up your current solution.

1. Install Designer.
2. Launch Designer, then specify a location for your workspace.
3. Select whether you want to check for online updates, then click OK.
4. On the Welcome page, click Run Designer.
5. On the toolbar, select Project > Import Project > Identity Vault.
6 Specify a name for the project, then either use the default location for your project or select a different location.

7 Click Next.

8 Specify the following values for connecting to the Identity Vault:
   - **Host Name**, which represents the IP address or DNS name of the Identity Vault server
   - **User name**, which represents the DN of the user used to authenticate to the Identity Vault
   - **Password**, which represents the password of the authentication user

9 Click Next.

10 Leave the Identity Vault Schema and the Default Notification Collection selected.

11 Expand the Default Notification Collection, then deselect the languages you do not need.
   The Default Notification Collections are translated into many different languages. You can import all languages or select only the languages that you use.

12 Click Browse, then browse to and select a driver set to import.

13 Repeat Step 12 for each driver set in this Identity Vault, then click Finish.

14 Click OK after the project is imported.

15 If you only have one Identity Vault, you are finished. If you have multiple Identity Vaults, proceed with Step 16.

16 Click Live > Import on the toolbar.

17 Repeat Step 8 through Step 14 for each additional Identity Vault.

**Exporting the Configuration of the Drivers**

Creating an export of the drivers makes a backup of your current configuration. However, Designer currently does not create a backup of the Roles Based Entitlements driver and policies. Use iManager to verify that you have an export of the Roles Based Entitlement driver.

- “Using Designer to Export the Driver Configurations” on page 143
- “Using iManager to Create an Export of the Driver” on page 144

**Using Designer to Export the Driver Configurations**

1 Verify that your project in Designer has the most current version of your driver. For more information, see “Importing a Library, a Driver Set, or a Driver from the Identity Vault” in the NetIQ Designer for Identity Manager Administration Guide.

2 In the Modeler, right-click the line of the driver that you are upgrading.

3 Select Export to a Configuration File.

4 Browse to a location to save the configuration file, then click Save.

5 Click OK on the results page.

6 Repeat Step 1 through Step 5 for each driver.
Using iManager to Create an Export of the Driver

1. In iManager, select Identity Manager > Identity Manager Overview.
2. Browse to and select the location in the tree to search for Driver Set objects, then click the search icon.
3. Click the Driver Set object that holds the driver you want to upgrade.
4. Click the driver you want to upgrade, then click Export.
5. Click Next, then select Export all contained policies, linked to the configuration or not.
6. Click Next, then click Save As.
7. Select Save to Disk, then click OK.
8. Click Finish.
9. Repeat Step 1 through Step 8 for each driver.
Upgrading Identity Manager Components

This section provides specific information for upgrading individual components of Identity Manager. For example, you might want to upgrade Designer to the latest version without upgrading iManager. This section also provides steps that you might need to take after performing an upgrade.

- “Upgrading Designer” on page 145
- “Upgrading the Identity Manager Engine Components” on page 146
- “Upgrading Identity Applications” on page 152
- “Upgrading Identity Reporting” on page 160
- “Upgrading Analyzer” on page 162
- “Stopping and Starting Identity Manager Drivers” on page 162
- “Upgrading the Identity Manager Drivers” on page 165
- “Adding New Servers to the Driver Set” on page 166
- “Restoring Custom Policies and Rules to the Driver” on page 168

Upgrading Designer

1. Log in as an administrator to the server where Designer is installed.
2. To create a backup copy of your projects, export your projects.
   
   For more information about exporting, see “Exporting a Project” in the NetIQ Designer for Identity Manager Administration Guide.
3. Launch the Designer installation program from the Identity_Manager_4.8_Designer_Windows.zip file. (<Designer zip extracted location>\designer_install\install.exe)
4. Select the language to install Designer in, then read and accept the license agreement.
5. Specify the directory where Designer is installed, then click Yes in the message stating you already have Designer installed.
6. Select whether the shortcuts should be placed on your desktop and in your desktop menu.
7. Review the summary, then click Install.
8. Review the Release Notes, then click Next.
9. Select to launch Designer, then click Done.
10. Specify a location for your Designer workspace, then click OK.
11. Click OK in the warning message stating that your project needs to be closed and converted.
12. In the Project view, expand the project, then double-click Project needs conversion.
13. Review the steps that the Project Converter Wizard performs, then click Next.
14. Specify a name for the backup of your project, then click Next.
After upgrading to the current version of Designer, you must import all Designer projects from the older version. When you initiate the import process, Designer runs the Project Converter Wizard, which converts the older projects to the current version. In the wizard, select Copy project into the workspace. For more information about the Project Converter, see the NetIQ Designer for Identity Manager Administration Guide.

Upgrading the Identity Manager Engine Components

Ensure that you upgrade Identity Vault before upgrading the Identity Manager engine. The Identity Manager engine upgrade process updates the driver shim files that are stored in the file system on the host computer.

Upgrading the Identity Vault

1 Download the Identity_Manager_4.8_Windows.iso as instructed in Where to Get Identity Manager in the NetIQ Identity Manager Overview and Planning Guide.
2 Mount the downloaded .iso.
3 Navigate to the $iso mounted location$/IdentityManagerServer/products/eDirectory/x64 directory.
4 Run the eDirectory_920_Windows_x86_x64.exe file.
5 In the Basic tab, specify the following details:
   - If you select New Tree, specify the following details:
     - Tree Name: Specify a tree name for Identity Vault.
     - Server FDN: Specify a server FDN.
   - If you select Existing Tree, specify the following details:
     - IP Address: Specify the IP address of the of the existing tree for Identity Vault.
     - Port Number: Specify the port number for the existing tree. The default value is 524.
     - Server FDN: Specify a server FDN.
     - Tree Admin: Specify the existing administrator name for Identity Vault.
     - Admin Password: Specify the administrator password.
6 (Conditional) In the Advanced tab, specify the following details:
NOTE: NetIQ recommends that you enable this option. To enable IPv6 addressing after installation, you must run the setup program again.

- To enable Enhanced Background Authentication (EBA), select Enable EBA.
- Specify the HTTP clear text and secure ports. The default values are 8028 and 8030 respectively.
- Specify the LDAP clear text and secure ports. The default values are 389 and 636 respectively.

7 In the Install Location field, specify the location where Identity Vault is installed.
8 In the DIB Location field, specify the location where the DIB files are located.
9 Click Upgrade and proceed with the upgrade process.

Upgrading the Identity Manager Engine

Verify that the drivers are stopped. For more information, see “Stopping the Drivers” on page 162.

Perform the following steps to upgrade the Identity Manager Engine:

1 Download the Identity_Manager_4.8_Windows.iso from the NetIQ Downloads website.
2 Mount the downloaded .iso.
3 Navigate to the <ISO installed location>\IdentityManagerServer folder and run the install.exe.
4 Select the language that you want to use for the installation and click OK.
5 In the Introduction page, click Next.
6 Read and accept the license agreement and then click Next.
   The installed components and their versions are displayed.
7 Select Identity Manager Engine and click Next.
8 Specify the configuration settings for Identity Manager Engine. For more information, see “Configuration Worksheet for Identity Manager Engine” on page 51.
9 In the pre-upgrade summary page, review the settings and click Upgrade.

Working with MapDB 3.0.5

The addition to Identity Manager Engine, MapDB is used by the following Identity Manager drivers:

- Data Collection Services
- JDBC
- LDAP
- Managed System Gateway
- Office 365 and Azure Active Directory
- Salesforce
If you are using any of these drivers, you must review the following sections before upgrading the driver:

- “Understanding Identity Manager 4.8 Engine Support for Driver Versions” on page 148
- “Manually Removing the MapDB Cache Files” on page 148

**Understanding Identity Manager 4.8 Engine Support for Driver Versions**

Review the following considerations before upgrading an Identity Manager driver that uses MapDB:

- Drivers shipped with Identity Manager 4.8 are compatible with Identity Manager 4.8 Engine or Remote Loader. You must follow the driver upgrade steps from the specific driver implementation guide.
- Drivers shipped before Identity Manager 4.8 are not compatible with Identity Manager 4.8 Engine or Remote Loader.
- Drivers shipped with Identity Manager 4.8 are not backward compatible with Identity Manager 4.7.x Engine or Remote Loader.
- Drivers shipped with Identity Manager 4.8 are not backward compatible with Identity Manager 4.6.x Engine or Remote Loader.

**Manually Removing the MapDB Cache Files**

The Identity Manager Engine upgrade process leaves some of the existing MapDB cache files (dx*) in the Identity Vault’s DIB directory. You must manually remove these files for your driver after upgrading the driver. This action ensures that your driver works correctly with Identity Manager 4.8 engine.

The following table lists the MapDB cache files that must be removed:

<table>
<thead>
<tr>
<th>Identity Manager Driver</th>
<th>MapDB State Cache File To Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Collection Services</td>
<td>DCSDriver_&lt;driver instance guid&gt;*</td>
</tr>
<tr>
<td></td>
<td>&lt;driver instance guid&gt;*</td>
</tr>
<tr>
<td>JDBC</td>
<td>jdbc_&lt;driver instance guid&gt;_*</td>
</tr>
<tr>
<td>LDAP</td>
<td>ldap_&lt;driver instance guid&gt;*</td>
</tr>
<tr>
<td>Managed System Gateway</td>
<td>MSGW-&lt;driver-instance-guid&gt;*</td>
</tr>
<tr>
<td>Office 365 and Azure Active Directory</td>
<td>&lt;Azure driver name&gt;_obj.db.*</td>
</tr>
<tr>
<td>Salesforce</td>
<td>&lt;Salesforce driver name&gt;*</td>
</tr>
</tbody>
</table>

where * represents the name of the MapDB state cache file. In case of a Salesforce driver, the MapDB state cache files are also represented by the driver name. Below are some examples of these files.

- DCSDriver_<driver instance guid>-0.t,<driver instance guid>-1.p
- jdbc_<driver instance guid>_0.t,jdbc_<driver instance guid>_1
Upgrading Identity Manager Components

- ldap_<driver instance guid>b, ldap_<driver instance guid>b.p
- MSGW-<driver instance guid>.p, MSGW-<driver instance guid>.t
- <Azure driver name>_obj.db.t, <Azure driver name>_obj.db.p
- <Salesforce driver name>.p, <Salesforce driver name>.t, Salesforce
driver1

Upgrading the Remote Loader

If you are running the Remote Loader, you need to upgrade the Remote Loader files.

**NOTE:** Before upgrading .NET Remote Loader, ensure that you have successfully installed all the Windows updates on your system.

1. Create a backup of the Remote Loader configuration files. The default location of the files is C:\...\RemoteLoader\remoteloadername-config.txt.
2. Verify that the drivers are stopped. For instructions, see Stopping, Starting, or Restarting a Driver in Designer in the NetIQ Identity Manager Driver Administration Guide.
3. Stop the Remote Loader service or daemon for each driver.
   In the Remote Loader Console, select the Remote Loader instance, then click Stop.
4. Stop the lcache process using Windows Task Manager.
5. Download the Identity_Manager_4.8_Windows.iso from the NetIQ Downloads website.
6. Mount the downloaded .iso.
7. Navigate to the <ISO installed location>\IdentityManagerServer folder and run the install.exe.
8. Select the language that you want to use for the installation and click OK.
9. In the Introduction page, click Next.
10. Read and accept the license agreement and then click Next.
    The installed components and their versions are displayed.
11. Select Remote Loader Service and click Next.
12. In the pre-upgrade summary page, click Upgrade.
13. After the upgrade is complete, verify that your configuration files contain your environment’s information.
14. (Conditional) If there is a problem with the configuration file, copy the backup file that you created in step 1. Otherwise, continue with the next step.
15. Start the Remote Loader service or daemon for each driver.

**IMPORTANT:** If your driver uses MapDB, manually remove the existing MapDB state cache files for the driver after upgrading the driver. This is required because Identity Manager engine upgrade process does not remove all of these files from the Identity Vault’s DIB directory. For more information, see “Working with MapDB 3.0.5” on page 147.
Upgrading the Java Remote Loader

1. Create a backup of the Remote Loader configuration files. The default location of the files is C:\....\RemoteLoader\remoteloadername-config.txt.

2. Verify that the drivers are stopped. For instructions, see Stopping, Starting, or Restarting a Driver in Designer in the NetIQ Identity Manager Driver Administration Guide.

3. Stop the Remote Loader service or daemon for each driver.

   In the Remote Loader Console, select the Remote Loader instance, then click Stop.

4. Stop the lcachе process using Windows Task Manager.

5. Download the Identity_Manager_4.8_Windows.iso from the NetIQ Downloads website.

6. Mount the downloaded .iso.

7. Navigate to the <ISO installed location>\IdentityManagerServer\products\IDM\java_remoteloader folder.

8. Copy and replace the dirxml_jremote_dev.tar.gz file in your existing Java Remote Loader installed directory.

9. Based on the file present in your existing setup, copy and replace one of the following files in your existing Java Remote Loader installed directory:
   - dirxml_jremote.tar.gz
   - dirxml_jremote_mvs.tar

10. Extract the files that you have copied in step 8 and step 9.

    Use the 7-zip or supported software to unzip the .tar.gz file.

11. (Conditional) If there is a problem with the configuration file, copy the backup file that you created in step 1. Otherwise, continue with the next step.

    NOTE: Use the version.txt file to ensure that you have the latest version of Java Remote Loader.

12. Start the Remote Loader service or daemon for each driver.

Upgrading iManager

The upgrade process for iManager uses the existing configuration values in the configiman.properties file, such as port values and authorized users. Before upgrading iManager to the 3.2 version, NetIQ recommends that you:

- Upgrade eDirectory to the 9.2 version.
- Back up the server.xml and context.xml configuration files.

The upgrade process includes the following activities:

- “Upgrading iManager” on page 151
- “Updating Role-Based Services” on page 151
- “Re-installing or Migrating Plug-ins for Plug-in Studio” on page 152
- “Updating iManager Plug-ins after an Upgrade or Re-installation” on page 152
Upgrading iManager

Before upgrading iManager, ensure that the computer meets the prerequisites and system requirements.

NOTE: The upgrade process uses the HTTP port and SSL port values that were configured in the previous version of iManager.

1. Download the Identity_Manager_4.8_Windows.iso from the NetIQ Downloads website.
2. Mount the downloaded .iso.
3. Navigate to the <ISO installed location>\IdentityManagerServer folder and run the install.exe.
4. Select the language that you want to use for the installation and click OK.
5. In the Introduction page, click Next.
6. Read and accept the license agreement and then click Next.
   The installed components and their versions are displayed.
7. Select iManager Web Administration and click Next.
8. Specify the settings for iManager. For more information, see “Configuration Worksheet for Identity Manager Engine” on page 51.
9. In the pre-upgrade summary page, review the settings and click Upgrade.

Updating Role-Based Services

NetIQ recommends that you update your RBS modules to the latest version so that you can see and use all of the available functionality in iManager.

NOTE: • When updating or re-installing iManager, the installation program does not update existing plug-ins. To update plug-ins manually, launch iManager and navigate to Configure > Plug-in Installation > Available Novell Plug-in Modules.
   • Different installations of iManager might have a different number of plug-ins locally installed. As a result, you might see discrepancies in the module report for any given collection from the Role Based Services > RBS Configuration page. For the numbers to match between iManager installations, ensure that you install the same subset of plug-ins on each iManager instance in the tree.

To check for and update outdated RBS objects:

1. Log in to iManager.
2. In the Configure view, select Role Based Services > RBS Configuration.
   Review the table in the 2.x Collections tabbed page for any out-of-date modules.
3. To update a module, complete the following steps:
   3a For the Collection that you want to update, select the number in the Out-Of-Date column.
      iManager displays the list of outdated modules.
Re-installing or Migrating Plug-ins for Plug-in Studio

You can migrate or replicate Plug-in Studio plug-ins to another iManager instance, as well as to a new or updated version of iManager.

1 Log in to iManager.
2 In the iManager Configure view, select Role Based Services > Plug-in Studio.
   The Content frame displays the Installed Custom Plug-ins list, including the location of the RBS collection to which the plug-ins belong.
3 Select the plug-in that you want to re-install or migrate, then click Edit.
   **NOTE:** You can edit only one plug-in at a time.
4 Click Install.
5 Repeat these steps for every plug-in that you need to re-install or migrate.

Updating iManager Plug-ins after an Upgrade or Re-installation

When you upgrade or re-install your iManager, the installation process does not update the existing plug-ins. Ensure that the plug-ins match the correct iManager version.

**NOTE:** This is the only method for updating Identity Manager plug-ins from iManager on Open Enterprise Server 2018.

1 Open iManager.
2 Navigate to Configure > Plug-in Installation > Available Novell Plug-in Modules.
3 Update the plug-ins.

Upgrading Identity Applications

This section provides information about upgrading Identity Applications and supporting software, which includes updating the following components:

- Identity Manager User Application
- One SSO Provider (OSP)
- Self-Service Password Reset (SSPR)
- Tomcat, JDK, and ActiveMQ

After the upgrade, the components are upgraded to the following versions:

- Tomcat – 8.5.40
- ActiveMQ – 5.15.9
- Java 8 Update 222
Upgrading Identity Manager Components

- One SSO Provider – 6.3.4
- Self-Service Password Reset – 4.4.0.3
- Identity Applications – 4.8
- Identity Reporting – 6.5

This section provides information about the following topics:

- “Understanding the Upgrade Program” on page 153
- “Prerequisite for Upgrade” on page 153
- “System Requirements” on page 154
- “Upgrading the PostgreSQL Database” on page 154
- “Upgrading the Driver Packages for Identity Applications” on page 156
- “Upgrading Identity Applications” on page 156
- “Post-Upgrade Tasks” on page 157

**Understanding the Upgrade Program**

The upgrade process reads the configuration values from the existing components. This information includes `ism-configuration.properties`, `server.xml`, `SSPRConfiguration.xml` and other configuration files. Using these configuration files the upgrade process internally invokes the upgrade program for the components. In addition, this program also creates a backup of the current installation.

**Prerequisite for Upgrade**

If your database is configured over SSL, replace `ssl=true` with `sslmode=requite` in the `server.xml` file from PATH located at `C:\NetIQ\idm\apps\tomcat\conf`.

For example, change

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb?ssl=true
```

to

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb?sslmode=requite
```
Upgrading Identity Manager Components

System Requirements

The upgrade process creates a back-up of the current configuration for the installed components. Ensure that your server has sufficient space to store the back-up and additional free space available for upgrade.

Upgrading the PostgreSQL Database

**IMPORTANT:** The upgrade process may take time depending on the size of the database. Therefore, plan your upgrade accordingly.

1. Stop the PostgreSQL service that is running on your server.
2. Rename the `postgres` directory from `C:\Netiq\idm\apps`. For example, rename `postgres` to `postgresql_old`.
3. Remove the old service by executing the following command:
   ```
   sc delete <postgres service name>
   ```
4. Install PostgreSQL version supported on your operating system.
   You must choose a location other than the current installation location of PostgreSQL.
   4a. Mount the `Identity_Manager_4.8_Windows.iso` image file and navigate to the `\common\postgres_tomcat` directory.
   4b. Run the `TomcatPostgreSQL.exe` file.
      Select only PostgreSQL option during installation.

**NOTE:**
- Do not provide any database details in PostgreSQL details page. Ensure that Create database login account and Create empty database are deselected.
- Ensure that you have the Administrator privileges for the old and new PostgreSQL installation directories.

5. Stop the newly installed PostgreSQL service. Go to Services, search for `<PostgreSQL version number>` service, and stop the service.

**NOTE:** Appropriate users can perform stop operations after providing valid authentication.

6. Change the permissions for the newly installed PostgreSQL directory by performing the following actions:
   Create a postgres user:
   2. Click Add a user account.
   3. In the Add a User page, specify `postgres` as the user name and provide a password for the user.
   Provide permissions to `postgres` user to the existing and newly installed PostgreSQL directories:
   1. Right click the PostgreSQL directory and go to Properties > Security > Edit.
2. Select **Full Control** for the user to provide complete permissions.
3. Click **Apply**.

7 **Access the PostgreSQL directory as postgres user.**
   1. Log in to the server as postgres user.
      Before logging in, make sure that postgres can connect to the Windows server by verifying if a remote connection is allowed for this user.
   2. Delete the data directory from the new postgres install location. For example,
      C:\NetIQ\idm\apps\postgres\data
   3. Open a command prompt and set **PGPASSWORD** by using the following command:
      ```
      set PGPASSWORD=<your pg password>
      ```
   4. Change to the newly installed PostgreSQL directory.
   5. Execute `initdb` as postgres database user.
      ```
      initdb.exe -D <new_data_directory> -E UTF8 -U postgres
      ```
      For example,
      ```
      initdb.exe -D C:\NetIQ\idm\apps\postgres\data -E UTF8 -U postgres
      ```
8 **Upgrade PostgreSQL from new PostgreSQL bin directory. Run the following command and click Enter.**
   ```
   pg_upgrade.exe --old-datadir "C:\NetIQ\idm\apps\postgres\data" --new-datadir "C:\NetIQ\idm\apps\postgresql962\data" --old-bindir "C:\NetIQ\idm\apps\postgres\bin" --new-bindir "C:\NetIQ\idm\apps\postgresql962\bin"
   ```
   9 After successful upgrade, replace **pg_hba.conf** and **postgresql.conf** files located in the new postgres data directory (C:\NetIQ\idm\apps\postgres\data) with the files from the old postgres directory.
10 Start the upgraded PostgreSQL database service.
   Go to Services, search for `<PostgreSQL version number>` service, and start the service.

   **NOTE:** Appropriate users can perform start operations after providing valid authentication.
11 Disable the old PostgreSQL service to ensure that the service does not automatically start.
12 **(Optional) Delete the old data files from the bin directory of the newly installed PostgreSQL service.**
   1. Login as postgres user.
   2. Navigate to the bin directory and run `analyze_new_cluster.bat` and `delete_old_cluster.bat` files.
      For example: C:\NetIQ\idm\apps\postgresql\bin

   **NOTE:** You must run this step only if you want to delete the old data files.
Upgrading the Driver Packages for Identity Applications

You must stop Tomcat and update the packages for the User Application Driver and Role and Resource Service drivers to the latest version. For information about upgrading packages to the latest version, see Upgrading Installed Packages of the NetIQ Designer for Identity Manager Administration Guide.

After upgrading the User Application driver packages, you must manually add the workflow templates package:

1. In Designer, navigate to the User Application driver > Properties.
2. Click Packages, then click the .
3. Select the Create Workflow Templates.
4. Click OK and then click Finish to complete the installation.
5. Deploy the User Application driver.

**IMPORTANT:** If any Email notifications template is installed or upgraded as part of User Application Driver upgrade, then you need to deploy Default Notification Collection object.

Upgrading Identity Applications

The following procedure describes how to upgrade the following components:

- Identity Applications
- OSP
- Tomcat
- PostgreSQL
- SSPR (if installed on the same computer as Identity Applications)
- ActiveMQ

Perform the following steps to upgrade Identity Applications:

1. Download the Identity_Manager_4.8_Windows.iso from the NetIQ Downloads website.
2. Mount the downloaded .iso.
3. Navigate to the <ISO installed location>\IdentityApplications folder and run the install.exe.
4. Select the language that you want to use for the installation and click OK.
5. In the Introduction page, click Next.
6. Read and accept the license agreement and then click Next.
   The installed components and their versions are displayed.
7. Select Identity Applications and click Next.
8. Specify the configuration settings for Identity Applications. For more information, see “Configuration Worksheet for Identity Applications” on page 53.
NOTE: NetIQ recommends you to create the Workflow database using the Identity Manager installer, if you have installed the PostgreSQL database on the same server as Identity Applications.

- While Upgrading, you must manually specify the database JDBC JAR file. For example, if you are using PostgresQL database, you need to specify the location of the database JAR file which is located outside the tomcat\lib folder.

In the pre-upgrade summary page, review the settings and click Upgrade.

Depending on where you installed the components, the process creates the backup directory in that location and appends a time stamp (indicating the time of backup) to the backed-up directory.

For example,

- **Tomcat** - C:\NetIQ\idm\apps\tomcat_backup_02262018_033634
- **OSP and SSPR** - C:\NetIQ\idm\apps\osp_sspr_backup_02262018_033634
- **ActiveMQ** - C:\NetIQ\idm\apps\activemq_backup_02262018_033634
- **User Application** - C:\NetIQ\idm\apps\UserApplication_backup_02262018_033634
- **Identity Reporting** - C:\NetIQ\idm\apps\IdentityReporting_backup_02262018_033634

### Post-Upgrade Tasks

If you have Identity Applications and SSPR on different servers, then you must import the SSPR trusted certificate with the CN as Identity Applications to the cacerts of Identity Applications server.

You must also restore the customized settings for Tomcat, SSPR, OSP, or Identity Applications, manually.

Perform the post-upgrade steps for the required components:

- “Java” on page 157
- “Tomcat” on page 158
- “Identity Applications” on page 159
- “One SSO Provider” on page 159
- “Self-Service Password Reset” on page 159
- “Kerberos” on page 160

### Java

Verify the certificates in newly upgrade JRE location: jre\lib\security\cacerts with your older JRE location. Manually import the missed certificates into your cacerts.

1. Import java cacerts using keytool command:

   ```
   keytool -import -trustcacerts -file Certificate_Path -alias ALIAS_NAME -keystore cacerts
   ```
NOTE: After upgrade, JRE is stored in the identity applications install location. For example: C:\NetIQ\idm\apps\jre

2 Restart the Identity Vault.
3 Verify JRE home location is tomcat\bin\setenv.bat.
4 Launch Configuration Update utility and verify the path of your cacerts.

Tomcat

1 (Conditional) To restore the customized files from the backup taken earlier by the upgrade process, perform the following tasks:

- Restore customized https certificates. To restore these certificates, copy the Java Secure Socket Extension (JSSE) contents from the backed up server.xml to the new server.xml file in the \tomcat\conf directory.
- Do not copy the configuration files from the backed-up Tomcat directory to the new Tomcat directory. Start with the default configuration of the new version and make changes as needed. For more information, see this Apache Website.

Verify that new server.xml file has the following entries

```xml
<Connector port="8543" protocol="HTTP/1.1"
  maxThreads="150" SSLEnabled="true" scheme="https"
  secure="true"
  clientAuth="false" sslProtocol="TLS"
  keystoreFile="path_to_keystore_file"
  keystorePass="keystore_password" />
<!--
  <Cluster
    className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
-->

or

```xml
<Connector port="8543"
  maxThreads="150" SSLEnabled="true" scheme="https"
  secure="true"
  clientAuth="false" sslProtocol="TLS"
  keystoreFile="path_to_keystore_file"
  keystorePass="keystore_password" />
<!--
  <Cluster
    className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
-->
```

NOTE: On a cluster environment, manually uncomment the Cluster tag in server.xml and copy osp.jks on to all nodes from the first node located at C:\netiq\idm\apps\osp_backup_<date>.

- If you have customized keystore files, include the correct path in the new server.xml file.
- Import identity applications certificates into the Identity Vault at C:\NetIQ\eDirectory\jre\lib\security\cacerts.
For example, you can use the following keytool command to import certificates into Identity Vault:

```
keytool -importkeystore -alias <User Application certificate alias> -srckeystore <backup cacert> -srcstorepass changeit -destkeystore C:\NetIQ\eDirectory\jre\lib\security\cacerts
```

2 (Conditional) Navigate to the User Application and restore the customized settings manually by reading the backed-up configuration.

**Identity Applications**

While upgrading Identity Applications from 4.6 SP4 to 4.8, you must ensure that `Dcom.novell.afw.wf.engine-id=IDMProv` parameter is present in the `setenv` file inside `tomcat/bin` folder. In case this parameter is missing after upgrading Identity Applications, you must manually add the parameter in the `setenv` file and restart the Tomcat server.

**One SSO Provider**

By default, the `LogHost` entry located in the `logevent.conf` file is set to `localhost`. To modify the `LogHost` entry, manually restore the customized OSP configurations from the backup taken during the upgrade process.

**Self-Service Password Reset**

After upgrading SSPR, update SSO client parameter using Configuration Update Utility. For more information, see “SSO Clients Parameters” on page 88.

To update the SSPR configuration details, perform the following steps:

1 Log in to SSPR portal as an administrator.

2 Update the audit server details:

   2a Navigate to YourID > Configuration Editor, specify the configuration password.
   2b Select Settings > Auditing > Audit Forwarding > Syslog Audit Server Certificates.
   2c Import these certificates from the server and click Save.

3 Import the LocalDB into SSPR:

   3a Navigate to YourID > Configuration Manager from the drop-down menu.
   3b Click LocalDB.
   3c Click Import (Upload) LocalDB Archive File.

4 (Conditional) To restrict configuration for SSPR:

   4a Navigate to YourID > Configuration Manager from the list.
   4b Click Restrict Configuration.

5 Configure administrator permissions for SSPR, see “Post-Installation Steps” on page 58.

To verify that the upgrade is successful, launch the upgraded components.

For example, launch the Identity Manager Dashboard, click About. Check whether the application displays the new version, such as 4.8.0.
Kerberos

The upgrade utility creates a new Tomcat folder on your computer. If any of the Kerberos files such as keytab and Kerberos_login.config resided in the old Tomcat folder, copy these files to the new Tomcat folder from backed-up folder.

Upgrading Identity Reporting

Identity Reporting includes two drivers. Also, you might need to migrate content from NetIQ Event Auditing Service to Sentinel Log Management for IGA. Perform the upgrade in the following order:

1. Upgrade Sentinel Log Management for IGA. For more information, see Upgrading Sentinel Log Management for IGA in the NetIQ Identity Manager Setup Guide for Linux.
2. Upgrade Identity Reporting.

Prerequisite for Upgrade

If your database is configured over SSL, replace ssl=true with sslmode=require in the server.xml file from PATH located at C:\NetIQ\idm\apps\tomcat\conf.

For example, change

jdbc:postgresql://<postgres db>:5432/idmrptdb?ssl=true

to

jdbc:postgresql://<postgres db>:5432/idmrptdb?sslmode=require

Upgrading Identity Reporting

Before upgrading Identity Reporting, you must upgrade the identity applications and SLM for IGA. To upgrade Identity Reporting, install the new version on top of the older version.

Perform the following steps to upgrade Identity Reporting:

1. Download the Identity_Manager_4.8_Windows.iso from the NetIQ Downloads website.
2. Mount the downloaded .iso.
3. Navigate to the <ISO installed location>\IdentityReporting folder and run the install.exe.
4. Select the language that you want to use for the installation and click OK.
5. In the Introduction page, click Next.
6. Read and accept the license agreement and then click Next. The installed components and their versions are displayed.
7. Select Identity Reporting and click Next.
8. Specify the configuration settings for Identity Reporting. For more information, see “Configuration Worksheet for Identity Reporting” on page 55.
9. In the pre-upgrade summary page, review the settings and click Upgrade.
NOTE: The com.netiq.rpt.ssl-keystore.type property in ism-configuration.properties file will retain the value (JKS/PKCS12) that was set prior to upgrade.

Post-upgrade Steps for Reporting

After upgrading Identity Reporting to 4.8, navigate to the ism-configuration.properties file located at /opt/netiq/idm/apps/tomcat/conf/ directory and perform the following actions:

- Change the value of the com.netiq.rpt.landing.url property as follows:
  com.netiq.rpt.landing.url = ${com.netiq.idm.osp.url.host}/idmdash/#/landing

- Change the value of the com.netiq.idmdcs.landing.url property as follows:
  com.netiq.idmdcs.landing.url = ${com.netiq.idm.osp.url.host}/idmdash/#/landing

- Specify the value for the com.netiq.rpt.redirect.url property in the following format:
  For example, com.netiq.rpt.redirect.url = https://192.168.0.1:8543/IDMRPT/oauth.html

Changing the References to reportRunner in the Database

After upgrading Identity Reporting and before starting Tomcat for the first time, ensure that you update the references to reportRunner from the database.

1. Stop Tomcat.
2. Navigate to the Identity Reporting installation directory and rename the reportContent folder to ORG-reportContent.
   For example: C:\NetIQ\idm\apps\IdentityReporting
3. Clean the temporary and work directories under the Tomcat folder.
4. Log in to the PostgreSQL database.
   4a. Locate the reportRunner references in the following tables:
      * idm_rpt_cfg.idmrpt_rpt_params
      * idm_rpt_cfg.idmrpt_definition
   4b. Issue the following delete statements:
      
      ```
      DELETE FROM idm_rpt_cfg.idmrpt_rpt_params WHERE rpt_def_id='com.novell.content.reportRunner';
      ```
      
      ```
      DELETE FROM idm_rpt_cfg.idmrpt_definition WHERE def_id='com.novell.content.reportRunner';
      ```
5. Start Tomcat.
   Check the logs to see if the reports are regenerated with the correct reportRunner.
6. Log into Identity Reporting and run the reports.
Verifying the Upgrade for Identity Reporting

1. Launch Identity Reporting.
2. Verify that old and new reports are being displayed in the tool.
3. Look at the Calendar to see whether your scheduled reports appear.
4. Ensure that the Settings page displays your previous settings for managed and unmanaged applications.
5. Verify that all other settings look correct.
6. Verify whether the application lists your completed reports.

Upgrading Analyzer

To upgrade Analyzer, NetIQ provides patch files in .zip format. Before upgrading Analyzer, ensure that the computer meets the prerequisites and system requirements. For more information, see the Release Notes accompanying the update.

1. Download the patch file, such as Identity_Manager_4.8_Analyzer_Windows, from the NetIQ download website.
2. Extract the .zip file to the directory that contains the Analyzer installation files, such as the plug-ins, uninstallation script, and other Analyzer files.
3. Restart Analyzer.
4. To verify that you successfully applied the new patch, complete the following steps:
   4a. Launch Analyzer.
   4b. Click Help > About Analyzer.
   4c. Check whether the program displays the new version, such as 4.6 Update 1 and Build ID 20121128.

Stopping and Starting Identity Manager Drivers

You might need to start or stop the Identity Manager drivers to ensure that an upgrade or installation process can modify or replace the correct files. This section explains the following activities:

- “Stopping the Drivers” on page 162
- “Starting the Drivers” on page 163

Stopping the Drivers

Before you modify any files for a driver, it is important to stop the drivers.

- “Using Designer to Stop the Drivers” on page 163
- “Using iManager to Stop the Drivers” on page 163
Using Designer to Stop the Drivers

1. In Designer, select the Identity Vault object in the Outline tab.
2. In the Modeler toolbar, click the Stop All Drivers icon. This stops all drivers that are part of the project.
3. Set the drivers to manual start to ensure that the drivers do not start until the upgrade process is complete:
   3a. Double-click the driver icon in the Outline tab.
   3b. Select Driver Configuration > Startup Options.
   3c. Select Manual, then click OK.
   3d. Repeat Step 3a through Step 3c for each driver.

Using iManager to Stop the Drivers

1. In iManager, select Identity Manager > Identity Manager Overview.
2. Browse to and select the location in the tree to search for Driver Set objects, then click the search icon.
3. Click the Driver Set object.
4. Click Drivers > Stop all drivers.
5. Repeat Step 2 through Step 4 for each Driver Set object.
6. Set the drivers to manual start to ensure that the drivers do not start until the upgrade process is complete:
   6a. In iManager, select Identity Manager > Identity Manager Overview.
   6b. Browse to and select the location in the tree to search for Driver Set objects, then click the search icon.
   6c. Click the Driver Set object.
   6d. In the upper right corner of the driver icon, click Edit properties.
   6e. On the Driver Configuration page under Startup Options, select Manual, then click OK.
   6f. Repeat Step 6a through Step 6e for each driver in your tree.

Starting the Drivers

After all of the Identity Manager components are updated, restart the drivers. NetIQ recommends that you test the drivers after they are running to verify that all of the policies still work.

- “Using Designer to Start the Drivers” on page 163
- “Using iManager to Start the Drivers” on page 164

Using Designer to Start the Drivers

1. In Designer, select the Identity Vault object in the Outline tab.
2. Click the Start All Drivers icon in the Modeler toolbar. This starts all of the drivers in the project.
3 Set the driver startup options:
   3a Double-click the driver icon in the Outline tab.
   3b Select Driver Configuration > Startup Option.
   3c Select Auto start or select your preferred method of starting the driver, then click OK.
   3d Repeat Step 3a through Step 3c for each driver.

4 Test the drivers to verify the policies are working as designed. For information on how to test your policies, see “Testing Policies with the Policy Simulator” in NetIQ Identity Manager - Using Designer to Create Policies.

Using iManager to Start the Drivers

1 In iManager, select Identity Manager > Identity Manager Overview.
2 Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
3 Click the Driver Set object.
4 Click Drivers > Start all drivers to start all of the drivers at the same time.
   or
   In the upper right corner of the driver icon, click Start driver to start each driver individually.
5 If you have multiple drivers, repeat Step 2 through Step 4.
6 Set the driver startup options:
   6a In iManager, select Identity Manager > Identity Manager Overview.
   6b Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
   6c Click the Driver Set object.
   6d In the upper right corner of the driver icon, click Edit properties.
   6e On the Driver Configuration page, under Startup Options, select Auto start or select your preferred method of starting the driver, then click OK.
   6f Repeat Step 6b through Step 6e for each driver.
7 Test the drivers to verify the policies are working as designed.
   There is no policy simulator in iManager. To test the policies, cause events to happen that make the policies execute. For example, create a user, modify a user, or delete a user.
Upgrading the Identity Manager Drivers

NetIQ delivers new driver content through packages instead of through driver configuration files. You manage, maintain, and create packages in Designer. Although iManager is package-aware, Designer does not maintain any changes to driver content that you make in iManager. For more information about managing packages, see “Understanding Packages” in the NetIQ Designer for Identity Manager Administration Guide.

You can upgrade your drivers to packages in the following ways:

- “Creating a New Driver” on page 165
- “Replacing Existing Content with Content from Packages” on page 165
- “Keeping the Current Content and Adding New Content with Packages” on page 166

**IMPORTANT:** If your driver uses MapDB, manually remove the existing MapDB state cache files for the driver after upgrading the driver. This is required because Identity Manager engine upgrade process does not clean all of these files. For more information, see “Working with MapDB 3.0.5” on page 147.

Creating a New Driver

The simplest and cleanest way to upgrade drivers to packages is to delete your existing driver and create a new driver with packages. Add all the functionality you want in the new driver. The steps are different for each driver. For instructions, see the individual driver guides on the Identity Manager Drivers documentation website. The driver now functions as before, but with content from packages instead of from a driver configuration file.

Replacing Existing Content with Content from Packages

If you need to keep the associations created by the driver, you do not need to delete and re-create the driver. You can keep the associations and replace the driver content with packages.

To replace the existing content with content from packages:

1. Create a backup of the driver and all of the customized content in the driver.
   
   For instructions, see “Exporting the Configuration of the Drivers” on page 143.

2. In Designer, delete all objects stored inside of the driver. Delete the policies, filters, entitlements, and all other items stored inside of the driver.

   **NOTE:** Designer provides the auto-import facility for importing the latest packages. You do not need to manually import the driver packages into the package catalog.

   For more information, see “Importing Packages into the Package Catalog” in the NetIQ Designer for Identity Manager Administration Guide.

3. Install the latest packages to the driver.

---

Upgrading Identity Manager Components 165
These steps are specific for each driver. For instructions, see each driver guide at the Identity Manager Drivers documentation website.

4 Restore any custom policies and rules to the driver. For instructions, see “Restoring Custom Policies and Rules to the Driver” on page 168.

**Keeping the Current Content and Adding New Content with Packages**

You can keep the driver as it currently is and add new functionality to the driver through packages, as long as the functionality in packages does not overlap the current functionality of the driver.

Before you install a package, create a backup of the driver configuration file. When you install a package, it can overwrite existing policies, which might cause the driver to stop working. If a policy is overwritten, you can import the backup driver configuration file and recreate the policy.

Before you begin, make sure that any customized policies have different policy names than the default policies. When a driver configuration is overlaid with a new driver file, the existing policies are overwritten. If your custom policies do not have a unique name, you will lose them.

To add new content to the driver with packages:

1 Create a backup of the driver and all of the customized content in the driver.
   For instructions, see “Exporting the Configuration of the Drivers” on page 143.

```NOTE: Designer provides the auto-import facility for importing the latest packages. You do not need to manually import the driver packages into the package catalog.
For more information, see “Importing Packages into the Package Catalog” in the NetIQ Designer for Identity Manager Administration Guide.
```

2 Install the packages on the driver.
   For instructions, see each driver guide at the Identity Manager Drivers documentation website.

3 Add the desired packages to the driver. These steps are specific for each driver.
   For more information, see the Identity Manager Drivers documentation website.

The driver contains the new functionality added by the packages.

**Adding New Servers to the Driver Set**

When you upgrade or migrate Identity Manager to new servers, you must update the driver set information. This section guides you through the process. You can use Designer or iManager to update the driver set.
Adding the New Server to the Driver Set

If you are using iManager, you must add the new server to the driver set. Designer contains a Migration Wizard for the server that does this step for you. If you are using Designer, skip to “Copying the Server-specific Information in Designer” on page 179. If you are using iManager, complete the following procedure:

1. In iManager, click the Identity Manager Administration page.
2. Click Identity Manager Overview.
3. Browse to and select the container that holds the driver set.
4. Click the driver set name to access the Driver Set Overview page.
5. Click Servers > Add Server.
6. Browse to and select the new Identity Manager server, then click OK.

Removing the Old Server from the Driver Set

After the new server is running all of the drivers, you can remove the old server from the driver set.

- “Using Designer to Remove the Old Server from the Driver Set” on page 167
- “Using iManager to Remove the Old Server from the Driver Set” on page 167
- “Decommissioning the Old Server” on page 168

Using Designer to Remove the Old Server from the Driver Set

1. In Designer, open your project.
2. In the Modeler, right-click the driver set, then select Properties.
3. Select Server List.
4. Select the old Identity Manager server in the Selected Servers list, then click the < to remove the server from the Selected Servers list.
5. Click OK to save the changes.
6. Deploy the change to the Identity Vault.
   
   For more information, see “Deploying a Driver Set to an Identity Vault” in the NetIQ Designer for Identity Manager Administration Guide.

Using iManager to Remove the Old Server from the Driver Set

1. In iManager, click the Identity Manager Administration page.
2. Click Identity Manager Overview.
3. Browse to and select the container that holds the driver set.
4. Click the driver set name to access the Driver Set Overview page.
5. Click Servers > Remove Server.
6. Select the old Identity Manager server, then click OK.
Decommissioning the Old Server

At this point, the old server is not hosting any drivers. If you no longer need this server, you must complete additional steps to decommission it:

1. Remove the eDirectory replicas from this server.
   For more information, see “Deleting Replicas” in the NetIQ eDirectory Administration Guide.
2. Remove eDirectory from this server.
   For more information, see TID 10056593, “Removing a Server From an NDS Tree Permanently”.

Restoring Custom Policies and Rules to the Driver

After installing or upgrading to new packages for your drivers, you must restore any custom policies or rules to the driver after you overlay the new driver configuration file. If these policies have different names, they are still stored in the driver, but the links are broken and need to be reestablished.

- “Using Designer to Restore Custom Policies and Rules to the Driver” on page 168
- “Using iManager to Restore Custom Policies and Rules to the Driver” on page 169

Using Designer to Restore Custom Policies and Rules to the Driver

You can add policies into the policy set. You should perform these steps in a test environment before you move the upgraded driver to your production environment.

1. In the Outline view, select the upgraded driver, then click the Show Policy Flow icon.
2. Right-click the policy set where you need to restore the customized policy to the driver, then select Add Policy > Copy Existing.
3. Browse to and select the customized policy, then click OK.
4. Specify the name of the customized policy, then click OK.
5. Click Yes in the file conflict message to save your project.
6. After the Policy Builder opens the policy, verify that the information is correct in the copied policy.
7. Repeat Step 2 through Step 6 for each customized policy you need to restore to the driver.
8. Start the driver and test the driver.
   For more information on starting the driver, see Stopping, Starting, or Restarting a Driver in Designer in the NetIQ Identity Manager Driver Administration Guide. For more information on testing the driver, see “Testing Policies with the Policy Simulator” in NetIQ Identity Manager - Using Designer to Create Policies.
9. After you verify that the policies work, move the driver to the production environment.
Using iManager to Restore Custom Policies and Rules to the Driver

Perform these steps in a test environment before you move the upgraded driver to your production environment.

1. In iManager, select Identity Manager > Identity Manager Overview.
2. Browse to and select the location in the tree to search for Driver Set objects, then click the search icon.
3. Click the Driver Set object that contains the upgraded driver.
4. Click the driver icon, then select the policy set where you need to restore the customized policy.
5. Click Insert.
6. Select Use an existing policy, then browse to and select the custom policy.
7. Click OK, then click Close.
8. Repeat Step 3 through Step 7 for each custom policy you need to restore to the driver.
9. Start the driver and test the driver.
   For information on starting the driver, see Stopping, Starting, or Restarting a Driver in Designer in the NetIQ Identity Manager Driver Administration Guide. There is no policy simulator in iManager. To test the policies, cause events to happen that make the policies execute. For example, create a user, modify a user, or delete a user.
10. After you verify that the policies work, move the driver to the production environment.
12 Switching from Advanced Edition to Standard Edition

You should switch to Standard Edition only if you do not want any Advanced Edition functionality in your environment and want to scale down your Identity Manager deployment.

1. (Conditional) If you have already applied the Advanced Edition activation, remove the activation.

2. (Conditional) To switch to the Standard Edition evaluation mode, perform the following actions:
   2a. Navigate to the Identity Vault dib directory in C:\Novell\NDS\DIBFiles.
   2b. Create a new file, name it .idme, and add 2 (numeric) to the file.
   2c. Restart eDirectory.
   2d. Continue with Step 4.

3. (Conditional) If you have already purchased a Standard Edition activation, apply the activation.

4. Stop Tomcat.

5. Remove the following WAR files and Webapps folder from the C:\NetIQ\idm\apps\tomcat\webapps directory:
   - IDMProv*
   - IDMRPT*
   - dash*
   - idmdash*
   - landing*
   - rra*
   - rptdoc*

6. Move the following existing folders to a backup directory:
   - IDMReporting
   - UserApplication

7. Copy the ism-configuration.properties file from C:\NetIQ\IDM\apps\tomcat\conf directory to a backup directory.

8. Install Identity Reporting from the Identity Manager 4.8 iso file.

9. Start configupdate.bat from the <reporting install folder>/bin directory and specify values for the following parameters:
   Reporting tab: Specify the settings in the following sections:
   - ID Vault
   - Identity Vault User Identity
Switching from Advanced Edition to Standard Edition

- Report Administrators
  - Report Admin Role Container DN. For example, ou=sa,o=data
  - Report Administrators. For example, cn=uaadmin, ou=sa, o=data

Authentication tab: Specify the settings in the following sections:

- Authentication Server
  - OAuth server host identifier. For example, IP address or DNS name of the authentication server such as 192.99.17.22
  - OAuth server TCP port
  - OAuth server is using TLS/SSL

- Authentication Configuration
  - OAuth keystore file. For example, C:\NetIQ\idm\apps\osp\osp.jks
  - Key alias of key for use by OAuth
  - Key password of key for use by OAuth
  - Session Timeout (minutes). For example, 60 minutes.

SSO Clients tab: Specify the settings in the following sections:

- Reporting
  - URL link to landing page. For example, http://192.168.0.1:8180/IDMRPT

- Self Service Password Reset
  - OAuth client ID. For example, sspr
  - OAuth client secret For example, <sspr client secret>
  - OSP OAuth redirect url. For example, http://192.168.0.2:8180/sspr/public/oauth

For more information about Configuration Utility, see “Running the Identity Applications Configuration Utility” on page 71.

10 Save the changes and exit the Configuration Utility.

11 Start Tomcat.
Migrating Identity Manager Data to a New Installation

This section provides information on migrating existing data in Identity Manager components to a new installation. Most migration tasks apply to the Identity Applications. To upgrade Identity Manager components, see Part VI, “Upgrading Identity Manager,” on page 133. For more information about the difference between upgrade and migration, see “Understanding Upgrade and Migration” on page 137.
Preparing to Migrate Identity Manager

This section provides information to help you prepare for migrating your Identity Manager solution to the new installation.

Checklist for Performing a Migration

To perform a migration, NetIQ recommends that you complete the steps in the following checklist.

<table>
<thead>
<tr>
<th>Checklist Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Ensure that you have the latest installation kit to migrate your Identity Manager data.</td>
</tr>
<tr>
<td>2. Ensure that your computers meet the hardware and software prerequisites for a newer version of Identity Manager.</td>
</tr>
<tr>
<td>3. Upgrade Identity Vault to the latest supported version.</td>
</tr>
<tr>
<td>4. Add the eDirectory replicas that are on the current Identity Manager server to the new server. For more information, see Section 14, “Migrating Identity Manager to a New Server,” on page 177.</td>
</tr>
<tr>
<td>5. Install Identity Manager on the new server. For more information, see “Planning to Install Identity Manager” on page 33.</td>
</tr>
<tr>
<td>6. (Conditional) If any of the drivers in the driver set are Remote Loader drivers, upgrade the Remote Loader server for each driver. For more information, see “Upgrading the Remote Loader” on page 149.</td>
</tr>
<tr>
<td>7. (Conditional) If you are running the User Application on your old server, update the component and its drivers. For more information, see “Checklist for Migrating Identity Manager” on page 177.</td>
</tr>
<tr>
<td>8. Add the new server to the driver set. For more information, see “Adding the New Server to the Driver Set” on page 167.</td>
</tr>
<tr>
<td>9. Change the server-specific information for each driver. For more information, see “Copying the Server-specific Information in Designer” on page 179.</td>
</tr>
<tr>
<td>10. (Conditional) If you have RBPM, update the server-specific information from the old server to the new server for the User Application. For more information, see “Copying Server-specific Information for the Driver Set” on page 179.</td>
</tr>
<tr>
<td>11. Update your drivers to the package format. For more information, see “Upgrading the Identity Manager Drivers” on page 165.</td>
</tr>
<tr>
<td>12. (Conditional) If you have custom policies and rules, restore your customize settings. For more information, see “Restoring Custom Policies and Rules to the Driver” on page 168.</td>
</tr>
</tbody>
</table>
| 13. Remove the old server from the driver set. For more information, see “Removing the Old Server from the Driver Set” on page 167.
<table>
<thead>
<tr>
<th>Checklist Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>14. Activate your upgraded Identity Manager solution. For more information, see &quot;Activating Identity Manager&quot; on page 131.</td>
</tr>
</tbody>
</table>
# Migrating Identity Manager to a New Server

This section provides information for migrating from the User Application to the identity applications on a new server. You might also need to perform a migration when you cannot upgrade an existing installation. This section includes the following activities:

- “Checklist for Migrating Identity Manager” on page 177
- “Preparing Your Designer Project for Migration” on page 178
- “Copying Server-specific Information for the Driver Set” on page 179
- “Migrating the Identity Manager Engine to a New Server” on page 180
- “Migrating the User Application Driver” on page 181
- “Upgrading the Identity Applications” on page 182
- “Migrating Identity Applications” on page 182
- “Completing the Migration of the Identity Applications” on page 184

## Checklist for Migrating Identity Manager

NetIQ recommends that you complete the steps in the following checklist.

<table>
<thead>
<tr>
<th>Checklist Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Back up the directories and databases of your Identity Manager solution.</td>
</tr>
</tbody>
</table>
| 2. Ensure that you have installed the latest versions of the Identity Manager components, except for the identity applications.  
**NOTE:** To continue using your current User Application database, specify Existing Database in the installation program. |
| 3. Run a health check of the Identity Vault to ensure that the schema extends properly. Use TID 3564075 to complete the health check. |
| 4. Import your existing User Application drivers into Designer. |
| 5. Archive the Designer project. It represents the pre-migration state of the drivers. For more information, see “Preparing Your Designer Project for Migration” on page 178. |
| 6. (Conditional) To migrate the Identity Manager engine to a new server, copy the eDirectory replicas to the new server. For more information, see “Migrating the Identity Manager Engine to a New Server” on page 180. |
| 7. Create a new Designer project in the latest version of Designer, then import the User Application driver to prepare for migration. |
Preparing Your Designer Project for Migration

Before you migrate the driver, you need to perform some setup steps to prepare the Designer project for migration.

NOTE: If you do not have an existing Designer project to migrate, create a new project by using File > Import > Project (From Identity Vault).

1. Launch Designer.
2. (Conditional) If you have an existing Designer project that contains the User Application that you want to migrate, back up the project:
   2a Right-click the name of the project in Project view, then select Copy Project.
   2b Specify a name for the project, then click OK.
3. To update the schema for your existing project, complete the following steps:
   3a In the Modeler view, select the Identity Vault.
   3b Select Live > Schema > Import.
4. (Optional) To verify that the version number for Identity Manager is correct in your project, complete the following steps:
   4a In the Modeler view, select the Identity Vault and then click Properties.
   4b In the left navigation menu, select Server List.
   4c Select a server and then click Edit.
      The Identity Manager version field should show the latest version.

   8. Migrate the User Application driver. For more information, see “Migrating the User Application Driver” on page 181.
   9. Deploy the two drivers to the Identity Vault.
   10. Upgrade the Identity Applications. For more information, see “Upgrading Identity Applications” on page 152.
   11. Ensure that your browsers do not contain content from the previous versions of Identity Manager. For more information, see “Flushing the Browser Cache” on page 185.
   12. (Conditional) Reinstate your custom settings for the SharedPagePortlet. For more information, see “Updating the Maximum Timeout Setting for the SharedPagePortlet” on page 185.
   13. Ensure that the search option for groups does not display information until the user provides filter parameters. For more information, see “Disabling the Automatic Query Setting for Groups” on page 186.
Copying Server-specific Information for the Driver Set

You must copy all server-specific information that is stored in each driver and driver set to the new server’s information. This also includes GCVs and other data on the driver set that will not be there on the new server and need to be copied. The server-specific information is contained in:

- Global configuration values
- Engine control values
- Named passwords
- Driver authentication information
- Driver startup options
- Driver parameters
- Driver set data

You can do this in Designer or iManager. If you use Designer, it is an automated process. If you use iManager, it is a manual process. If you are migrating from an Identity Manager server earlier than 3.5 version to an Identity Manager server greater than or equal to 3.5, you should use iManager. For all other supported migration paths, you can use Designer.

- “Copying the Server-specific Information in Designer” on page 179
- “Changing the Server-specific Information in iManager” on page 180
- “Changing the Server-specific Information for the User Application” on page 180

Copying the Server-specific Information in Designer

This procedure affects all drivers stored in the driver set.

1. In Designer, open your project.
2. In the Outline tab, right-click the server, then select Migrate.
3. Read the overview to see what items are migrated to the new server, then click Next.
4. Select the target server from the list available servers, then click Next.
   The only servers listed are servers that are not currently associated with a driver set and are equal to or newer than the source server’s Identity Manager version.
5. Select one of the following options:
   - Make the target server active: Copies the settings from the source server to the target server and disables the drivers on the source server. NetIQ recommends using this option.
   - Keep the source server active: Does not copy the settings and disables all drivers on the target server.
   - Makes both target and source servers active: Copies settings from the source server to the target server without disabling the drivers on the source or target servers. This option is not recommended. If both drivers are started, the same information is written to two different queues and this can cause corruption.
6. Click Migrate.
7. Deploy the changed drivers to the Identity Vault.
For more information, see “Deploying a Driver to an Identity Vault” in the NetIQ Designer for Identity Manager Administration Guide.

8 Start the drivers.

For more information, see Stopping, Starting, or Restarting a Driver in Designer in the NetIQ Identity Manager Driver Administration Guide.

Changing the Server-specific Information in iManager

1 In iManager, click to display the Identity Manager Administration page.
2 Click Identity Manager Overview.
3 Browse to and select the container that holds the driver set.
4 Click the driver set name to access the Driver Set Overview page.
5 Click the upper right corner of the driver, then click Stop driver.
6 Click the upper right corner of the driver, then click Edit properties.
7 Copy or migrate all server-specific driver parameters, global configuration values, engine control values, named passwords, driver authentication data, and driver startup options that contain the old server’s information to the new server’s information. Global configuration values and other parameters of the driver set, such as max heap size, Java settings, and so on, must have identical values to those of the old server.
8 Click OK to save all changes.
9 Click the upper right corner of the driver to start the driver.
10 Repeat Step 5 through Step 9 for each driver in the driver set.

Changing the Server-specific Information for the User Application

You must reconfigure the User Application to recognize the new server. Run configupdate.bat.

1 Navigate to the configuration update utility located by default in the installation subdirectory of the User Application.
2 At a command prompt, launch the configuration update utility (configupdate.bat).
3 Specify the values as described in “Configuring the Settings for the Identity Applications” on page 71.

Migrating the Identity Manager Engine to a New Server

When migrating the Identity Manager engine to a new server, you can keep the eDirectory replicas that you currently use on the old server.

1 Install a supported version of eDirectory on the new server.
2 Copy the eDirectory replicas that are on the current Identity Manager server to the new server.
For more information, see “Administering Replicas” in the NetIQ eDirectory Administration Guide.

3 Install the Identity Manager engine on the new server.

Migrating the User Application Driver

When upgrading to a new version of Identity Manager or migrating to a different server, you might need to import a new base package for the User Application driver, or upgrade the existing package. For example, User Application Base Version 2.2.0.20120516011608.

When you begin working with an Identity Manager project, Designer automatically prompts you to import new packages into the project. You can also manually import the package at that time.

Importing a New Base Package

1 Open your project in Designer.
2 Right-click Package Catalog > Import Package, then select the appropriate package.
3 (Conditional) If the Import Package dialog does not list the User Application Base package, complete the following steps:
   3a Click the Browse button.
   3c Click OK.
4 Click OK.

Upgrading an Existing Base Package

1 Open your project in Designer.
2 Right-click the User Application Driver.
3 Click Driver > Properties > Packages.
   If the base package can be upgraded, the application displays a check mark in the Upgrades column.
4 Click Select Operation for the package that indicates there is an upgrade available.
5 From the drop-down list, click Upgrade.
6 Select the version to which you want to upgrade. Then click OK.
7 Click Apply.
8 Fill in the fields with appropriate information to upgrade the package. Then click Next.
9 Read the summary of the installation. Then click Finish.
10 Close the Package Management page.
11 Deselect Show only applicable package versions.
Deploying the Migrated Driver

The driver migration is not complete until you deploy the User Application driver to the Identity Vault. After the migration, the project is in a state in which only the entire migrated configuration can be deployed. You cannot import any definitions into the migrated configuration. After the entire migration configuration has been deployed, this restriction is lifted, and you can deploy individual objects and import definitions.

1. Open the project in Designer and run the Project Checker on the migrated objects.
   
   For more information, see “Validating Provisioning Objects” in the NetIQ Identity Manager - Administrator’s Guide to Designing the Identity Applications. If validation errors exist for the configuration, you are informed of the errors. These errors must be corrected before you can deploy the driver.

2. In the Outline view, right-click the User Application driver.

3. Select Deploy.

4. Repeat this process for each User Application driver in the driver set.

Upgrading the Identity Applications

When you run the Upgrade program for the identity applications, ensure that you incorporate the following considerations:

- Use the same database that you used for the previous User Application. That is, the installation from which you are migrating. In the installation program, specify Existing Database for the database type.

- You can specify a different name for the User Application context.

- Specify an installation location that is different from the one for the previous installation.

- Point to a supported version of Tomcat.

- Do not use case-sensitive collation for your database. Case-sensitive collation is not supported. The case-insensitive collation might cause duplicate key errors during migration. If a duplicate key error is encountered, check the collation and correct it, then re-install the identity applications. The only supported collation is SQL_Latin1_General_CP1_CI_AS.

For more information about upgrading the Identity Applications, see “Upgrading Identity Applications” on page 152.

Migrating Identity Applications

Do not use case-sensitive collation for your database. Case-sensitive collation is not supported. The case-sensitive collation might cause duplicate key errors during migration. If a duplicate key error is encountered, check the collation and correct it, then re-install the identity applications. The only supported collation is SQL_Latin1_General_CP1_CI_AS.

Before you migrate Identity Applications, you must install the libssl.so.1.0.0 and libcrypto.so.1.0.0 libraries from the /opt/netiq/common/openssl/lib64/ directory.
The migration of Identity Applications involves the following:

- “Migrating the Database to the New Server” on page 183
- “Installing Identity Applications on the New Server” on page 184

**Migrating the Database to the New Server**

If your User Application database is on PostgreSQL, perform the following steps:

1. Log in to the server where PostgreSQL is installed.
2. Open command prompt, navigate to `postgres` bin directory and export the data to a `.sql` file.
   
   Example: `pg_dumpall -U postgres > dump.sql`

3. Log in to the new server where you want to install PostgreSQL.
4. Install the PostgreSQL as mentioned below:
   
   
   4b. Navigate to the location where you have mounted the `Identity_Manager_4.8.x_Windows.iso`.
   
   4c. Navigate to: `<Mount location>` common\packages\postgres\ directory.
   
   4d. Run the PostgreSQL installer.

5. Navigate to `C:\NetIQ\IDM\postgres` and delete the Data directory.

6. Create a data directory in the PostgreSQL installed location and make sure `postgres` user has access rights to the directory.

7. Open command prompt, navigate to `postgres` bin directory and initialize the database as shown below:

   Example: `initdb.exe -D C:\NetIQ\IDM\postgres\data -E WIN1252 -U postgres`.

8. Ensure that the following entries are present in `pg_hba.conf` file located under `C:\NetIQ\IDM\postgres\data`.

   # IPv6 local connections:
   
   host all all ::1/128 trust
   host all all 0.0.0.0/0 trust

9. Ensure that the following is uncommented in `postgresql.conf` file:

   listen_addresses = '*'
   port = 5432

10. Restart `postgres` services from running `services.msc` from run.

11. Open command prompt, navigate to `postgres` bin directory, and import the data to the new PostgreSQL database, and then use the collected dump as explained in step 2.

    Example: `psql -U postgres < dump.sql`.
Installing Identity Applications on the New Server

The following procedure explains about installing Identity Application on the New Server:

1. Download the Identity_Manager_4.8.x_Windows.iso from the NetIQ Downloads Website (https://dl.netiq.com).
3. Navigate to Identity apps directory, install Identity Applications and skip the deployment of User Application, and Roles & Resources Service driver.
   3a. Select the Custom Installation mode.
   3b. Enter the Identity Vault details.
   3c. Uncheck Deploy Identity Applications Driver.
4. Select Existing PostgreSQL server, provide the required details, and proceed with the installation.

Completing the Migration of the Identity Applications

After upgrading or migrating the identity applications, complete the migration process.

Preparing an Oracle Database for the SQL File

During the installation process, you might have chosen to write a SQL file to update the identity applications database. If your database runs on an Oracle platform, you must perform some steps before you can run the SQL file.

1. In the database, run the following SQL statements:

   ```sql
   ALTER TABLE DATABASECHANGELOG ADD ORDEREXECUTED INT;
   UPDATE DATABASECHANGELOG SET ORDEREXECUTED = -1;
   ALTER TABLE DATABASECHANGELOG MODIFY ORDEREXECUTED INT NOT NULL;
   ALTER TABLE DATABASECHANGELOG ADD EXECTYPE VARCHAR(10);
   UPDATE DATABASECHANGELOG SET EXECTYPE = 'EXECUTED';
   ALTER TABLE DATABASECHANGELOG MODIFY EXECTYPE VARCHAR(10) NOT NULL;
   ```

2. Run the following updateSQL command:

   ```bash
   C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m -Dwar.context.name=IDMProv -Ddriver.dn="cn=User Application Driver, cn=driverset1, o=system" -Duser.container="o=data" -jar C:\NetIQ\idm\jre\liquibase.jar --databaseClass=liquibase.database.core.PostgresDatabase --driver=org.postgresql.Driver --classpath=C:\NetIQ\idm\apps\postgresql\postgresql-9.4.1212jdbc42.jar C:\NetIQ\idm\apps\UserApplication\IDMProv.war --changeLogFile=DatabaseChangeLog.xml --url="jdbc:postgresql://localhost:5432/idmuserappdb" --contexts="prov, newdb" --logLevel=info --logFile=C:\NetIQ\idm\apps\UserApplication\db.out --username=******** --password=******** update
   ```
3 In a text editor, open the SQL file, by default in the `\installation_path\userapp\sql` directory.

4 Insert a backslash (/) after the definition of the function CONCAT_BLOB. For example

```sql
-- Changeset icfg-data-load.xml::700::IDMRBPM
CREATE OR REPLACE FUNCTION CONCAT_BLOB(A IN BLOB, B IN BLOB) RETURN BLOB
AS
  C BLOB;
BEGIN
  DBMS_LOB.CREATETEMPORARY(C, TRUE);
  DBMS_LOB.APPEND(C, A);
  DBMS_LOB.APPEND(C, B);
  RETURN C;
END;
/
```

5 Execute the SQL file.

   For more information about running the SQL file, see “Manually Creating the Database Schema” on page 94.

   **NOTE:** Do not use SQL*Plus to execute the SQL file. The line lengths in the file exceed 4000 characters.

---

Flushing the Browser Cache

Before you log in to the identity applications, you should flush the cache on the browser. If you do not flush the cache, you might experience some runtime errors.

Updating the Maximum Timeout Setting for the SharedPagePortlet

If you have customized any of the default settings or preferences for the SharedPagePortlet, then it has been saved to your database and this setting will get overwritten. As a result, navigating to the Identity Self-Service tab might not always highlight the correct Shared Page. To be sure that you do not have this problem, complete the following steps:

1 Log in as a User Application Administrator.
2 Navigate to Administration > Portlet Administration.
3 Expand Shared Page Navigation.
4 In the portlet tree on the left, click Shared Page Navigation.
5 On the right side of the page, click Settings.
6 Ensure that Maximum Timeout is set to 0.
7 Click Save Settings.
Disabling the Automatic Query Setting for Groups

By default, the DNLookup Display for the Group entity in the Directory Abstraction Layer is enabled. This means that whenever the object selector is opened for a group assignment, all the groups are displayed by default without the need to search them. You should change this setting, since the window to search for groups should be displayed without any results until the user provides input for search.

You can change this setting in Designer by unchecking Perform Automatic Query, as shown below:

\[
\text{uncheck this if you don't want the autoquery to occur}
\]
Deploying Identity Manager on Microsoft Azure

This section explains the planning and implementation of Identity Manager on the Microsoft Azure cloud.

- Chapter 15, “Planning and Implementation of Identity Manager on Microsoft Azure,” on page 189
- Chapter 16, “Example Scenarios of Hybrid Identity Manager,” on page 199
Planning and Implementation of Identity Manager on Microsoft Azure

Identity Manager adds support for deploying the following Identity Manager components on Microsoft Azure.

- Identity Manager engine
- Identity Manager drivers and Remote Loaders
- iManager
- Designer
- Identity Applications
- Identity Reporting

NOTE: Deployment of Sentinel Log Management is not supported on Microsoft Azure.

Prerequisites

In addition to the system requirements of Identity Manager components, ensure that you meet the following prerequisites:

- An administrative account on Microsoft Azure.
- Identity_Manager_4.8_Windows.iso and Designer are downloaded, extracted, and available on Identity Manager component instances.
- Remote desktop to connect to Azure VM instances from your local client machine.

Deployment Procedure

Identity Manager components can be deployed on a private or a public network based on your requirement. Figure 15-1 illustrates a sample deployment that is used in the subsequent sections.
Identity Manager components can be deployed on Microsoft Azure in different combinations depending on how the components are distributed on different servers. However, the deployment procedure is the same for all scenarios.

The deployment procedure consists of the following steps:

- “Creating a Resource Group” on page 191
- “Creating a Virtual Network and Subnet” on page 191
- “Creating an Application Gateway” on page 192
- “Creating a Virtual Machine Instance” on page 193
- “Updating host entries in VM” on page 194
- “Setting Up Designer” on page 196
- “Configuring the Application Gateway” on page 196
Creating a Resource Group

NetIQ recommends you to create a resource group and add the required resources to the group to use with Identity Manager. Perform the following steps to create a new resource group:

1. Log in to the Azure portal.
2. Click Resource groups.
3. Click Create.
4. In the Basics tab:
   - 4a Select your Subscription from the drop-down list.
   - 4b Enter a new resource group name.
   - 4c Select the location from the Region drop-down list. For example, Central India.
   - 4d Click Next : Tags >.
5. In the Tags tab, click Next : Review + Create >.
6. In the Review + create tab, click Create.

Creating a Virtual Network and Subnet

1. Log in to the Azure Portal.
2. Type virtual network in the search.
4. Click Create.
5. In the Basics tab, specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription</td>
<td>Select your Subscription from the drop-down list.</td>
</tr>
<tr>
<td>Resource Group</td>
<td>Select the existing resource group from the drop-down.</td>
</tr>
<tr>
<td>Name</td>
<td>Specify the name for virtual network.</td>
</tr>
<tr>
<td>Region</td>
<td>Select the location from the drop-down list. For example, Central India.</td>
</tr>
</tbody>
</table>

   - 5a Click Next : IP Addresses >.
6. In the IP Addresses tab, click Add subnet.
   - 6a Click Add subnet.
     - 6a1 Specify the subnet name. For example, default.
     - 6a2 Specify the subnet address range. For example, 10.1.0.0/24.
     - 6a3 Click Add.
   - 6b Click Next : Security >.
7. In the Security tab, keep the default values for all the fields, then click Next : Tags >.
8 In the Tags tab, click Next : Review + create >.
9 In the Review + create tab, review your settings, then click create.

Creating an Application Gateway

1 Log in to the Azure portal.
2 Click Create a Resource.
3 Go to Categories > Networking > Application Gateway.
4 In the Basics tab, specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription</td>
<td>Select your Subscription from the drop-down list.</td>
</tr>
<tr>
<td>Resource Group</td>
<td>Select the existing resource group from the drop-down.</td>
</tr>
<tr>
<td>Application gateway name</td>
<td>Specify the Application gateway name.</td>
</tr>
<tr>
<td>Region</td>
<td>Select the location from the drop-down list. For example, Central India.</td>
</tr>
<tr>
<td>Tier</td>
<td>Select the required tier. For example, Standard V2.</td>
</tr>
<tr>
<td>Minimum instance count</td>
<td>Specify the value 0.</td>
</tr>
<tr>
<td>Maximum instance count</td>
<td>Specify the value 10.</td>
</tr>
<tr>
<td>Virtual Network</td>
<td>Select the virtual network and corresponding subnet that is already created. See “Creating a Virtual Network and Subnet” on page 191.</td>
</tr>
</tbody>
</table>

4a Keep the default values for the rest of the fields then click Next : Frontends >.
5 In the Frontends tab:

5a Select Public.
5b Under Public IP address, click Add new.

5b1 Specify public IP address name. For example, idmgateway.centralindia.cloudapp.azure.com.
5b2 Click OK.
5c Click Next : Backends >
6 In the Backends tab:

6a Click Add a backend pool.
6a1 Specify backend pool name.
6a2 Select Yes to add a backend pool without targets.
6a3 Click Add.
6b Click Next : Configuration >.
7 In the Configuration tab:
   7a Under Routing rules, click Add a routing rule.
   7b Specify the Rule name.
   7c In the Listener tab, specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listener Name</td>
<td>Specify the Listener name.</td>
</tr>
<tr>
<td>Frontend IP</td>
<td>Select Public from the drop-down.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select HTTP.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the value 80.</td>
</tr>
</tbody>
</table>

7d Keep the default values for the rest of the fields.

7e In the Backend targets tab, specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backend target</td>
<td>Select the backend target from the drop-down.</td>
</tr>
<tr>
<td>HTTP Settings</td>
<td>Click Add new, specify the HTTP settings name. Keep the default values for all the fields, then click Add.</td>
</tr>
</tbody>
</table>

7e1 Click Add.

7f Click Next : Tags >.

8 In the Tags tab, click Next : Review + create >.

9 In the Review + create > tab, review your settings, then click Create.

NOTE: For more information related to configuring the application gateway, see “Configuring the Application Gateway” on page 196.

Creating a Virtual Machine Instance

Create a separate virtual machine to host the Identity Manager components.

1 Log in to the Azure portal.
2 Type virtual machines in the search.
3 Under Services, select Virtual machines.
4 Click Create, then select Virtual machine.
5 In the Basics tab:
   5a Select your Subscription from the drop-down list.
   5b Select the existing resource group from the drop-down list (see “Creating a Resource Group” on page 191).
   5c Specify the Virtual machine name.
Select the location from the Region drop-down list. For example, Central India.

Select the required Windows Server from the Image drop-down list. For example, Windows Server 2019.

Select the virtual machine size from the Size drop-down list.

Specify Username, Password, and Confirm password.

Under Licensing, select Windows Server License, then select eligible Windows Server License with Software Assurance to confirm.

Keep the default values for the rest of the fields.

Click Next : Disks >.

In the Disks tab:

Select the disk type from the OS disk type drop-down list. For example, Premium SSD.

Select the required Encryption type from the drop-down list.

Click Next : Networking >.

In the Networking tab:

Select the virtual network and corresponding subnet that is already created. See, “Creating a Virtual Network and Subnet” on page 191.

Under network security group, select Advanced.

Select the existing network security group from the drop-down list.

(Conditional) If network security group is not available, click Create new.

Specify network security group name.

Click Add an inbound role, specify the required details.

Click Add an outbound role, specify the required details.

Click OK.

Keep the default values for the rest of the fields.

Click Next : Management >.

In the Management tab, keep the default values for all the fields, then click Next : Advanced >.

In the Advanced tab, keep the default values for all the fields, then click Next : Tags >.

In the Tags tab, keep the default values for all the fields, then click Next : Review + create >.

In the Review + create tab, review your settings, then click Create.

Updating host entries in VM

You can access the Identity Manager components using the public DNS name of the application gateway or the alias DNS record set. To allow Identity Manager components to communicate with one another, edit the hosts files on each VM and add an entry to resolve its hostname.
Table 15-1  Updating host entries

<table>
<thead>
<tr>
<th>Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Engine</td>
<td>Navigate to hosts file in Identity engine VM. For example,</td>
</tr>
<tr>
<td></td>
<td>C:\Windows\System32\drivers\etc\hosts</td>
</tr>
<tr>
<td></td>
<td>Modify the hosts file with the following entry:</td>
</tr>
<tr>
<td></td>
<td>&lt;IP address of Identity engine VM&gt; &lt;Private DNS Name of Identity engine VM&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>10.0.1.1 identityengine.example.com</td>
</tr>
<tr>
<td></td>
<td>&lt;IP address of Identity applications VM&gt; &lt;Public DNS Name of application gateway&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>10.0.1.2 idmgateway.centralindia.cloudapp.azure.com</td>
</tr>
<tr>
<td>Identity Applications</td>
<td>Navigate to hosts file in Identity engine VM. For example,</td>
</tr>
<tr>
<td></td>
<td>C:\Windows\System32\drivers\etc\hosts</td>
</tr>
<tr>
<td></td>
<td>Modify the hosts file with the following entry:</td>
</tr>
<tr>
<td></td>
<td>&lt;IP address of Identity engine VM&gt; &lt;Private DNS Name of Identity engine VM&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>10.0.1.1 identityengine.example.com</td>
</tr>
<tr>
<td></td>
<td>&lt;IP address of Identity applications VM&gt; &lt;Public DNS Name of application gateway&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>10.0.1.2 idmgateway.centralindia.cloudapp.azure.com</td>
</tr>
</tbody>
</table>

To update the host entries for Identity Reporting and iManager, see Identity Applications in Table 15-1 on page 195.

NOTE: For the installation of Identity Manager components, see “Installation Procedures” on page 45.
Setting Up Designer

   For the Windows security group, use `rdesktop` port only. For example `3389`.

Configuring the Application Gateway

Configure the application gateway to allow external networks to use Identity Manager components that are hosted on the virtual machines.

1 Configure a separate backend pool for Identity Manager components such as iManager, Identity Applications, forms and Identity Reporting.
   1a In Backend pools, click Add.
   1b Specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of a backend pool to identify the Identity Manager component.</td>
</tr>
<tr>
<td>Type</td>
<td>Specify the type in one of the following ways:</td>
</tr>
<tr>
<td></td>
<td>- <strong>IP address or FQDN</strong>: Specify the IP address or FQDN of the required Identity Manager component.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Virtual Machine</strong>: Select the Virtual Machine that is hosting the required Identity Manager component.</td>
</tr>
</tbody>
</table>

1c Click OK.
   Repeat this step to configure additional backend pools.

2 Configure separate HTTP settings for Identity Manager components such as iManager, Identity Applications, forms and Identity Reporting.

   **NOTE:** Ensure that you have exported the public certificate for the required Identity Manager components.

   2a In HTTP Settings, click Add.
   2b Specify the following details:
Repeat this step to configure additional HTTP settings.

3 Configure a separate listener for each Identity Manager component such as iManager, Identity Applications, forms and Identity Reporting.

**NOTE:** Ensure that you have exported the .PFX certificate from the Identity Vault.

3a In Listeners, click Basic.

3b Specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of an HTTP setting to identify the Identity Manager component.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select HTTPS.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port of the Identity Manager Component.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>• <strong>iManager</strong>: 8443</td>
</tr>
<tr>
<td></td>
<td>• <strong>Identity Applications</strong>: 8543</td>
</tr>
<tr>
<td></td>
<td>• <strong>Forms</strong>: 8600</td>
</tr>
<tr>
<td></td>
<td>• <strong>Identity Reporting</strong>: 8643</td>
</tr>
</tbody>
</table>

2c Click OK.
Click OK.

Repeat this step to configure additional listeners.

4 Create a basic rule for Identity Manager components such as iManager, Identity Applications, forms and Identity Reporting and associate this rule with the respective backend pool, Listener, and HTTP setting.

4a In Rule, click Add.

4b Specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of a rule that helps in identifying the Identity Manager component.</td>
</tr>
<tr>
<td>Listener</td>
<td>Select the respective listener that is created in Step 3.</td>
</tr>
<tr>
<td>Backend Pool</td>
<td>Select the respective backend pool that is created in Step 1.</td>
</tr>
<tr>
<td>HTTP setting</td>
<td>Select the respective HTTP setting that is created in Step 2.</td>
</tr>
</tbody>
</table>

4c Click OK.

Repeat this step to configure additional rules.
Example Scenarios of Hybrid Identity Manager

You can configure Identity Manager components where the identities are synchronized seamlessly between your enterprise premise and MS Azure cloud. Implementing this type of a hybrid scenario requires you to configure a VPN connection between the Azure subnet and the enterprise network. This section explains the following hybrid scenarios:

- “Using Multi-Server Driver Set Connection” on page 199
- “Using eDirectory Driver Connection” on page 200

Using Multi-Server Driver Set Connection

In this scenario, at least two Identity Manager servers use the same eDirectory tree and driver set where one server is installed on Azure cloud and the other server is installed on the enterprise premise. This includes full replica servers that use the Identity Vault replication channel to synchronize the identities through VPN connection. The Identity Manager server that is running on the enterprise network or Azure cloud synchronizes the identities across their respective connected applications.

Figure 16-1  Hybrid Scenario Using Multi-Sever Driver Set Connection
Using eDirectory Driver Connection

This scenario is suitable if you have Identity Manager servers installed on two separate eDirectory trees where one tree belongs to Azure cloud and the other tree belongs to the enterprise network. This configuration uses eDirectory driver to synchronize identities between Azure cloud and the enterprise network through a VPN connection. The Identity Manager server that is running on the enterprise network or Azure cloud synchronizes the identities across their respective connected applications.

**Figure 16-2  Hybrid Scenario Using eDirectory Driver Connection**

The communication between the Azure cloud and the enterprise network is limited. It only synchronizes the delta changes. You can control the attributes to synchronize by configuring the driver filter. You can also leverage the policy engine to define additional controls for synchronizing attributes. For example, limit the password attribute from synchronizing and allow users to use different passwords to access Identity Manager servers from the Azure cloud and the enterprise network.
Uninstalling Identity Manager Components

This section describes the process for uninstalling the components of Identity Manager. Some components have prerequisites for uninstallation. Ensure that you review full section for each component before beginning the uninstallation process.

**NOTE:** You must stop all services such as Tomcat, PostgreSQL, and ActiveMQ before uninstalling the Identity Manager components.

### Uninstalling the Identity Vault

Before you uninstall the Identity Vault, you must understand your eDirectory tree structure and replica placements. For example, you should know whether you have more than one server in the tree.

1. **(Conditional) If you have more than one server in your eDirectory tree, complete the following steps:**
   1a. **(Conditional) If the server where you installed eDirectory holds any master replicas,** promote another server in the replica ring to be a master before you remove eDirectory. For more information, see “Managing Partitions and Replicas” in the *NetIQ eDirectory Administration Guide*.
   1b. **(Conditional) If the tree on the server where you installed eDirectory holds the only copy of a partition,** either merge this partition into the parent partition or add a replica of this partition to another server and make it the master replica holder. For more information, see “Managing Partitions and Replicas” in the *NetIQ eDirectory Administration Guide*.
   1c. **Perform a health check on the eDirectory database.** Fix any errors that occur before proceeding. For more information, see “Keeping eDirectory Healthy” in the *NetIQ eDirectory Administration Guide*.

2. **Uninstall the Identity Vault:**
   Use the Control Panel utility for adding and removing programs. For example, on Windows Server 2012 R2, click **Programs and Features.** Right-click **NetIQ eDirectory,** then click **Uninstall.**

3. **(Conditional) If you have more than one server in your eDirectory tree, complete the following steps:**
   3a. **Delete any server-specific objects left in the tree.**
   3b. **Perform another health check to verify that the server was properly removed from the tree.** For more information, see “Keeping eDirectory Healthy” in the *NetIQ eDirectory Administration Guide*. 
Removing Objects from the Identity Vault

The first step in uninstalling Identity Manager is to delete all Identity Manager objects from the Identity Vault. When the driver set is created, the wizard prompts you to make the driver set a partition. If any driver set objects are also partition root objects in eDirectory, the partition must be merged into the parent partition before you can delete the driver set object.

To remove objects from the Identity Vault:

1. Perform a health check on the eDirectory database, then fix any errors that occur before proceeding.
   For more information, see “Keeping eDirectory Healthy” in the NetIQ eDirectory Administration Guide.
2. Log in to iManager as an administrator with full rights to the eDirectory tree.
4. Browse to and select the driver set object that is the partition root object, then click OK.
5. Wait for the merge process to complete, then click OK.
6. Delete the driver set object.
   When you delete the driver set object, the process deletes all the driver objects associated with that driver set.
7. Repeat Step 3 through Step 6 for each driver set object that is in the eDirectory database, until they are all deleted.
8. Repeat Step 1 to ensure that all merges completed and all of the objects have been deleted.

Uninstalling the Identity Manager Engine

When you install the Identity Manager engine, the installation process places an uninstallation script on the Identity Manager server. This script allows you to remove all services, packages, and directories that were created during the installation.

NOTE: Before uninstalling the Identity Manager engine, prepare the Identity Vault. For more information, see “Removing Objects from the Identity Vault” on page 202.

To uninstall the Identity Manager engine on a Windows server, use the Control Panel utility for adding and removing programs. For example, on Windows 2012 R2, click Programs and Features. Right-click Identity Manager, then click Uninstall.

Uninstalling the Remote Loader

When you install the Remote Loader, the installation process places an uninstallation script on the server. This script allows you to remove all services, packages, and directories that were created during the installation.

To uninstall the Remote Loader on a Windows server, use the Control Panel utility for adding and removing programs.
Uninstalling Identity Manager Components

Uninstalling the Identity Applications

You must uninstall each component of the Roles Based Provisioning Module (RBPM), such as the drivers and the database.

If you need to uninstall the runtime components associated with RBPM, the uninstallation program automatically reboots your server, unless you are running the uninstall program in silent mode on Windows. You must manually reboot the Windows server.

NOTE: Before uninstalling RBPM, uninstall the Identity Manager engine. For more information, see “Uninstalling the Identity Manager Engine” on page 202.

Deleting the Drivers for the Roles Based Provisioning Module

You can use Designer or iManager to delete the User Application driver and the Role and Resource Service driver.

1. Stop the User Application driver and the Role and Resource Service driver. Depending on the component that you use, complete one of the following actions:
   - **Designer**: Right-click the driver line, then click **Live > Stop Driver**.
   - **iManager**: On the Driver Set Overview page, click the upper right corner of the driver image, then click **Stop Driver**.

2. Delete the User Application driver and the Role and Resource Service driver. Depending on the component that you use, complete one of the following actions:
   - **Designer**: Right-click the driver line, then click **Delete**.
   - **iManager**: On the Driver Set Overview page, click **Drivers > Delete drivers**, then click the driver that you want to delete.

Uninstalling the Identity Applications

You must uninstall the User Application and its database from Tomcat. This procedure explains how to remove the User Application and its database from Tomcat and PostgreSQL. If you are using another application server and database, refer to that product’s documentation for instructions.

IMPORTANT: Be cautious when you remove the User Application because the process removes all the folders and files from the folder where the User Application scripts and supporting files were installed. When you remove the files, you might unintentionally uninstall Tomcat or PostgreSQL. For example, the installation folder is typically `C:\NetIQ\idm\apps\UserApplication`. This folder also contains the folders for Tomcat and PostgreSQL.

1. Log in to the server where you installed the User Application.

2. Open the Control Panel utility for adding and removing programs. For example, on Windows Server 2012 R2, click **Programs and Features**.

3. Right-click **Identity Manager User Application**, then click **Uninstall**.
Uninstalling the Identity Reporting Components

You must uninstall the Identity Reporting components in the following order:

1. Delete the drivers. For more information, see “Deleting the Reporting Drivers” on page 204.
2. Delete Identity Reporting. For more information, see “Uninstalling Identity Reporting” on page 204.
3. Delete Sentinel. For more information, see Uninstalling Sentinel Log Management for IGA in the NetIQ Identity Manager Setup Guide for Linux.

**NOTE:** To conserve disk space, the installation programs for Identity Reporting do not install a Java virtual machine (JVM). Therefore, to uninstall one or more components, ensure that you have a JVM available and also make sure that the JVM is in the PATH. If you encounter an error during an uninstallation, add the location of a JVM to the local PATH environment variable, then run the uninstallation program again.

Deleting the Reporting Drivers

You can use Designer or iManager to delete the Data Collection and Managed System Gateway drivers.

**1** Stop the drivers. Depending on the component that you use, complete one of the following actions:

- **Designer:** For each driver, right-click the driver line, then click Live > Stop Driver.
- **iManager:** On the Driver Set Overview page, click the upper right corner of each driver image, then click Stop Driver.

**2** Delete the drivers. Depending on the component that you use, complete one of the following actions:

- **Designer:** For each driver, right-click the driver line, then click Delete.
- **iManager:** On the Driver Set Overview page, click Drivers > Delete drivers, then click the driver that you want to delete.

Uninstalling Identity Reporting

Before deleting Identity Reporting, ensure you have deleted the Data Collection and Managed System Gateway drivers. For more information, see “Deleting the Reporting Drivers” on page 204.

**IMPORTANT:** Before running the Identity Reporting uninstallation program, ensure you copied your generated reports from the Reporting installation directory to another location on your computer because the uninstallation process removes all the files and folders from the directory where Reporting was installed. For example, the Reporting installation folder C:\NetIQ\idm\apps\IDMReporting.

To uninstall Identity Reporting, use the Control Panel utility for adding and removing programs. For example, on Windows Server 2012 R2, click Programs and Features. Right-click Identity Reporting, then click Uninstall.
Uninstalling Analyzer

1. Close Analyzer.
2. Uninstall Analyzer.

Use the Control Panel utility for adding and removing programs. For example, on Windows Server 2008, click Programs and Features. Right-click Analyzer for Identity Manager, then click Uninstall.

Uninstalling iManager

This section explains how to uninstall iManager and iManager Workstation. You do not need to follow a specific sequence for uninstalling iManager or the associated third-party components. NetIQ recommends reviewing the considerations for uninstalling any of these components:

- If you uninstall either the web server or the servlet container, you cannot run iManager.
- On all platforms, the uninstallation removes only files that the process installed in the first place. The uninstallation process does not remove any files that the application creates as it runs. For example, the log files and auto-generated configuration files that are created while Tomcat runs.
- The uninstallation process does not remove any files that were created or modified files within the directory structure that were originally added during the installation. This action ensures that the process does not unintentionally delete data.
- Uninstalling iManager does not affect any of the RBS configurations that you have set in your tree. The uninstallation process does not remove log files or custom content.

IMPORTANT: Before uninstalling iManager, back up any custom content or other special iManager files that you want to retain. For example, customized plug-ins.

Uninstalling iManager on Windows

To uninstall iManager components use the Control Panel utility for adding and removing programs. The following conditions apply to the uninstallation process:

- The Control Panel utility lists Tomcat and NICI separately from iManager. If you are no longer using them, uninstall these programs.
- If eDirectory is installed on the same server as iManager, do not uninstall NICI. eDirectory requires NICI to run.
- When uninstalling iManager, the program asks whether you want to remove all iManager files. If you select Yes, the program removes the files, including all custom content. However, the program does not remove 2.7 RBS objects from the eDirectory tree, and the schema remains in the same state.

Uninstalling iManager Workstation

To uninstall iManager Workstation, delete the directory where you extracted the files.
Uninstalling Designer

1 Close Designer.

2 Uninstall Designer according to the operating system:
   Use the Control Panel utility for adding and removing programs. For example, on Windows Server 2008, click **Programs and Features**. Right-click **Designer for Identity Manager**, then click **Uninstall**.
High availability ensures efficient manageability of critical network resources including data, applications, and services. NetIQ supports high availability for your Identity Manager solution through clustering or Hypervisor clustering, such as VMWare Vmotion. When planning a high-availability environment, the following considerations apply:

- You can install the following components in a high-availability environment:
  - Identity Vault
  - Identity Manager engine
  - Remote Loader
  - Identity applications, except Identity Reporting
- When you run the Identity Vault in a clustered environment, the Identity Manager engine is also clustered.

**NOTE:** Identity Manager does not support load balancing LDAP or LDAPS communication between Identity Vault and Identity Applications.

<table>
<thead>
<tr>
<th>For more information about...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determining the server configuration for Identity Manager components</td>
<td>see High Availability Configuration in NetIQ Identity Manager Overview and Planning Guide.</td>
</tr>
<tr>
<td>Running the Identity Vault in a cluster</td>
<td>Sample Identity Manager Cluster Deployment Solution</td>
</tr>
<tr>
<td>Running the identity applications in a cluster</td>
<td>Sample Identity Applications Cluster Deployment Solution</td>
</tr>
</tbody>
</table>

For more information on implementing high availability and disaster recovery in your Identity Manager environment, contact NetIQ Technical Support (https://www.netiq.com/support/).

This following chapters provide the steps for installing and configuring Identity Manager components in a high availability environment:

- Chapter 18, “Preparing for Installing Identity Manager in a Cluster Environment,” on page 209
- Chapter 19, “Sample Identity Manager Cluster Deployment Solution,” on page 213
- Chapter 20, “Sample Identity Applications Cluster Deployment Solution,” on page 215
Preparing for Installing Identity Manager in a Cluster Environment

- Prerequisites
- Preparing a Cluster for the Identity Applications

Prerequisites

- Identity Vault
- Identity Applications
- Database for Identity Applications

Identity Vault

Before installing the Identity Vault in a clustered environment, NetIQ recommends reviewing the following considerations:

- You must have two or more Windows servers with clustering software.
- You must have external shared storage supported by the cluster software, with sufficient disk space to store all Identity Vault and NICI data:
  - The Identity Vault DIB must be located on the cluster shared storage. State data for the Identity Vault must be located on the shared storage so that it is available to the cluster node that is currently running the services.
  - The root Identity Vault instance on each of the cluster nodes must be configured to use the DIB on the shared storage.
  - You must also share NICI (NetIQ International Cryptographic Infrastructure) data so that server-specific keys are replicated among the cluster nodes. NICI data used by all cluster nodes must be located on the cluster shared storage.
  - NetIQ recommends storing all other eDirectory configuration and log data on the shared storage.
- You must have a virtual IP address.
- (Conditional) If you are using eDirectory as the support structure for the Identity Vault, the `nds-cluster-config` utility supports configuring the root eDirectory instance only. eDirectory does not support configuring multiple instances and non-root installations of eDirectory in a cluster environment.

For more information about installing the Identity Vault in a clustered environment, see Deploying eDirectory on High Availability Clusters in the NetIQ eDirectory Installation Guide.
Identity Applications

You can install the database for the identity applications in an environment supported by Tomcat clusters with the following considerations:

- The cluster must have a unique cluster partition name, multicast address, and multicast port. Using unique identifiers separates multiple clusters to prevent performance problems and anomalous behavior.
  - For each member of the cluster, you must specify the same port number for the listener port of the identity applications database.
  - For each member of the cluster, you must specify the same hostname or IP address of the server hosting the identity applications database.
- You must synchronize the clocks of the servers in the cluster. If server clocks are not synchronized, sessions might time out early, causing HTTP session failover not to work properly.
- NetIQ recommends to not use multiple logins across browser tabs or browser sessions on the same host. Some browsers share cookies across tabs and processes, so allowing multiple logins might cause problems with HTTP session failover (in addition to risking unexpected authentication functionality if multiple users share a computer).
- The cluster nodes reside in the same subnet.
- A failover proxy or a load balancing solution is installed on a separate computer.

Database for Identity Applications

Database clustering is a feature of each respective database server. NetIQ does not officially test with any clustered database configuration because clustering is independent of the product functionality. Therefore, we support clustered database servers with the following caveats:

- By default, the maximum number of connections is set to 100. This value might be too low to handle the workflow request load in a cluster. You might see the following exception:

  (java.sql.SQLException: Data source rejected establishment of connection, message from server: "Too many connections.")

  To increase the maximum number of connections, set the max_connections variable in the my.cnf file to a higher value.
- Some features or aspects of your clustered database server might need to be disabled. For example, Transactional Replication must be disabled on certain tables due to constraint violations when trying to insert a duplicate key.
- We do not provide assistance on the installation, configuration, or optimization of the clustered database server, including installation of our products into a clustered database server.
- We exert our best effort to resolve any issues that might arise with the use of our products in a clustered database environment. Troubleshooting methods in a complex environment often require cooperative work to resolve issues. NetIQ provides expertise to analyze, plan, and troubleshoot the NetIQ products. The customer must provide expertise to analyze, plan and troubleshoot any third-party products. We ask customers to reproduce issues or analyze behavior of their components in a non-clustered environment to help isolate potential cluster setup issues from NetIQ product issues.
Preparing a Cluster for the Identity Applications

The identity applications supports HTTP session replication and session failover. If a session is in process on a node and that node fails, the session can be resumed on another server in the cluster without intervention. Before installing the identity applications in a cluster, you should prepare the environment.

- “Understanding Cluster Groups in Tomcat Environments” on page 211
- “Setting System Properties for Workflow Engine IDs” on page 211
- “Using the Same Master Key for Each User Application in the Cluster” on page 211

Understanding Cluster Groups in Tomcat Environments

The User Application cluster group uses a UUID name to minimize the risk of conflicts with other cluster groups that users might add to their servers. You can modify the configuration settings for User Application cluster group using the User Application administration features. Changes to the cluster configuration take effect for a server node only when you restart that node.

Setting System Properties for Workflow Engine IDs

Each server that hosts the identity applications in the cluster can run a workflow engine. To ensure performance of the cluster and the workflow engine, every server in the cluster should use the same partition name and partition UDP group. Also, each server in the cluster must be started with a unique ID for the workflow engine, because clustering for the workflow engine works independently of the cache framework for the identity applications.

To ensure that your workflow engines run appropriately, you must set system properties for Tomcat.

1. Create a new JVM system property for each identity applications server in the cluster.
2. Name the system property `com.novell.afw.wf.engine-id` where the engine ID is a unique value.

Using the Same Master Key for Each User Application in the Cluster

The identity applications encrypt sensitive data using a master key. All identity applications in a cluster must use the same master key. This section helps you ensure that all identity applications in a cluster use the same master key.

For more information about encrypting sensitive data in the identity applications, see Encrypting Sensitive Identity Applications Data in the NetIQ Identity Manager - Administrator’s Guide to the Identity Applications.

1. Install the User Application on the first node in the cluster.
2. In the Security - Master Key window of the installation program, note the location of the `master-key.txt` file that will contain the new master key for the identity applications. By default, the file is in the installation directory.
3. Install the identity applications on the other nodes in the cluster.
4 In the Security - Master Key window, click Yes and then click Next.

5 In the Import Master Key window, copy the master key from the text file that was created in Step 2.
Sample Identity Manager Cluster Deployment Solution

This section provides step-by-step instructions on how to configure Identity Manager into a cluster environment on Windows 2016 platform.

- “Prerequisites” on page 213
- “Configuring NetIQ Identity Manager on eDirectory Cluster” on page 213
- “Clustering Remote Loader” on page 214

Prerequisites

Identity Vault 9.2 running in a cluster environment on Windows 2016. For detailed information about setting up an eDirectory cluster, see Clustering eDirectory Services on Windows in the NetIQ eDirectory Installation Guide.

NOTE: Identity Vault does not support load balancing by using multiple cluster nodes. eDirectory clustering is only meant for achieving failover capability.

Configuring NetIQ Identity Manager on eDirectory Cluster

This section assumes that you have already set up an eDirectory cluster.

Use the following procedure to configure Identity Manager in an eDirectory cluster environment.

1 In Cluster Manager, set the eDirectory clustered roles priority to No Auto Start on the primary node.
2 Stop the secondary node.
3 Install Identity Manager engine on the primary node by selecting the Metadirectory Server option in the Identity Manager installation wizard.

IMPORTANT: Ensure that you are installing Identity Manager engine on a local storage.

4 Identity Manager installation wizard stops the eDirectory cluster role during installation. When this role is stopped, the status of this role may appear as failed. After installation, start the eDirectory cluster role from Cluster Manager.
5 Set the required priority for the eDirectory clustered role and make the secondary node active.
6 Install the Identity Manager engine on a secondary node using the DCLUSTER_INSTALL command.

For example, idm_install.exe -DCLUSTER_INSTALL=true
Clustering Remote Loader

1 Install the Remote Loader on the primary and secondary cluster nodes.

**NOTE:** For both primary and secondary node, ensure that Remote Loader is installed on the same shared storage path.

2 (Conditional) If you are using secured communications with the Remote Loader, store all the SSL certificates in a shared storage.

3 Before creating the Remote Loader cluster role, open the Remote Loader console and select Remote Loader as a Windows Service.

4 In Cluster Manager > Roles, create a new Remote Loader cluster role.

Specify the following information for the role:

**Role Type:** Generic Service

**Select Service:** Remote Loader instance registered as a Windows service.

**Name:** Cluster Role Name

**Address:** Unique IP address

**Select Storage:** Shared Cluster Storage

**Replicate Registry Settings:**

1. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\RLConsole`

2. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\DirXML Remote Loader\Command port 8000`  
   Specify the registry path for the Remote Loader instance which you want to cluster.

3. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\PassSync`

**NOTE:** By default, each cluster role accepts only one Windows service. Therefore, specify a command port and a corresponding registry path unique to each Remote Loader instance.

* Active Directory driver’s password filter is not supported on a Windows cluster.
The section provides instructions on how to configure the identity applications into a cluster environment on the Tomcat application server with an example deployment.

Clustering allows you to run the identity applications on several parallel servers (cluster nodes) and allows you to achieve high availability. To build a cluster, you need to group several Tomcat instances (nodes) together. The load is distributed across different servers, and even if any of the servers fail, the identity applications are accessible through other cluster nodes. For failover, you can create a cluster of Identity Applications and configure them to act as a single server. However, this configuration does not include Identity Reporting.

It is recommended to use a load balancer software that processes all user requests and dispatches them to the server nodes in the cluster. The load balancer is typically part of the cluster. It understands the cluster configuration as well as failover policies. You can select a solution that best suits you.

Figure 20-1 shows a sample deployment with a two-node cluster with the following assumptions:

- All the communication is routed through the load balancer.
- Components such as Identity Manager engine and User Application are installed on separate servers. For a production-level deployment, this is the recommended approach.
- You are familiar with the installation procedures for eDirectory, Identity Manager engine, Identity Applications, Apache Tomcat application server, and databases for the User Application.
- OSP (One Single-Sign On Provider) and User Application are installed on the same cluster node. However, you can install OSP on a different server in a production environment. In this case, you need to perform some configuration changes mentioned in “Installation Procedure” on page 217.
- SSPR (Single Sign-On Password Reset) is installed on a separate computer. For a production-level deployment, this is the recommended approach.
- PostgreSQL is used as a database for the User Application. However, you can use any of the Identity Manager 4.8 supported databases, such as Oracle, SQL Server, or PostgreSQL.
- All the User Application nodes communicate to the same instance of eDirectory and the User Application database. Based on your requirement, you can increase the number of User Application instances.
NOTE: A two-node cluster is the minimum configuration used for high availability. However, the concepts in this section can easily be extended to a cluster with additional nodes.

To help you understand the step-by-step configuration, this sample deployment is referred throughout the subsequent sections of the document.

Prerequisites

- Identity Manager components installed with a minimum version of 4.8. For upgrading to Identity Manager 4.8, see Chapter 11, “Upgrading Identity Manager Components,” on page 145.
- All the nodes have the same application server clocks. The easiest way to ensure this is to configure the nodes to use the same network time server for time synchronization using NTP.
- The cluster nodes reside in the same subnet.
- A failover proxy or a load balancing solution is installed on a separate computer.
- To achieve clustering for forms, start two instances of load balancer on the server, one for the Identity Applications and the other for the form renderer.
Installation Procedure

This section provides step-by-step instructions of installing a new instance of the identity applications on Tomcat and then configuring it for clustering.

1. Install the Identity Manager engine. For step-by-step instructions, see “Installation Procedures” on page 45. For a production-level deployment, it is recommended to install Identity Manager engine on a separate server.

2. Create and deploy the following drivers for the Identity Applications:
   - User Application driver
   - Roles and Resource Service driver

3. On Node1, install the following Identity Manager components:
   a. User Application
      During the installation process, configure the following settings:
      i. Select Tomcat as the application server.
      ii. Select PostgreSQL as the database platform.
      iii. Provide the required database details in the subsequent pages.
      iv. Copy the database driver jar file postgresql-9.4.1212.jar from the PostgreSQL server to all the User application nodes in the cluster.
      **NOTE:** You can use any of the Identity Manager 4.8 supported databases.
      v. Browse and select the copied database driver jar file.
      vi. In the New Database or Existing Database details page, select the New Database option.
      vii. In the Identity Manager Configuration page, provide a unique name in the Workflow Engine ID field. For example, you can use the unique name as Engine1 for Node1.
      viii. To create a new master key, select No in the Security – Master Key page.
      The identity applications encrypt sensitive data using a master key. As this is the first instance of the identity applications in a cluster; therefore, you must instruct the installation program to create a new master key by selecting No. In a cluster, the User Application clustering requires every instance of the User Application to use the same master key. To ensure that the same master key is used, import the existing key by selecting Yes while configuring these instances.

4. On Node2, perform the following actions:
   a. Install Tomcat by using the convenience installer (select only Tomcat during the installation process).
   b. Install OSP.
During the installation process, provide the IP address and port number of the Identity Manager engine (eDirectory) server in the Authentication details page.

c. Install the User Application.

During the installation process, configure the following settings:

i. Select **Tomcat** as the application server.

ii. Select **PostgreSQL** as the database platform.

**NOTE:** You can use any of the Identity Manager 4.8 supported databases.

iii. Provide the required database details in the subsequent pages of the installation procedure.

iv. Copy the database driver jar file `postgresql-9.4.1212.jar` from the PostgreSQL server to Node2.

**NOTE:** If you are using any other Identity Manager 4.8 supported databases, such as Oracle or SQL Server, ensure that you copy the respective driver jar files from the server where the database is installed to all the User application nodes in the cluster.

v. Browse and select the copied database driver jar file.

vi. In the New Database or Existing Database details page, select the **Existing Database** option.

vii. In the Identity Manager Configuration page, provide a unique name in the **Workflow Engine ID** field. For example, you can use the unique name as Engine2 for Node2.

viii. To create a new Master key in the Security – Master Key page, select **Yes**.

The User Application clustering requires every instance of the User Application to use the same master key. To ensure that the same master key is used, import the existing key by selecting **Yes**. This key is created when you installed the first instance of the User Application in Node1.

You can obtain the master key from the ism-configuration properties file located in `C:\NetIQ\IDM\apps\tomcat\conf` on Node1. The parameter that contains the master key is `com.novell.idm.masterkey`.

ix. Click **Install** to complete the installation.

**NOTE:** For detailed information about installing the Identity Applications, see “Installation Procedures” on page 45.

5. In load balancer server, start an instance of load balancer with Identity Applications port number and another instance of load balancer with form renderer port number for all clustered nodes. For example,

   - `./balance 8543 apps1-au.edu.in:8543 ! apps2-au.edu.in:8543`
   - `./balance 8600 apps1-au.edu.in:8600 ! apps2-au.edu.in:8600`

6. Install SSPR on a separate computer.

Before installing, make a note of the following settings and specify them during installation process:

a. Install **Tomcat**. For installation instructions, see Step 4a.

b. Install **SSPR**.
During the SSPR installation, perform the following actions:

i. In the Application Server connection page, select **Connect to external authentication server** and provide the DNS name of the server where the load balancer is installed.

ii. In the Authentication details page, provide the **IP address** and the **port** of the Identity Manager engine server. The password for the CA certificates is **changeit**.

c. After completing the SSPR installation, launch SSPR ([https://<IP>:<port>/sspr/private/config/ConfigEditor](https://<IP>:<port>/sspr/private/config/ConfigEditor)) and log in. Click **Configuration Editor > Settings > Security > Redirect Whitelist**.

   i. Click **Add value** and specify the following URL:

   ```
   https:<dns of the failover><port>/osp
   ```

   ii. Save the changes.

   iii. In the SSPR Configuration page, click **Settings > OAuth SSO** and modify the OSP links by replacing the IP addresses with the DNS name of the server where the load balancer software is installed.

   iv. Click **Settings > Application** and update the forward and logout URLs by replacing the IP addresses with the DNS name of the server where the load balancer software is installed.

d. To update the SSPR information on Node1, launch the Configuration utility located at **C:\NetIQ\idm\apps\UserApplication\configupdate.bat**.

   In the window that opens, click **SSO clients > Self Service Password Reset** and enter values for **Client ID**, **Password**, and **OSP Auth redirect URL** parameters.

   **NOTE:** Verify that the values for these parameters are updated in Node2.

7. Perform the following configuration tasks on the cluster nodes:

   a. Restart Tomcat on all the cluster nodes.

   b. To change the Change my password link, see “Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment” on page 68.

   c. Verify that the Forgot Password link and Change my password links are updated with the SSPR IP address on Node2.

   **NOTE:** If the Change Password and Forgot Password links are already updated with the SSPR IP address, no changes are required.

8. In Node1, stop Tomcat and generate a new **osp.jks** file by specifying the DNS name of the load balancer server by using the following command:

   ```
   C:\NetIQ\Common\JRE\bin\keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass <password> -keypass <password> -alias osp -validity 1800 -dname "cn=<loadbalancer IP/DNS>"
   ```

   **NOTE:** Ensure that the key password is the same as the one provided during OSP installation. Alternatively, this can also be changed using Configuration Update utility including the keystore password.
9. (Conditional) To verify if the osp.jks file is updated with the changes, run the following command:

```
C:\NetIQ\Common\JRE\bin\keytool -list -v -keystore osp.jks -storepass changeit
```

10. Take backup of the original osp.jks file located at C:\NetIQ\idm\apps\osp\ and copy the new osp.jks file to this location. The new osp.jks file was created in Step 8.

11. Copy the new osp.jks file located at from Node1 to other User Application nodes in the cluster.

12. On each clustered node,
   a. Navigate to the C:\netiq\idm\apps\sites directory and edit the ServiceRegistry.json file to add the load balancer details.

   ```json
   {"serviceRegisteries": [{"serviceID": "IDM", "restUrl": "https://<DNS of the load balancer>:8543/IDMProv"}]
   }
   ```

   b. Navigate to the C:\netiq\idm\apps\sites directory and edit the config.ini file to add the load balancer DNS and port number.

   ```ini
   OSPIssuerUrl=https://<DNS of the load balancer>:8543/osp/a/idm/
   auth/oauth2
   OSPRedirectUrl=https://<DNS of the load balancer>:8600/forms/
   oauth.html
   ClientID=forms
   OSPLogoutUrl=https://<DNS of the load balancer>:8543/osp/a/idm/
   auth/app/logout
   ```

13. Launch the Configuration utility in Node1 and change all of the URL settings, such as URL link to landing page and OAuth redirect URL to the load balancer DNS name under the SSO Client tab.
   a. Save the changes in the Configuration utility. Check the ism-configuration properties file for the changes and modify if any URLs are still pointing to Node 1 DNS and port.
   b. To reflect this change in all other nodes of the cluster, copy the ism-configuration properties file located in C:\NetIQ\IDM\apps\tomcat\conf from Node1 to other User Application nodes in the cluster.

**NOTE:** You copied the ism.properties file from Node1 to the other nodes in the cluster. If you specified custom installation paths during the User Application installation, ensure that referential paths are corrected by using Configuration update utility in the cluster nodes.

In this scenario, both OSP and User Application are installed on the same server; therefore, the same DNS name is used for redirect URLs.

If OSP and User Application are installed on separate servers, change the OSP URLs to a different DNS name pointing to the load balancer. Do this for all the servers where OSP is installed. Doing this ensures that all OSP requests are dispatched through load balancer to the OSP cluster DNS name. This involves having a separate cluster for OSP nodes.
14. Perform the following actions in the `setevn.sh` file located at `/TOMCAT_INSTALLED_HOME/bin/` directory:
   a. To ensure that the `mcast_addr` binding is successful, JGroups requires that the `preferIPv4Stack` property be set to `true`. To do so, add the JVM property `-Djava.net.preferIPv4Stack=true` in the `setenv.sh` file in all nodes.
   b. Add `^-Dcom.novell.afw.wf.Engine-id=Engine1` in the `setenv.sh` file on Node1. Similarly, add a unique engine name for each node of the cluster. For example, for Node2, you can add the engine name as Engine2.

15. Enable clustering in the User Application.
   a. Start Tomcat on Node1.
      Do not start any other servers.
   b. Log in to the User Application as a User Application administrator.
   c. Click the Configuration > Caching and Cluster option.
      The User Application displays the Caching Management page.
   d. Click Cluster Cache Configuration and select True for the Cluster Enabled property.
   e. Click Save.
   f. Restart Tomcat.

   **NOTE:** If you have selected Enable Local settings, repeat this procedure for each server in the cluster.
   The User Application cluster uses JGroups for cache synchronization across nodes using default UDP. In case you want to change this protocol to use TCP, see Configuring User Application to use TCP.

16. Enable the permission index for clustering. For more information see “Enabling the Permission Index for Clustering” on page 222.

17. Enable Tomcat cluster.
   Open the Tomcat `server.xml` file from `/TOMCAT_INSTALLED_HOME/conf/` and uncomment this line in this file on all the cluster nodes:
   ```xml
   <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
   ```
   For advanced Tomcat clustering configuration, follow the steps from the Apache documentation website.

18. Restart Tomcat on all the nodes.

19. Configure the User Application Driver for clustering.
   In a clustered environment, you can use a single User Application driver with multiple instances of the User Application. The driver stores various kinds of information (such as workflow configuration and cluster information) that is application-specific. You must configure the driver to use the host name or IP address of the dispatcher or load balancer for the cluster.
   a. Log in to the instance of iManager that manages your Identity Vault.
   b. In the navigation frame, select Identity Manager.
   c. Select Identity Manager Overview.
   d. Use the search page to display the Identity Manager Overview for the driver set that contains your User Application driver.
e. Click the round status indicator in the upper right corner of the driver icon:
   f. Select **Edit Properties**.
   g. For **Driver Parameters**, change **Host** to the host name or IP address of the Load Balancer.
   h. Click **OK**.
   i. Restart the driver.

20. To change the URL of Roles and Resource Service Driver, repeat steps from 19a to 19f and click **Driver Configuration** and update the **User application URL** with the load balancer DNS name.

21. Ensure session stickiness is enabled for the cluster created in the load balancer software for the User Application nodes.

Most loadbalancers provide a healthcheck feature for determining whether an HTTP server is up and listening. The User Application contains a URL that can be used for configuring HTTP healthchecks on your loadbalancer. The URL is:

```
http://<NodeIP>:port/IDMProv/jsps/healthcheck.jsp
```

## Enabling the Permission Index for Clustering

This section provides instructions for enabling the permission index for clustering.

1. Log in to iManager in the first node of the cluster and navigate to **View Objects**.
2. Under **System**, navigate to the driver set containing the **User Application driver**.
3. Select **AppConfig > AppDefs > Configuration**.
4. Select the XMLData attribute and set the **com.netiq.idm.cis.clustered property** to **true**.
   
   For example:
   ```xml
   <property>
   <key>com.netiq.idm.cis.clustered</key>
   <value>true</value>
   </property>
   ```
5. Click **OK**.
Troubleshooting

This section provides useful information for troubleshooting problems with installing Identity Manager. For more information about troubleshooting Identity Manager, see the guide for the specific component.

Troubleshooting Identity Manager Engine

The following table lists the issues you might encounter and the suggested actions for working on these issues. If the problem persists, contact your NetIQ representative.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Identity Manager Engine fails to start when the eDirectory initialization process is in progress. This issue is mostly observed when the eDirectory DIB is very large.</td>
<td>Perform the following steps to workaround this issue:</td>
</tr>
<tr>
<td></td>
<td>1. Create a system environment variable called as $SLEEP_BEFORE_ENGINE_STARTUP$ and set the value of the variable from 0 to 600. The value is denoted in seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you provide an invalid value or a value greater than 600, the value defaults to 600.</td>
</tr>
<tr>
<td></td>
<td>2. Restart eDirectory.</td>
</tr>
<tr>
<td></td>
<td>3. (Conditional) Check the dhost.log to view the messages and logs.</td>
</tr>
<tr>
<td>In a multi-server environment, an unrecognized extended exception is displayed.</td>
<td>Ensure that the primary server has a read-write partition for the secondary server:</td>
</tr>
<tr>
<td></td>
<td>1. Log in to iManager.</td>
</tr>
<tr>
<td></td>
<td>2. Click Roles and Tasks &gt; Partitions and Replicas &gt; Replica View.</td>
</tr>
<tr>
<td></td>
<td>3. Select the secondary server.</td>
</tr>
<tr>
<td></td>
<td>4. Assign read-write permissions to the server.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Ensure that you have added the secondary server in the driver set.</td>
</tr>
</tbody>
</table>

In a multi-server environment, an unrecognized extended exception is displayed.
## Troubleshooting the Identity Applications and RBPM Installation

The following table lists the issues you might encounter and the suggested actions for working on these issues. If the problem persists, contact your NetIQ representative.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Actions</th>
</tr>
</thead>
</table>
| The **Roles** and **Self tasks** widgets on the Dashboard page do not display any data. If you check in your browser’s Console, a 404 error is displayed. This issue is observed when the default `IDMProv` deployment context is changed to a custom context. | To resolve this issue, you must change the REST API URL on the impacted widgets. Perform the following steps:  
1. Log in to the Identity Manager Dashboard as an administrator.  
2. Navigate to the Dashboard page and click Manage Dashboard.  
3. To edit the widget configuration in the **Roles** widget:  
   a. Click .  
   b. In the **URL** field, change the default `IDMProv` context to a custom context as follows: `<custom-context>/rest/access/assignments/advanced?nextIndex=1&sortBy=name&sortOrder=ASC&forceRefresh=true&searchScope=role&size=20`  
   Where, `<custom-context>` is the context that you are using in your Identity Manager deployment.  
   c. Click Apply.  
4. To edit the widget configuration in **Self tasks** widget:  
   a. Click .  
   b. In the **URL** field, change the default `IDMProv` context to a custom context as follows: `<custom-context>/rest/access/tasks/list?fromIndex=1&size=10&q=*&sortBy=createTime&assignedTo=assignedTo&recipient=recipientAsMe&expireUnit=weeks&expireWithin=&proxyUser=&assignStatus=&delegatedTasks=false&status=`  
   c. Click Apply.  
5. Click **Edit Done**. |
### Troubleshooting

<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Actions</th>
</tr>
</thead>
</table>
| When Identity Applications installed in a cluster is upgraded and Tomcat is restarted, clustering does not work as expected. | Perform the following actions in all the nodes of the cluster:  
1. Navigate to the server.xml file located at the C:\NetIQ\IDM\apps\tomcat\conf folder.  
2. Uncomment the following line in the server.xml.  
   `<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>`  
3. Restore all the custom configurations from the backed up Tomcat directory.  
4. Restart Tomcat. |
| The upgrade process does not set the default Identity Applications Administrative account as cn=uaadmin.ou=sa.o=data. The following error is logged to the catalina.out file. | 1. Navigate to the setenv.bat file and change the value for -Dncpclient_req_timeout property to 1150 in the CATALINA_OPTS entry.  
2. Restart Tomcat. |

AuthorizationManagerService [RBPM] Error occurred calculating effective rights for attribute: nrfAccessMgrRevokeRole on object:  

```bash  
@com.novell.idm.security.authorization.LdapRightsUtil.getPropertyRights(LdapRightsUtil.java:152)  
Unable to fetch roles from edirectory in the predefined time set. 
```

You want to modify one or more of the following the Identity Applications configuration settings created during installation:  
- Identity Vault connections and certificates  
- E-mail settings  
- Identity Manager Engine User Identity and User Groups  
- Access Manager or iChain settings

Run the configuration utility independent of the installer.  
Run the following command from the installation directory (by default, C:\NetIQ\idm\apps\UserApplication\):  
```
configupdate.bat
```
<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Tomcat causes the following exception: port 8180 already in use</td>
<td>Shut down any instances of Tomcat (or other server software) that might already be running. If you reconfigure Tomcat to use a port other than 8180, edit the config settings for the User Application driver.</td>
</tr>
<tr>
<td>When Tomcat starts, the application reports it cannot find trusted certificates.</td>
<td>Ensure that you start Tomcat by using the JDK specified during the installation of the Identity Applications.</td>
</tr>
<tr>
<td>Cannot log in to the portal admin page.</td>
<td>Ensure that the Identity Applications Administrator account exists. This account is not the same as your iManager administrator account.</td>
</tr>
<tr>
<td>Cannot create new users even with administrator account.</td>
<td>The Identity Applications Administrator must be a trustee of the top container and should have Supervisor rights. You can try setting the Identity Applications Administrator’s rights equivalent to the LDAP Administrator’s rights (using iManager).</td>
</tr>
<tr>
<td>Starting application server throws keystore errors.</td>
<td>Your application server is not using the JDK specified during the installation of the Identity Applications. Use the keytool command to import the certificate file: keytool -import -trustcacerts -alias aliasName -file certFile -keystore ../lib/security/cacerts -storepass changeit</td>
</tr>
<tr>
<td></td>
<td>✔ Replace aliasName with a unique name of your choice for this certificate.</td>
</tr>
<tr>
<td></td>
<td>✔ Replace certFile with the full path and name of your certificate file.</td>
</tr>
<tr>
<td></td>
<td>✔ The default keystore password is changeit (if you have a different password, specify it).</td>
</tr>
<tr>
<td>Email notification not sent.</td>
<td>Run the configupdate utility to check whether you supplied values for the following Identity Applications configuration parameters: Email From and Email Host.</td>
</tr>
<tr>
<td></td>
<td>Run the following command from the installation directory (by default, C:\NetIQ\idm\apps\UserApplication): configupdate.bat</td>
</tr>
</tbody>
</table>

**Troubleshooting Installation and Uninstallation**

The following table lists the issues you might encounter and the suggested actions for working on these issues. If the problem persists, contact your NetIQ representative.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Manager authorizes and securely communicates with its</td>
<td>To fix this issue, enable CRL distribution point checking by setting the –</td>
</tr>
<tr>
<td>components using digital certificates. The Identity Vault certificates</td>
<td>Dcom.sun.security.enableCRLDP property to true.</td>
</tr>
<tr>
<td>must be imported into the idm.jks and tomcat.ks keystore files.</td>
<td></td>
</tr>
<tr>
<td>However, when attempting to access Identity Applications after</td>
<td></td>
</tr>
<tr>
<td>importing the certificates, you might hit the following error:</td>
<td></td>
</tr>
<tr>
<td>javax.net.ssl.SSLHandshakeException: PKIX path validation failed:</td>
<td>To set the property, perform the following actions:</td>
</tr>
<tr>
<td>revocation status.</td>
<td>2. Go to the setenv.sh file located in the Tomcat’s bin folder. For example,</td>
</tr>
<tr>
<td>The certificates are validated by checking the Certificate Revocation</td>
<td>C:\NetIQ\idm\apps\tomcat\bin\setenv.bat.</td>
</tr>
<tr>
<td>Lists (CRLs) specified by the CRL Distribution Point (CDP) field to</td>
<td>3. Add the property – Dcom.sun.security.enableCRLDP=true in CATALINA_OPTS as:</td>
</tr>
<tr>
<td>determine whether the certificate has been revoked or not. The CRLDPs</td>
<td>export CATALINA_OPTS=&quot;-Dcom.sun.security.enableCRLDP=true&quot;</td>
</tr>
<tr>
<td>are available in both the root certificate and the intermediate</td>
<td>4. Start Tomcat.</td>
</tr>
<tr>
<td>certificates present in the keystore files tomcat.ks and idm.jks.</td>
<td>(Conditional) The following steps apply to Identity Manager 4.8.5 and later.</td>
</tr>
<tr>
<td>Certificate revocation checking, however, is disabled by default.</td>
<td>1. Log in to the server where Identity Applications is upgraded to 4.8.5 version.</td>
</tr>
<tr>
<td>As a result, the PKIX trust manager is unable to determine the</td>
<td>2. Navigate to the C:\NetIQ\IDM\apps\tomcat\conf location.</td>
</tr>
<tr>
<td>revocation status of the certificates.</td>
<td>3. Open the ism-configuration.properties file in a text editor.</td>
</tr>
<tr>
<td>After upgrading Identity Manager, logging in to Identity Manager</td>
<td>4. At the end of the file, add the following property:</td>
</tr>
<tr>
<td>Dashboard is extremely slow for non-admin users. There is a</td>
<td>DirectoryService/realms/jndi/params/USE_NESTED_GROUPS=false</td>
</tr>
<tr>
<td>significant delay in loading the Applications and the Dashboard</td>
<td>5. Save the file and restart Tomcat.</td>
</tr>
<tr>
<td>pages.</td>
<td></td>
</tr>
<tr>
<td>This issue occurs due to the nested group search, which is enabled</td>
<td></td>
</tr>
<tr>
<td>by default. The application will look for the permissions inherited</td>
<td></td>
</tr>
<tr>
<td>by the logged-in user via the nested group membership, regardless of</td>
<td></td>
</tr>
<tr>
<td>whether there are any nested groups in the environment.</td>
<td></td>
</tr>
</tbody>
</table>
After upgrading Identity Applications to 4.8.x version, you are unable to login to the Identity Applications Dashboard. This issue occurs when the Identity Vault truststore path is not updated to proper keystore (cacerts) file location during the Identity Applications upgrade. The following exception is logged to the catalina.out file:

com.netiq.idm.auth.oauth.AuthenticationException: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path validation failed: sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, OU=idm, O=***, L=***, ST=***, C=**" is not a CA certificate

Identity Applications uses JAVA_HOME environment variable which is set to <install_path>\Common\JRE. When the truststore path is not set to cacerts file at JAVA_HOME, the SSL communication fails resulting in SSL error associated with 'TrustAnchor' (Trust anchor is used as enhanced java security check for SSL certificates).

After you upgrade Identity Manager in a distributed environment to 4.8.1 version, login to the Identity Applications fails. The following error message is displayed:

Your login process did not complete successfully.

Logging to the Identity Applications requires trust anchor certificates for establishing a secure connection between the Identity Applications and the OSP. A trust anchor certificate must include the Basic Constraints extension with the Subject Type set to CA. Identity Manager makes use of the property jdk.security.allowNonCaAnchor to validate the trust anchors in the certificate. By default, this property is set to false. Therefore, when the trust anchors are not found in the certificates, the connection between Identity Applications and OSP cannot be established and the login fails. You will also notice the following exception in the idm-osp.log file:

sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, L=***, O=***" is not a CA certificate

To resolve this issue, perform the following actions:

1. Stop the Tomcat service.
2. Log in to the Identity Applications server and launch the configupdate utility located at <install_path>\idm\apps\configupdate.
3. In User Application tab, go to Identity Vault Certificates and ensure that the Truststore path is set to <install_path>\Common\JRE\lib\security\cacerts.
4. Start the Tomcat service.

To resolve this issue, you must satisfy either of the following conditions:

- Ensure that the certificates used to establish a secure connection between the Identity Applications and the OSP are trusted CA certificates with proper Basic Constraints extension.
- In case of self signed certificates and custom certificates that are trusted by the clients, you can change the property jdk.security.allowNonCaAnchor to allow non CA certificates without Basic Constraints extension. Perform the following actions to modify the Java security settings:
  1. Navigate to the C:\NetIQ\idm\apps\jre\lib\security\java.security directory.
  2. Set the value of the property jdk.security.allowNonCaAnchor=true.
  3. Save the file.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>After upgrading to Identity Applications 4.8.1 version, you are not able to open forms while requesting for permissions in the Identity Applications Dashboard.</td>
<td>To resolve this issue, perform the following steps:</td>
</tr>
<tr>
<td></td>
<td>1. Press Windows + R on your keyboard, type services.msc and select OK to open the Windows Services interface.</td>
</tr>
<tr>
<td></td>
<td>2. Search for the service names, NetIQ Nginx Service and NetIQ IGA Form Renderer Service. Right-click the service and select the Restart option.</td>
</tr>
<tr>
<td></td>
<td>The Identity Applications uses NGNIX service for rendering forms in the Identity Applications Dashboard.</td>
</tr>
<tr>
<td>After upgrading Identity Applications or Identity Reporting to the 4.8 version, multiple entries of PostgreSQL are displayed in the Control Panel.</td>
<td>Uninstall the previous versions of PostgreSQL from the Control Panel.</td>
</tr>
<tr>
<td>Uninstallation process reports as incomplete but the log file shows no failures.</td>
<td>The process failed to delete the netiq directory that contains the installation files by default. You can delete the directory if you have removed all NetIQ software from your computer.</td>
</tr>
<tr>
<td>After you upgrade Identity Manager, the following property is added to the ism-configuration.properties file:</td>
<td>Comment out the property in the ism-configuration.properties file and restart Tomcat. It does not cause any functionality loss.</td>
</tr>
<tr>
<td>com.netiq.idm.osp.ldap.admin-dn = cn=admin,ou=sa,o=system</td>
<td></td>
</tr>
<tr>
<td>After you upgrade Identity Manager, the following SSPR property is added to the ism-configuration.properties file, even if you do not have SSPR in your deployment:</td>
<td>Comment out the property in the ism-configuration.properties file and restart Tomcat. It does not cause any functionality loss.</td>
</tr>
<tr>
<td>com.netiq.sspr.redirect.url = https://<em><strong>SSPR_IP</strong></em>:_<strong>SSPR_TOMCAT_HTTPS_PORT</strong>/sspr/public/oauth</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting Login

The following table lists the issues you might encounter and the suggested actions for working on these issues. If the problem persists, contact your NetIQ representative.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Actions</th>
</tr>
</thead>
</table>
| Unable to start Tomcat after Identity Manager upgrade. You will notice few exceptions in tomcat logs and a communication failure between the workflow engine and the Identity Vault. | 1. Log in to iManager.  
3. Select the SSL CertificateDNS check box and click Export.  
4. In the Certificates drop-down list, select the SSL CertificateDNS.  
5. Clear the Export private key check box. Ensure that the Export format is set to DER.  
6. Click Next > Save the exported certificate to download the certificate in your system.  
7. Log in to the Identity Applications server.  
8. Stop Tomcat.  
9. Navigate to C:\NetIQ\Common\JRE\bin\ directory and import the certificate to idm.jks file using the following command:  
   <Installed_path>\NetIQ\Common\JRE\bin\keytool -import -trustcacerts -alias <certificate_alias_name> -keystore idm.jks -file <certificate_file_downloaded>  
10. Restart Tomcat.                                                                 |
| After upgrading Identity Manager from 4.7.4 to 4.8, the Tomcat service does not come up and no errors are reported in the log files. This issue occurs when the Heartbeat timer is not updated properly in afenginestate table in the igaworkflow database. | To resolve this issue, log in to a database admin tool such as pgAdmin. Run the following query to manually update the Heartbeat timer in afenginestate table in the igaworkflow database.  
update afenginestate set heartbeat=now()::timestamp; |
<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>When Identity Applications and Identity Reporting are installed on the same server and you perform configuration changes using the configuration update utility located at &lt;reporting install folder&gt;\bin directory, the Identity Manager Dashboard fails to launch. The following error is reported in catalina.out log file: EboPortalBootServlet [RBPM] ++++WARNING!!!!: This portal application context, IDMProv, does not match the portal.context property set in the PortalService-conf/config.xml file. Only one portal per database is allowed. Data has been loaded using the previous portal context. To correct this you must revert back to the previous portal name of, NoCacheFilter, please consult the documentation.</td>
<td>For any configuration changes, use the configuration update utility located at C:\NetIQ\idm\apps\UserApplication directory.</td>
</tr>
<tr>
<td>User is unable to login in large scale environment (&gt;2 million objects)</td>
<td>Add an index for <code>mail</code> (Internet Mail Address) attribute with the rule set as <code>Value</code> in both eDirectory master and replica servers.</td>
</tr>
<tr>
<td>When you sign out from Identity Applications page, SSPR shows an error 5053 ERROR_APP_UNAVAILABLE.</td>
<td>Ignore this error. It does not cause any functionality loss.</td>
</tr>
<tr>
<td>Challenge Responses are not prompted at the first login to the Identity Applications.</td>
<td>1. Ensure that the SSPR server has a certificate created using FQDN. 2. Log in to the Identity Application server and launch ConfigUpdate utility (&lt;installation_path&gt;\apps\UserApplication). 3. Navigate to SSO Clients &gt; Self Service Password Reset and make sure the settings are correct. If SSPR is installed on a separate server, make sure that the SSPR certificate is imported into idm.jks located in the Identity Applications server at \netiq\idm\apps\tomcat\conf.</td>
</tr>
<tr>
<td>Issue</td>
<td>Suggested Actions</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Browser displays a blank page when SSPR URL is accessing.</td>
<td>This occurs when SSPR is not properly configured with OSP. The SSPR log shows the following information:</td>
</tr>
<tr>
<td></td>
<td>1. Verify that the Tomcat server where OSP is running has a valid certificate created using FQDN. Log in to the Identity Applications server and launch ConfigUpdate utility. Navigate to SSO Clients &gt; Self Service Password Reset and make sure the settings are correct.</td>
</tr>
<tr>
<td></td>
<td>2. Log in to SSPR by overriding the OSP login method. (for example, https://&lt;sspr sserv er ip&gt;:\port&gt;/sspr/private/Login?sso=false)</td>
</tr>
<tr>
<td></td>
<td>3. Navigate to Configuration Editor in the top right corner of the page.</td>
</tr>
<tr>
<td></td>
<td>4. Specify Configure Password, then click Sign In.</td>
</tr>
<tr>
<td></td>
<td>5. Navigate to LDAP &gt; LDAP Directories &gt; Default &gt; Connection.</td>
</tr>
<tr>
<td></td>
<td>6. If the LDAP certificate is not correct, click Clear.</td>
</tr>
<tr>
<td></td>
<td>7. To reimport the certificate, click Import From Server.</td>
</tr>
<tr>
<td></td>
<td>8. Navigate to Settings &gt; Single Sign On (SSO)Client &gt; OAuth and verify that the certificate under OAUTH Web Service Server Certificate is correct.</td>
</tr>
<tr>
<td></td>
<td>9. If the certificate is not correct, click Clear.</td>
</tr>
<tr>
<td></td>
<td>10. To reimport the certificate, click Import From Server.</td>
</tr>
</tbody>
</table>

**Troubleshooting SSPR Page Request Error**

The following table lists the issues you might encounter and the suggested actions for working on these issues. If the problem persists, contact your NetIQ representative.
For general issues encountered during authentication or logging in to the identity applications, see the NetIQ Identity Manager - Administrator’s Guide to the Identity Applications.

## Troubleshooting .NET Remote Loader Not Starting Issue on Windows 2016

The following table lists the issues you might encounter and the suggested actions for working on these issues. If the problem persists, contact your NetIQ representative.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is a random issue. It might occur if the font settings of .NET Remote Loader’s command prompt are not same as the default settings of the host operating system.</td>
<td>Change the command prompt settings to match the system default settings by deleting the HKEY_CURRENT_USER\Console registry key and then restart the server.</td>
</tr>
</tbody>
</table>

## Troubleshooting 502 Bad gateway while loading the forms in Azure deployment

The following table lists the issues you might encounter and the suggested actions for working on these issues. If the problem persists, contact your NetIQ representative.
After deploying the IDM 4.8 components on Azure environment. In IDM dashboard, when you click on helpdesk ticket or when you try approve any task you might see the following error.

502 - Web server received an invalid response while acting as a gateway or proxy server.

Perform the following steps to resolve this issue:

1. Navigate to `Nginx\conf` location in your system.
   
   For example, `C:\NetIQ\Common\Nginx\conf`

2. In the `nginx.conf` file,
   
   a. Add the `error_page 404 =200 /404.html` below this line `error_page 502 /502.html;`.
   
   b. Set the `proxy_intercept_errors off;` to `proxy_intercept_errors on;`