NetIQ® Identity Manager

Setup Guide for Windows

March 2018

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/.

Contents

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 community.netiq.com.

Planning to Install Identity Manager

This section guides you through planning your Identity Manager installation. If you want to install a configuration that is not identified in this section, or if you have any questions, contact NetIQ Technical Support (https://www.netiq.com/support/).

1 Planning Overview

This section helps you plan the installation process for Identity Manager. You must install the components in a specific order because the installation program of some components requires access to previously installed components. For example, you should install and configure the Identity Manager Engine before installing Identity Applications.

- "Implementation Checklist" on page 19
- "Recommended Installation Scenarios and Server Setup" on page 21
- "Meeting System Requirements" on page 22

Implementation Checklist

Use the following checklist to plan, install, and configure Identity Manager.

If you are upgrading from a previous version of Identity Manager, do not use this checklist. For information about upgrading, see Part VII, "Upgrading Identity Manager," on page 245.

	Checklist Items
□	1. Review the product architecture information to learn about Identity Manager components. For more information, see How Identity Manager Works in *NetIQ Identity Manager Overview and Planning Guide*.
□	2. Review the Identity Manager licensing information. For more information, see Understanding Licensing and Activationin *NetIQ Identity Manager Overview and Planning Guide*.
□	3. Ensure that the computers on which you install Identity Manager and its components meet the specified hardware and software requirements. For more information, see "Meeting System Requirements" on page 22. **NOTE:** Identity Manager supports Sentinel Log Management for Identity Governance and Administration (Sentinel Log Management for IGA) installation only on a Linux server. If you want to use Sentinel Log Management for IGA in your environment, see prerequisites and system setup need for this installation in Installing Sentinel Log Management for Identity Governance and Administration in the *NetIQ Identity Manager Setup Guide for Linux*. However, you can use a different auditing service if your identity solution is Windows only.
□	4. If there was a previous installation of Identity Manager, ensure that there are no files or system settings remaining from a previous installation. For more information, see Chapter 28, "Uninstalling Identity Manager Components," on page 315.
□	5. Determine the type of deployment suitable for your environment based on the features you want to implement. For more information, see Identity Manager Deployment Configurations in *NetIQ Identity Manager Overview and Planning Guide*.

	Checklist Items
❑	6. Review the latest Identity Manager release notes to understand the new functionality and the known issues. For more information, see the release notes at the Identity Manager 4.7 documentation website (https://www.netiq.com/documentation/identity-manager-47/).
❑	7. Determine whether you can run the installation programs in your preferred language. For more information, see Understanding Identity Manager Localization in *NetIQ Identity Manager Overview and Planning Guide*.
❑	8. Locate the files for installation. For more information, see Where to Get Identity Manager in *NetIQ Identity Manager Overview and Planning Guide*. **IMPORTANT:** For a hassle-free installation, do not run any CPU-intensive applications while installing the Identity Manager components. You must stop Windows services such as Windows Modules Installer and Windows Update before starting the Identity Manager installation and start them only after completing the installation.
❑	9. Install and configure Identity Manager components. For more information, see the following sections depending on Identity Manager edition you are installing: ◆ Installing Identity Manager Engine ◆ Installing Identity Applications ◆ Installing Identity Reporting ◆ Installing Designer ◆ Installing Analyzer
❑	10. Ensure that you have the appropriate credentials required to install the Identity Manager components on your servers and the accounts that you might create during the installation.
❑	11. Perform any post-installation tasks for the components to be fully functional. For more information, see Chapter 20, “Post-Installation Tasks,” on page 239.
❑	12. (Optional) To review the ports used by the Identity Manager components, see Understanding Identity Manager Communication in the *NetIQ Identity Manager Security Guide*.
❑	13. (Optional) The components are installed in pre-defined locations. For more information, see Locating the Executables and Default Installation Paths in *NetIQ Identity Manager 4.7 Release Notes*.

To install Identity Manager in a cluster, ensure that your environment meets the requirements. For more information, see Part X, “Deploying Identity Manager for High Availability,” on page 327.

You can deploy Identity Manager on Microsoft Azure cloud. NetIQ provides the flexibility of deploying Identity Manager on on-premises and cloud. Ensure that you review the recommended configuration details before beginning the deployment. For more information, see Chapter 24, “Planning and Implementation of Identity Manager on Microsoft Azure,” on page 291 and Chapter 25, “Example Scenarios of Hybrid Identity Manager,” on page 299.

Recommended Installation Scenarios and Server Setup

When you perform a standalone installation, you should install the components in a specific order and on specific servers. The installation programs for some components require information about previously installed components.

This section helps you determine the installation order and server setup in a single-server or in a distributed environment.

- "Deciding When to Install SLM for IGA" on page 21
- "Considerations for Installing in a Distributed Setup" on page 21

Deciding When to Install SLM for IGA

Sentinel is the preferred audit event destination for Identity Manager. Identity Manager provides event forwarding capabilities to Sentinel by configuring Sentinel Link using Sentinel Event Source Management (ESM). If you are already using Sentinel for auditing or as an integration framework for tracking identities, you might choose to use your existing Sentinel for auditing events instead of installing SLM for IGA.

Regardless of whether you choose to reuse your existing Sentinel server or perform a new installation of SLM for IGA shipped with Identity Manager, you must configure the Sentinel server as a source of audit data. You do this by creating a data synchronization policy on the Sentinel server in the Identity Manager Data Collection Services page for auditing events. For more information, see About the Data Sync Policies tab in the *Administrator Guide to NetIQ Identity Reporting*.

If you perform a new installation of SLM for IGA, install the components in the following order:

1. Identity Vault (eDirectory)
2. iManager
3. Identity Manager Engine
4. Designer
5. Remote Loader
6. Tomcat
7. OSP
8. SSPR
9. Identity Applications (not required for Standard Edition)
10. Identity Reporting
11. (Optional) Analyzer
12. SLM for IGA (can be installed only on a Linux system)

Considerations for Installing in a Distributed Setup

In a typical production environment, you might install Identity Manager on seven or more servers, as well as on client workstations. For example:

Computer setup	Component setup
All in One (Only recommended for demo / POC setup)	Install and configure all components on one computer (Identity Manager Engine, Identity Applications, Identity Reporting, OSP, SSPR, Identity Applications Database, and Reporting Database) and Sentinel Log Management for IGA on a separate computer.
Distributed setup	
Server 1	◆ Identity Vault ◆ Identity Manager Engine
Server 2	Identity Applications and OSP (can be clustered)
Server 3	Identity Reporting (OSP)
Server 4	SSPR
Servers 5 and 6	Identity Manager databases for: ◆ Identity applications ◆ Identity Reporting
Server 7	Sentinel Log Management for IGA

Meeting System Requirements

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.

For information about the recommended hardware, supported operating systems, and supported virtual environments, see the NetIQ Identity Manager Technical Information website.

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

2 Considerations for Installing Identity Manager Components

This section provides the prerequisites, considerations, and system setup needed to install the Identity Manager components.

- "Understanding the Installation Process" on page 23
- "Installation Order" on page 23
- "Using Self-Service Password Management in Identity Manager" on page 24
- "Using Single Sign-on Access in Identity Manager" on page 26

Understanding the Installation Process

NetIQ provides standalone installation programs for Identity Manager components to give you more flexibility in setting up your environment. For example, many of the Identity Manager components are data-intensive, such as the Identity Vault, and should be installed on separate servers.

The standalone installation process provides the following capabilities:

- Allows you to customize component settings, including the tree structure in the Identity Vault
- Allows you to install in distributed and clustered environments
- Allows you to select the drivers and create driver sets that you want to add to your identity management solution
- Allows you to select the iManager plug-ins that you want to add to your identity management solution
- Allows you use a non-administrator account to install some components
- Supports multiple database platforms
- Uses Apache Tomcat for all supported operating systems
- Creates a supported production environment
- Can be used to upgrade a previous version of Identity Manager

For best results, run the standalone installation programs in the order specified by your identity management solution. For more information, see "Recommended Installation Scenarios and Server Setup" on page 21.

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) (can be installed only on Linux computers)

- Identity Vault (eDirectory)
- iManager
- Identity Manager Engine
- Designer for Identity Manager
- Remote Loader
- Tomcat
- OSP
- SSPR
- Identity Applications components (only for Advanced Edition)
- Identity Reporting components
- Analyzer for Identity Manager

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

Using Self-Service Password Management in Identity Manager

Identity Manager includes NetIQ Self Service Password Reset (SSPR) to help users who have access to the identity applications to reset their passwords without administrative intervention. The installation process enables SSPR by default when you install or upgrade to the latest version of Identity Manager. In a new installation, SSPR uses a proprietary protocol for managing authentication methods. However, after an upgrade, you can instruct SSPR to use the NetIQ Modular Authentication Services (NMAS) that Identity Manager traditionally has used for its legacy password management program.

Depending on whether you want to use complex password management, you can configure one of the following providers:

SSPR

NetIQ Self Service Password Reset is the default option when you install or upgrade Identity Manager. For more information, see “Understanding the Default Self-Service Process” on page 25.

Legacy Provider for Password Management

Uses the password management process from Identity Manager 4.0.2, which supports the use of multiple password policies. For more information, see “Understanding the Legacy Password Management Provider” on page 25.

Third-Party Provider Password Management

You can use an third-party program for managing forgotten passwords. You need to modify some configuration settings for Identity Manager. For more information, see “Using an External System for Forgotten Password Management” on page 159.

Understanding the Default Self-Service Process

SSPR automatically integrates with the single sign-on process for the identity applications and Identity Reporting. It is the default password management program for Identity Manager, even when you do not install SSPR. When a user requests a password reset, SSPR requires the user to answer the challenge-response question. If the answers are correct, SSPR responds in one of the following ways:

- Allow users to create a new password
- Create a new password and send it to the user
- Create a new password, send it to the user, and mark the old password as expired.

You configure this response in the SSPR Configuration Editor. After upgrading to a new version of Identity Manager, you can configure SSPR to use the NMAS method that Identity Manager traditionally has used for password management. However, SSPR does not recognize your existing password policies for managing forgotten passwords. To continue using your policies, see "Understanding the Legacy Password Management Provider" on page 25.

You also can configure SSPR to use its proprietary protocol instead of NMAS. If you make this change, you cannot return to using NMAS without resetting your password policies.

For more information about...	See...
Installing SSPR	"Installing Password Management for Identity Manager" on page 107
Configuring password management for the identity applications	"Using Self Service Password Reset for Forgotten Password Management" on page 156
Managing and configuring SSPR	*NetIQ Self Service Password Reset Administration Guide*

Understanding the Legacy Password Management Provider

NOTE: The Legacy Password Self-Service feature of the User Application is deprecated with this release. NetIQ strongly recommends that you start using SSPR for all password-specific tasks. The installation process enables SSPR by default.

When you upgrade from an older version of Identity Manager, the identity applications default to SSPR as the password management program. SSPR can use the NMAS method that Identity Manager traditionally has used for password management. However, SSPR does not recognize your existing password policies for managing forgotten passwords. You can bypass SSPR and use the legacy password management provider.

When a user requests a password reset, the legacy provider compares the user's credentials to the password policies that you set. For example, it might requires the user to answer a challenge-response question. Based on the policy applied to that user, the program responds in one of the following ways:

- Resets the password
- Shows the password hint

- Emails the password hint to the user
- Emails a new password to the user

Use the legacy provider if your enterprise uses multiple or complex password policies. For example, your password policies are based on user roles. An intern might simply need a auto-generated password without a challenge response. For a manager who can access secure data, you might have more stringent requirements. This user might need to regularly reset the password. In both cases, you want the users to have self-service for password requests.

To use the legacy provider, modify the configuration settings for the identity applications after you install or upgrade Identity Manager. You do not need to reconfigure your password policies after the upgrade.

For more information about...	See...
Configuring Identity Manager to use the legacy provider	"Using the Legacy Provider for Forgotten Password Management" on page 158
Using the legacy provider for password management	*NetIQ Identity Manager Password Management Guide*

Using Single Sign-on Access in Identity Manager

To provide single sign-on access (SSO), Identity Manager uses the authentication service, NetIQ One SSO Provider (OSP). You must use OSP for the following components:

- Identity Applications Administration
- Identity Manager Dashboard
- Identity Reporting
- Self-Service Password Reset
- User Application

The `.iso` image for Identity Manager installation program include a method for installing OSP. For more information about installing OSP, see "Installing Password Management for Identity Manager" on page 107.

Understanding Authentication with One SSO Provider

OSP supports the OAuth2 specification and requires an LDAP authentication server. By default, Identity Manager uses Identity Vault (eDirectory). OSP can communicate other types of **authentication sources**, or **identity vaults**, to handle the authentication requests. You can configure the type of authentication that you want OSP to use: userID and password, Kerberos, or SAML. However, OSP does not support MIT-style Kerberos or SAP login tickets.

How do OSP and SSO work?

> If you use the Identity Vault as your authentication service and the specified containers in the Identity Vault have CNs and passwords, authorized users can log in to Identity Manager immediately after installation. Without these login accounts, only the administrator that you specify during installation can log in immediately.

When a user logs in to one of the browser-based components, the process redirects the user's name/password pair to the OSP service, which queries the authentication server. The server validates the user credentials. Then OSP issues an OAuth2 access token to the component and browser. The browser uses the token during the user's session to provide SSO access to any of the browser-based components.

If you use Kerberos or SAML, OSP accepts authentication from the Kerberos ticket server or SAML IDP then issues an OAuth2 access token to the component where the user logged in.

How does OSP work with Kerberos?

OSP and Kerberos ensure that users can log in once to create a session with one of the identity applications and Identity Reporting. If the user's session times out, authorization occurs automatically and without user intervention. After logging out, users should always close the browser to ensure that their sessions end. Otherwise, the application redirects the user to the login window and OSP reauthorizes the user session.

How do I set up Authentication and Single Sign-on Access?

For OSP and SSO to function, you must install OSP. Then specify the URLs for client access to each component, the URL that redirects validation requests to OSP, and settings for the authentication server. You can provide this information during installation or afterward with the RBPM configuration utility. You can also specify the settings for your Kerberos ticket server or SAML IDP.

For more information about configuring authentication and single sign-on access, see Configuring Single Sign-on Access in Identity Manager in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

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

Understanding the Keystore for One SSO Provider

Identity Manager uses a keystore that supports `http` and `https` communication between the OSP service and the authentication server. You create the keystore when you install OSP. You also create a password that the OSP service uses for authorized interactions with the authentication server. For more information, see "Installing Password Management for Identity Manager" on page 107.

Understanding Audit Events for One SSO Provider

OSP generates a single event to represent when a user logs in or out of the User Application or Identity Reporting:

- 003E0204 for login
- 003E0201 for logout

XDAS taxonomy then interprets these OSP events either as a successful login/logout or SOAP call to the User Application or as "other than success."

II

Installing Identity Manager Engine

This section provides information about installing some of the basic framework for your Identity Manager server. This installation program allows you to install the following components:

- Identity Manager drivers
- Identity Manager engine
- iManager plug-ins for Identity Manager

NetIQ bundles the components in the same installation program for your convenience. You can choose to install them on the same server or install them individually. The installation files are located in the `\products\idm` directory in the Identity Manager installation package. By default, the installation program installs the components in `C:\NetIQ`.

NetIQ recommends that you review the installation process before beginning. For more information, see "Checklist for Installing the Identity Manager Engine, Drivers, and Plug-ins" on page 55.

NOTE: This installation program also can install Remote Loader and Fanout Agent. For more information about installing Remote Loader, see Part 6, "Installing the Remote Loader," on page 65.

3 Installing the Identity Vault

This section guides you through the process of installing the required components for the Identity Vault, which stores information specific to Identity Manager, such as driver configurations, parameters, and policies.

The installation files are located in the `\products\eDirectory\`*`processor_type`*`\` directory within the `.iso` image file of the Identity Manager installation package. By default, the installation program installs the Identity Vault in `C:\NetIQ\eDirectory`.

NetIQ recommends that you review the installation process before beginning. For more information, see "Planning to Install the Identity Vault" on page 31.

Planning to Install the Identity Vault

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

- "Checklist for Installing the Identity Vault" on page 31
- "Prerequisites and Considerations for Installing the Identity Vault" on page 32
- "Understanding Identity Manager Objects in eDirectory" on page 33

Checklist for Installing the Identity Vault

NetIQ recommends that you perform the steps in the following checklist:

	Checklist Items
☐	1. Review the planning information. For more information, see Part I, "Planning to Install Identity Manager," on page 17.
☐	2. Review the hardware and software requirements for the computers that will host the Identity Vault. For more information, see "Meeting System Requirements" on page 22.
☐	3. Understand how to use escape characters when the names of containers in the Identity Vault include a period ("."). For more information, see "Using Escape Characters when a Container Name Includes a Period (".")" on page 34.
☐	4. Understand how to use the Identity Vault in an environment that uses IPv6 addresses. For more information, see "Using IPv6 Addresses on the Identity Vault Server" on page 40.
☐	5. Understand the ports required for LDAP communications. For more information, see "Using LDAP to Communicate with the Identity Vault" on page 40.

	Checklist Items
□	6. For installation instructions, see one of the following sections: ◆ For a guided installation (wizard), see “Using the Wizard to Install the Identity Vault” on page 42. ◆ For a silent installation (unattended), “Silently Installing and Configuring the Identity Vault” on page 43.
□	7. (Optional) Exclude the DIB directory on your eDirectory server from any antivirus or backup software process.
□	8. (Optional) Back up your DIB directory. For more information, see “Backing Up and Restoring NetIQ eDirectory” in the *NetIQ eDirectory Administration Guide*.
□	9. Install the Identity Manager engine. For more information, see Chapter 4, “Planning to Install the Engine, Drivers, and Plug-ins,” on page 55.

Prerequisites and Considerations for Installing the Identity Vault

Identity Vault uses a directory to store the objects that are synchronized through the Identity Manager solution. The follow sections contain guidelines that help you plan a deployment of NetIQ eDirectory to use as the framework for the Identity Vault.

NetIQ recommends that you review the following considerations before you install eDirectory as the framework for the Identity Vault:

- You must configure a static IP address on the server for the eDirectory infrastructure to perform efficiently. If you use DHCP addresses on the server, eDirectory might have unpredictable results.
- Synchronize time across all network servers. NetIQ recommends using Network Time Protocol’s (NTP) `ntp` option.
- (Conditional) To install a secondary server, all the replicas in the partition that you install the product on should be in the On state.
- (Conditional) To install a secondary server into an existing tree as a non-administrator user, create a container and then partition it. Ensure that you have the following rights:
  - Supervisor rights to the partition where you want to add the server.
  - Supervisor rights to the container where want to add the server.
  - All Attributes rights: read, compare, and write rights over the `W0`.KAP`.Security` object.
  - Attribute rights: read and compare rights over the Security container object.
  - Entry rights: browse rights over the Security container object.

  These rights are required for adding the replica when the replica count is less than 3.
- (Conditional) To install a secondary server into an existing tree as a non-administrator user, ensure that at least one of the servers in the tree has the same or higher eDirectory version as that of the secondary being added as container admin. If the secondary being added is of later version, the administrator of the tree must extend the schema before adding the secondary using container admin.

- While configuring eDirectory, you must enable a NetWare Core Protocol (NCP) port (the default is 524) in the firewall to allow the secondary server addition. Also, you can enable the following default service ports based on your requirements:
    - LDAP clear text - 389
    - LDAP secured - 636
    - HTTP clear text - 8028
    - HTTP secured - 8030
- You must install Novell International Cryptographic Infrastructure (NICI) on every workstation using management utilities for eDirectory, such as iManager. NICI and eDirectory support key sizes up to 4096 bits. For more information, see "Installing NICI" in the *NetIQ eDirectory Installation Guide*.
- (Conditional) If the names of containers in your eDirectory tree include a period, you must use escape characters to specify the Admin name, admin context, and server context parameters during installation and when adding server in to an existing tree. For more information, see "Using Escape Characters when a Container Name Includes a Period (".")" on page 34.
- You must have administrative rights to the server and to all portions of the eDirectory tree that contain domain-enabled User objects. For an installation into an existing tree, you need administrative rights to the Tree object so that you can extend the schema and create objects.
- Because NTFS provides a safer transaction process than a FAT file system provides, you can install eDirectory only on an NTFS partition. Therefore, if you have only FAT file systems, do one of the following:
    - Use Disk Administrator. Refer to the Windows Server documentation for more information.
    - Create a new partition and format it as NTFS.
    - Convert an existing FAT file system to NTFS, using the CONVERT command.
    - Refer to the Windows Server documentation for more information.

  If your server only has a FAT file system and you forget or overlook this process, the installation program prompts you to provide an NTFS partition.
- You must be running the latest version of the Windows SNMP service.
- Your Windows operating system must be running the latest service packs before you begin the installation process.
- To install on a virtual machine that has a DHCP address or on a physical or virtual machine in which SLP is not broadcast, ensure that the Directory Agent is configured in your network.

For installing Identity Vault in a cluster environment, see Part X, "Deploying Identity Manager for High Availability," on page 327.

Understanding Identity Manager Objects in eDirectory

The following list indicates the major Identity Manager objects that are stored in eDirectory and how they relate to each other. The installation process does not create objects. Instead, you create the Identity Manager objects when configuring the Identity Manager solution.

- **Driver Set:** A driver set is a container that holds Identity Manager drivers and library objects. Only one driver set can be active on a server at a time. However, more than one server might be associated to one driver set. Also, a driver can be associated with more than one server at a time. However, the driver should only be running on one server at a time. The driver should be in a disabled state on the other servers. Any server that is associated with a driver set must have the Identity Manager server installed on it.

- **Library:** The Library object is a repository of commonly used policies that can be referenced from multiple locations. The library is stored in the driver set. You can place a policy in the library so that every driver in the driver set can reference it.
- **Driver:** A driver provides the connection between an application and the Identity Vault. It also enables data synchronization and sharing between systems. The driver is stored in the driver set.
- **Job:** A job is automates a recurring task. For example, a job can configure a system to disable an account on a specific day, or initiate a workflow to request an extension of a person's access to a corporate resource. The job is stored in the driver set.

Preparing to Install the Identity Vault

Your environment for the Identity Vault must be configured appropriately. For example, the server must have a method (a service or specified file) that can be used to resolve tree names in Identity Vault to server referrals. This section helps you prepare your environment before you install the Identity Vault.

Using Escape Characters when a Container Name Includes a Period (".")

You can add a Windows server that has a period in the server name to a directory tree. For example, `O=netiq.com` or `C=u.s.a`. However, if the names of your containers in the tree include a period ("."), you must use escape characters. Review the following considerations:

- Do not use a period at the beginning of a server name. For example, `.netiq`.
- Escape the period in the container name with a backslash ("\"). For example:

  `O=novell\.com`

  or

  `C=a\.b\.c`

Include the escape characters when you enter a dotted admin name and context for utilities such as iMonitor, iManager, DHost iConsole, DSRepair, Backup, DSMerge, DSLogin, and ldapconfig. For example, when logging in to iMonitor, if the name of the O in your tree is `netiq.com`, enter `'admin.netiq\.com'` or `admin.netiq\.com`.

Using OpenSLP or hosts.nds for Resolving Tree Names

Before installing the Identity Vault infrastructure, the server should have a method (a service or specified file) that can be used to resolve tree names in Identity Vault to server referrals. NetIQ recommends using Service Location Protocol (SLP) services to resolve tree names. Previous versions of eDirectory included OpenSLP in the installation. However, starting with eDirectory 8.8, the installation does not include OpenSLP. You must separately install an SLP service or use a `hosts.nds` file. If you use an SLP service, the directory agents for the service (SLPDAs) must be stable.

This section provides the following information:

- "Using a hosts.nds File to Resolve Tree Names" on page 35
- "Understanding OpenSLP" on page 36
- "Configuring SLP for the Identity Vault" on page 38

Using a hosts.nds File to Resolve Tree Names

The `hosts.nds` file is a static lookup table that Identity Vault applications use to search Identity Vault partitions and servers. It helps you avoid SLP multicast delays when SLP DA is not present in the network. For each tree or server, you must specify the following information in a single line in the `hosts.nds` file:

- **Server Name or Tree Name**: Tree names should end with a trailing dot (.).
- **Internet Address**: This can be a DNS name or IP address. Do not use `localhost`.
- **Server Port**: Optional, appended with a colon (:) to the Internet address.

You do not have to include an entry for the local server in the file, unless the server listens on a non-default NCP port.

To configure a hosts.nds file:

1 Create a new or open an existing `hosts.nds` file.

2 Add the following information:

```
partition_name.tree_name. host_name/ip-addr:port server_name dns-addr/
ip-addr:port
```

For example:

```
# This is an example of a hosts.nds file:
# Tree name Internet address/DNS Resolvable Name
  CORPORATE. myserver.mycompany.com
  novell.CORPORATE. 1.2.3.4:524

# Server name Internet address
  CORPSERVER myserver.mycompany.com:524
```

3 (Optional) If you later decide to use SLP to resolve the tree name and ensure that the Identity Vault tree is available on the network, add the following text to the `hosts.nds` file:

```
/usr/bin/slptool findattrs services:ndap.novell///(svcname-
ws==[treename or *])"
```

For example, to search for the services whose `svcname-ws` attribute match with the value SAMPLE_TREE, enter the following command:

```
/usr/bin/slptool findattrs services:ndap.novell///(svcname-
ws==SAMPLE_TREE)"
```

NOTE: Perform this action after you install SLP and the Identity Vault.

If you have a service registered with its `svcname-ws` attribute as SAMPLE_TREE, then the output will be similar to `service:ndap.novell:///`SAMPLE_TREE. Otherwise, you will not receive an output response.

Understanding OpenSLP

OpenSLP is an open-source implementation of the IETF Service Location Protocol Version 2.0 standard, which is documented in IETF Request-For-Comments (RFC) 2608.

The interface provided by OpenSLP source code is an implementation of another IETF standard for programmatically accessing SLP functionality, documented in RFC 2614.

To fully understand the workings of SLP, it is worth reading these documents and internalizing them. They are not necessarily light reading, but they are essential to the proper configuration of SLP on an intranet.

For more information on the OpenSLP project, see the OpenSLP and the SourceForge websites. The OpenSLP website provides several documents that contain valuable configuration tips. Many of these are incomplete at the time of this document's publication.

This section includes the following discussions about the use of SLP and how it relates to the Identity Vault:

- "NetIQ Service Location Providers" on page 36
- "User Agents" on page 37
- "Service Agents" on page 37
- "Directory Agents" on page 38

NetIQ Service Location Providers

The NetIQ version of SLP takes certain liberties with the SLP standard in order to provide a more robust service advertising environment, but it does so at the expense of some scalability.

For example, in order to improve scalability for a service advertising framework, you can limit the number of packets that are broadcast or multicast on a subnet. The SLP specification manages this by imposing restrictions on service agents and user agents regarding directory agent queries. The first directory agent discovered that services the desired scope is the one that a service agent (and consequently, local user agents) will use for all future requests on that scope.

The NetIQ SLP implementation actually scans all of the directory agents it knows about looking for query information. It assumes a 300-millisecond round trip time is too long, so it can scan 10 servers in about 3 to 5 seconds. This doesn't need to be done if SLP is configured correctly on the network, and OpenSLP assumes the network is in fact configured correctly for SLP traffic. OpenSLP's response timeout values are greater than that of NetIQ's SLP service provider, and it limits the number of directory agents to the first one that responds, whether or not that agent's information is accurate and complete.

User Agents

A user agent (UA) takes the physical form of a static or dynamic library that is linked to an application. It allows the application to query for SLP services. The user agent’s job is to provide a programmatic interface for clients to query for services, and for services to advertise themselves. A user agent contacts a directory agent to query for registered services of a specified service class and within a specified scope.

User agents follow an algorithm to obtain the address of a directory agent to which queries will be sent. Once they obtain an address of a directory agent (DA) for a specified scope, they continue to use that address for that scope until it no longer responds, at which time they obtain another DA address for that scope. User agents locate a directory agent address for a specified scope by:

1. Checking to see if the socket handle on the current request is connected to a DA for the specified scope. If the request happens to be a multipart request, there may already be a cached connection present on the request.
2. Checking its local known DA cache for a DA matching the specified scope.
3. Checking with the local service agent (SA) for a DA with the specified scope (and adding new addresses to the cache).
4. Querying DHCP for network-configured DA addresses that match the specified scope (and adding new addresses to the cache).
5. Multicasting a DA discovery request on a well-known port (and adding new addresses to the cache).

The specified scope is “default,” if not specified. That is, if no scope is statically defined in the SLP configuration file, and no scope is specified in the query, then the scope used is the word “default”. It should also be noted that Identity Vault never specifies a scope in its registrations. If there is a statically configured scope, that scope becomes the default scope for all local UA requests and SA registrations in the absence of a specified scope.

Service Agents

Service agents take the physical form of a separate process on the host machine. The `slpd.exe` runs as a service on the local machine. User agents query the local service agent by sending messages to the loop-back address on a well-known port.

The service agent’s job is to provide persistent storage and maintenance points for local services that have registered themselves with SLP. The service agent essentially maintains an in-memory database of registered local services. In fact, a service cannot register with SLP unless a local SA is present. Clients can discover services with only a UA library, but registration requires an SA, primarily because an SA must reassert the existence of registered services periodically in order to maintain the registration with listening directory agents.

A service agent locates and caches directory agents and their supported scope list by sending a DA discovery request directly to potential DA addresses by:

1. Checking all statically configured DA addresses (and adding new ones to the SA’s known DA cache).
2. Requesting a list of DA’s and scopes from DHCP (and adding new ones to the SA’s known DA cache).

3. Multicasting a DA discovery request on a well-known port (and adding new ones to the SA's known DA cache).
4. Receiving DA advertising packets that are periodically broadcast by DAs (and adding new ones to the SA's known DA cache).

Since a user agent always queries the local service agent first, this is important, as the local service agent's response will determine whether or not the user agent continues to the next stage of discovery (in this case DHCP-- see Step 3 and Step 4 in "User Agents" on page 37.

Directory Agents

The directory agent's job is to provide a long-term persistent cache for advertised services, and to provide a point of access for user agents to look up services. As a cache, the DA listens for SAs to advertise new services, and caches those notifications. Over a short time, a DA's cache becomes more full or more complete. Directory agents use an expiration algorithm to expire cache entries. When a directory agent comes up, it reads its cache from persistent storage (generally a hard drive), and then begins to expire entries according to the algorithm. When a new DA comes up, or when a cache has been deleted, the DA detects this condition and sends out a special notification to all listening SAs to dump their local databases so the DA can quickly build its cache.

In the absence of any directory agents, the UA will resort to a general multicast query that SAs can respond to, building a list of the requested services in much the same manner that DAs use to build their cache. The list of services returned by such a query is an incomplete and much more localized list than that provided by a DA, especially in the presence of multicast filtering, which is done by many network administrators, limiting broadcasts and multicasts to only the local subnet.

In summary, everything hinges on the directory agent that a user agent finds for a given scope.

Configuring SLP for the Identity Vault

The following parameters in the `%systemroot%/slp.conf` file control directory agent discovery:

```
net.slp.useScopes = comma-delimited scope list
net.slp.DAAddresses = comma-delimited address list
net.slp.passiveDADetection = <"true" or "false">
net.slp.activeDADetection = <"true" or "false">
net.slp.DAActiveDiscoveryInterval = <0, 1, or a number of seconds>
```

useScopes

Indicates which scopes the SA will advertise into, and which scopes queries will be made to in the absence of a specific scope on the registration or query made by the service or client application. Because Identity Vault always advertises into and queries from the default scope, this list will become the default scope list for all Identity Vault registrations and queries.

DAAddresses

Represents a comma-delimited list of dotted decimal IP addresses of DAs that should be preferred to all others. If this list of configured DAs does not support the scope of a registration or query, then SAs and UAs will resort to multicast DA discovery, unless such discovery is disabled.

passiveDADetection

Is `True` by default. Directory agents will periodically broadcast their existence on the subnet on a well-known port if configured to do so. These packets are termed DAAdvert packets. If this option is set to False, all broadcast DAAdvert packets are ignored by the SA.

activeDADetection

Is `True` by default. This allows the SA to periodically broadcast a request for all DAs to respond with a directed DAAdvert packet. A directed packet is not broadcast, but sent directly to the SA in response to these requests. If this option is set to False, no periodic DA discovery request is broadcast by the SA.

DAActiveDirectoryInterval

Represents a tri-state parameter. The default value is `1`, which is a special value meaning that the SA should only send out one DA discovery request upon initialization. Setting this option to 0 has the same effect as setting the activeDADetection option to false. Any other value is a number of seconds between discovery broadcasts.

These options, when used properly, can ensure an appropriate use of network bandwidth for service advertising. In fact, the default settings are designed to optimize scalability on an average network.

Improving Identity Vault Performance

eDirectory, the underlying infrastructure for the Identity Vault, is I/O intensive application rather than being processor-intensive. Two factors increase performance of Identity Vault: more cache memory and faster processors. For best results, cache as much of the Directory Information Base (DIB) Set as the hardware allows.

While eDirectory scales well on a single processor, you might consider using multiple processors. Adding processors improves performance in areas such as user logins. Also, having multiple threads active on multiple processors improves performance.

The following table provides a general guideline for server settings, based on the expected number of objects in your eDirectory.

Objects	Memory	Hard Disk
100.000	384 MB	144 MB
1 million	4 GB	1.5 GB
10 million	2+ GB	15 GB

For example, a base installation of eDirectory with the standard schema requires about 74 MB of disk space for every 50,000 users. However, if you add a new set of attributes or completely fill in every existing attribute, the object size grows. These additions affect the disk space, processor, and memory needed. Also, requirements for processors depend on additional services available on the computer as well as the number of authentications, reads, and writes that the computer is handling. Processes such as encryption and indexing can be processor intensive.

Using IPv6 Addresses on the Identity Vault Server

Identity Vault supports both IPv4 and IPv6 addresses. You can enable IPv6 addresses when you install the Identity Vault. If you upgrade from a previous version, you must manually enable IPv6 addresses.

Identity Vault also supports Dual IP stack, Tunneling, and Pure IPv6 transition methods. It supports only the global IP addresses. For example:

- `[::]`
- `[::1]`
- `[2015::12]`
- `[2015::12]:524`

You must specify IPv6 addresses within square braces `[ ]`. To use hostname instead of an IP address, you must specify the name in the `C:\Windows\System32\drivers\etc\hosts` file and associate it with the IPv6 address.

To use IPv6 addresses on a Windows server, you must select the **Enable IPv6** check box under **IPv6 Preference** during the installation. This option enables the NCP, HTTP, and HTTPS protocols for the IPv6 addresses. If you do not enable IPv6 addresses during the installation process, and then decide to use them later, you must run the setup program again. For more information, see Chapter 3, "Installing the Identity Vault," on page 31.

You can access iMontior over IPv6 addresses using the following link: `http://[2015::3]:8028/nds`.

Using LDAP to Communicate with the Identity Vault

When you install the Identity Vault, you must specify the ports that the LDAP server monitors so that it can service LDAP requests. As part of default configuration, the ports numbers for clear text and SSL/TLS are set to 389 and 636.

An LDAP Simple Bind requires only a DN and a password. The password is in clear text. If you use port 389, the entire packet is in clear text. Because port 389 allows clear text, the LDAP server services Read and Write requests to the Directory through this port. This openness is adequate for environments of trust, where spoofing does not occur and no one inappropriately captures packets. By default, this option is disabled during the installation.

The connection through port 636 is encrypted. TLS (formerly SSL) manages the encryption. A connection to port 636 automatically instantiates a handshake. If the handshake fails, the connection is denied.

NOTE: The installation program selects port 636 by default for TLS/SSL communications. This default selection might cause a problem for your LDAP server. If a service already loaded on the host server (before eDirectory was installed) uses port 636, you must specify another port. Installations earlier than eDirectory 8.7 treated this conflict as a fatal error and unloaded `nldap`. After eDirectory 8.7.3, the installation program loads `nldap`, places an error message in the `dstrace.log` file, and runs without the secure port.

During the installation process, you can configure Identity Vault to disallow clear passwords and other data. The **Require TLS for Simple Bind with Password** option discourages users from sending observable passwords. If you do not select this setting, users are unaware that others can observe their passwords. This option, which does not allow the connection, only applies to the clear-text port. If you make a secure connection to port 636 and have a simple bind, the connection is already encrypted. No one can view passwords, data packets, or bind requests.

Consider the following scenarios:

Require TLS for Simple Bind with Password Is Enabled

Olga is using a client that asks for a password. After Olga enters a password, the client connects to the server. However, the LDAP server does not allow the connection to bind to the server over the clear-text port. Everyone is able to view Olga's password, but Olga is unable to get a bound connection.

Port 636 Is Already Used

Your server is running Active Directory. Active Directory is running an LDAP program, which uses port 636. You install eDirectory. The installation program detects that port 636 is already used and does not assign a port number for the NetIQ LDAP server. The LDAP server loads and appears to run. However, because the LDAP server does not duplicate or use a port that is already open, the LDAP server does not service requests on any duplicated port.

To verify whether port 389 or 636 is assigned to the NetIQ LDAP server, run the ICE utility. If the *Vendor Version* field does not specify NetIQ, you must reconfigure LDAP Server for eDirectory and select a different port. For more information, see "Verifying That the LDAP Server is Running" in the *NetIQ eDirectory Administration Guide*.

Active Directory Is Running

When Active Directory is running and clear-text port 389 open, you can run the ICE command to port 389 and ask for the vendor version. The report displays **Microsoft***. You then reconfigure the NetIQ LDAP server by selecting another port, so that the eDirectory LDAP server can service LDAP requests.

iMonitor can also report whether port 389 or 636 is already open. If the LDAP server is not working, use iMonitor to identify details. For more information, see "Verifying That the LDAP Server is Running" in the *NetIQ eDirectory Administration Guide*.

Installing the Identity Vault

The installation program can guide you through the configuration settings for the Identity Vault. The installation program automatically defaults to wizard mode. However, you can also perform a silent installation.

This section assumes that you want to use eDirectory as the base structure for the Identity Vault.

When you start the installation program, it checks for Novell International Cryptographic Infrastructure (NICI) and Novell Client for Windows. The installation program will install or update these components as needed. If you install the Identity Vault on a computer already containing the Novell Client, eDirectory will use the existing Novell Client. You can install the Identity Vault without the Novell Client.

For more information about NICI, see the *Novell International Cryptographic Infrastructure Administration Guide*. For more information on the Client, see the Novell Client for Windows documentation.

The installation program can install the server components for NetIQ Module Authentication Service (NMAS). During the installation, you must specify the login methods to use with NMAS. You must also install the NMAS client software on each client workstation where you want to use the NMAS login methods.

NOTE

- You can use case-sensitive passwords for all the utilities.
- Your container names can include a period (dot). For information on using dots in container names, see "Prerequisites and Considerations for Installing the Identity Vault" on page 32.

Using the Wizard to Install the Identity Vault

1. Log in as administrative user to the computer where you want to install eDirectory.
2. Navigate to the `\products\eDirectory\x64\` directory.
3. Run the `eDirectory_910_windows_x86_64.exe` file.
4. 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.

          NOTE: Though Identity Vault allows you to set the NCP server object's FDN up to 256 characters, NetIQ recommends that you restrict the variable to a much lesser value because Identity Vault creates other objects of greater length based on the length of this object.
        - **Tree Admin:** Specify an administrator name for Identity Vault.
        - **Admin Password:** Specify the administrator password.
    - 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.

5 (Conditional) In the **Advanced** tab, specify the following details:

- To use IPv6 addresses on the Identity Vault server, select **Enable IPv6**.

  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.

6 In the **Install Location** field, specify the location where Identity Vault is installed.

7 In the **DIB Location** field, specify the location where the DIB files are located.

8 Click **Install** and proceed with the installation.

Silently Installing and Configuring the Identity Vault

To support a silent (or unattended) installation or configuration of the Identity Vault, you can use a `response.ni` file that contains sections and keys, similar to a `Windows.ini` file.

NOTE: You must install and configure NetIQ SecreStore (`ss`). For more information, see "Adding SecretStore to the Identity Vault Schema" on page 51.

Editing the response.ni File

You can use an ASCII text edit to create and edit the `response.ni` file. The response file helps you:

- Perform a complete unattended installation with all required user inputs.
- Define the default configuration of components.
- Bypass all prompts during the installation.

NetIQ provides a `response.ni` file in the `products\eDirectory\x64\windows\x64\NDSonNT` folder of the installation kit. The file contains default settings for essential parameters. You must edit the values for the eDirectory instance in the NWI:NDS section.

NOTE: When you edit the `response.ni` file, do not include blank spaces between the key and values along with the equal sign ("=") in each key-value pair.

WARNING: You specify the administrator user credentials in the `response.ni` file for an unattended installation. To prevent the administrator credentials from being compromised, you should permanently delete the file after the installation or configuration.

The following sections describe the sections and keys required in the `response.ni` file:

- "NWI:NDS" on page 44
- "NWI:NMAS (NMAS Methods)" on page 46
- "eDir:HTTP (Ports)" on page 47
- "Novell:Languages:1.0.0 (Language Settings)" on page 47
- "Initialization" on page 48
- "NWI:SNMP" on page 48
- "EDIR:SLP" on page 48
- "Novell:ExistingTree:1.0.0" on page 48
- "Selected Nodes" on page 49
- "Novell:NOVELL_ROOT:1.0.0" on page 49

NWI:NDS

Upgrade Mode

Specifies whether to run the installation program as an upgrade. Valid values are `False`, `True`, and `Copy`.

Mode

Specifies the type of installation that you want to perform:

- **full** allows you to both install and configure the Identity Vault. Specify this value when you want to perform a fresh installation and configuration of the Identity Vault or an upgrade and configuration of only the required files.
- **install** allows you to install a fresh version of the Identity Vault or upgrade the required files.
- **configure** allows you to modify the Identity Vault settings. If you only perform an upgrade of the required files, then the installation program configures only the upgraded files.

NOTE

- If you specify *configure*, ensure that you do not change the `RestrictNodeRemove` value of the `ConfigurationMode` key in the [Initialization] section.
- If you specify *full*, you cannot opt for individual deconfiguration and uninstallation option when you uninstall the Identity Vault.

New Tree

Specifies whether this installation is for a new tree or a secondary server. Valid values are `Yes` and `No`. For example, if you want to install a new tree, specify `Yes`. For more information about specifying values for an existing tree, see "Novell:ExistingTree:1.0.0" on page 48.

Tree Name

If this is a new installation, specify the name of the tree that you want to install. To install a secondary server, specify the tree where you want to add the server.

Server Name

Specifies the name of the server that you want to install in the Identity Vault.

Server Container

Specifies the container object in the tree to which the server object will be added. The server object contains all the configuration details specific to the Identity Vault server. If you are installing a fresh version of the Identity Vault, the installation program creates this container with the server object.

Server Context

Specifies the complete distinguished name (DN) of the server object (server name), along with the container object. For example, if the Identity Vault server is EDIR-TEST-SERVER and the container is Netiq, specify `EDIR-TEST-SERVER.Netiq`.

Admin Context

Specifies the container object in the tree to which the Administrator object will be added. For example, `Netiq`. Any user added to a tree has a user object that contains all the user-specific details. If you are installing a fresh version of the Identity Vault, the installation program creates this container with the server object.

Admin Login Name

Specifies the relative distinguished name (RDN) of the Administrator object in the tree that has full rights, at least to the context to which this server is added. For example, `Admin`. The installation program uses this account to perform all operations in the tree.

Admin Password

Specifies the password for the Administrator object. For example, `netiq123`. If you are installing a fresh version of the Identity Vault, the installation program configures this password for the Administrator object.

NDS Location

Specifies the path in the local system where you want to install the Identity Vault libraries and binaries. When you configure the Identity Vault components, they refer to this installation location for relevant files. By default, the installation program places the files in `C:\Novell\NDS`.

DataDir

Specifies the path in the local system where you want to install the DIB files. By default, the installation program places the files in `C:\Novell\NDS\DIBFiles`.

You might want to specify a different path if the DIB data files for your environment will require more space that is available in the default location.

Installation Location

(Optional) Specifies a path that the installation program uses while copying files to the NDS Location. For example, `[Novell:DST:1.0.0_Location]` or `Path=file://C:\Novell\NDS`. The default value is `C:\Novell\NDS`, the same as the default for NDS Location. The installation program uses this path while copying files to the specified NDS and DataDir locations.

System Location

(Optional) Specifies a path to the system folder of the computer where you want to install the Identity Vault server. For example, `[Novell:SYS32_DST:1.0.0_Location]` or `Path=file:/C:\Windows\system32`. The installation program requires access to the system folder to copy DLLs and to access system-specific files during installation.

Require TLS

(Optional) Specifies whether the Identity Vault requires Transport Layer Security (TLS) protocol when receiving LDAP requests in clear text.

LDAP TLS Port

(Optional) Specifies the port on which the Identity Vault listens for LDAP requests in clear text.

LDAP SSL Port

(Optional) Specifies the port on which the Identity Vault should listen for LDAP requests using Secure Sockets Layer (SSL) protocol.

Install as Service

Instructs the installation program to install eDirectory as a service. You must specify `Yes`.

Prompt

Specifies whether the installation program prompts you for decisions such as tree name and server name. For example, in a silent or unattended installation, specify `False`.

NWI:NMAS (NMAS Methods)

The Identity Vault supports multiple NMAS methods, both during installation and upgrade. You must specify the NDS NMAS method in the `response.ni` file. If you do not specify any NMAS methods, the installation program installs the NDS method by default. However, if you are creating an explicit list, you must include NDS.

Choices

Specifies the number of NMAS methods that you want to install. For example, `5`.

Methods

Specifies the types of NMAS methods that you want to install. Use commas to separate multiple types. For example, `CertMutual,Challenge Response,DIGEST-MD5,NDS`.

The installation program matches the exact string (with case) for choosing the NMAS methods to install, so you must specify the values exactly as listed:

- `CertMutual`
- `Challenge Response` - which represents the NetIQ challenge response NMAS method.
- `DIGEST-MD5`

- `Enhanced Password`
- `Entrust`
- `GSSAPI` - which represents the SASL GSSAPI mechanism for eDirectory. Authentication to the Identity Vault occurs through LDAP using a Kerberos ticket.
- `NDS` - the default login method. REQUIRED.
- `NDS Change Password`
- `Simple Password`
- `Universal Smart Card`
- `X509 Advanced Certificate`
- `X509 Certificate`

When you specify the NMAS methods in the response file, the Identity Vault shows a status message while installing without prompting for user input.

eDir:HTTP (Ports)

The Identity Vault listens on preconfigured HTTP ports for access through the web. For example, iMonitor accesses the Identity Vault through web interfaces. They need to specify certain ports to access the appropriate applications. The following options allow you to configure the Identity Vault for specific ports:

Clear Text HTTP Port

Specifies the number of the port for the HTTP operations in clear text.

SSL HTTP Port

Specifies the number of the port for the HTTP operations using SSL protocol.

Novell:Languages:1.0.0 (Language Settings)

During installation, you can specify the locale and displayed language for the Identity Vault: English, French, or Japanese. These values are mutually exclusive.

LangID4

Represents English. For example, `LangID4=true`.

LangID6

Represents French.

LangID9

Represents Japanese.

NOTE

- Do not specify `true` for more than one language.
- You can also specify the language that the installation program uses to display messages throughout the installation. For more information, see "Initialization" on page 48.

Initialization

The [Initialization] section of the response.ni file specifies the settings for the installation process.

DisplayLanguage

Specifies the language used for messages displayed during the installation process. For example, DisplayLanguage=en_US.

InstallationMode

Specifies how you want to run the installation process. For example, to perform a silent or unattended installation, specify silent.

SummaryPrompt

Specifies whether the installation program prompts you to review a summary of the installation settings. For example, in a silent or unattended installation, specify false.

prompt

Specifies whether the installation program prompts you for decisions. For example, in a silent or unattended installation, specify false.

NWI:SNMP

Most Windows servers have SNMP configured and running. When you install the Identity Vault, you must stop SNMP services and then restart after the process completes. During a manual installation, the program prompts you to stop the SNMP services before continuing the installation.

To stop SNMP services without a prompt during a silent or unattended installation, in the [NWI:SNMP] section of the response.ni file, specify Stop Service=yes.

EDIR:SLP

The Identity Vault uses Service Location Protocol (SLP) services to identify other servers or trees in the subnet during installation or upgrade. If SLP services are already installed on your server, you can replace them with the version that ships with the current version of the Identity Vault or use your own SLP services.

Need to uninstall service

Specifies whether to uninstall any SLP services already installed on your server. The default value is true.

Need to remove files

Specifies whether to remove the files for any SLP services already installed on your server. The default value is true.

Novell:ExistingTree:1.0.0

The installation program provides options for the unattended install of a primary or a secondary server into a network. The installation program uses three different keys to decide whether to install a new tree or a secondary server in an existing tree.

NOTE: The `New Tree` key resides in the `NWI:NDS` section. For more information, see "NWI:NDS" on page 44.

ExistingTreeYes

Valid values are `True` and `False`. For example, if you want to install a new tree, specify `False`.

ExistingTreeNo

Valid values are `True` and `False`. For example, if you want to install a new tree, specify `True`.

To run a silent or unattended installation without prompts for decisions about primary or secondary server installation, in the `Existing Tree` section of the `response.ni` file, specify `prompt=false`.

Selected Nodes

This section in the `response.ni` file lists the components that are installed in the Identity Vault, along with information in the profile database that contains more information about the component, including source location, destination copy location, and component version. These details in the profile database are compiled into a `.db` file that is delivered in the Identity Vault release.

To run a silent or unattended installation without prompts for decisions such as the destination copy location or version details, in the `[Selected Nodes]` section of the `response.ni` file, specify `prompt=false`.

Your response file must include this section. Use the keys and values exactly as provided in the sample `response.ni` file.

Novell:NOVELL_ROOT:1.0.0

This section in the `response.ni` file contains the settings for image and status displays that occur during the installation process. For example, you can specify the settings for the way the installation program responds to scenarios such as file write conflicts and file copying decisions. You can also specify whether images are displayed. Most images contain information on what version of the Identity Vault is installed, what components are installed, a welcome screen, license files, customization options, a status message indicating the component currently being installed, percentage complete, etc. Some applications that intend to embed eDirectory might not want eDirectory displaying these images.

To run a silent or unattended installation without prompts for decisions such as the destination copy location or version details, in this section of the `response.ni` file, specify `prompt=false`.

Your response file should include this section. Use the keys and values provided in the sample `response.ni` file.

Performing a Silent or Unattended Installation

Before beginning, review the prerequisites for performing a silent or unattended installation. For more information, see "Prerequisites and Considerations for Installing the Identity Vault" on page 32. Also, create the `response.ni` file to use as a template for the installation. For more information, see "Editing the response.ni File" on page 43.

NOTE: To ensure that the operating system does not display a status window for installation, upgrade, or configuration, use the `nopleasewait` option in the command.

1. Create a new `response.ni` file or edit an existing response file. For more information about the values in the response file, see "Editing the response.ni File" on page 43.
2. Log in with an administrator account to the computer where you want to install the Identity Vault.
3. Open a command prompt with the **Run as administrator** option enabled.
4. At the command line, enter the following command:

   ```
   path_to_installation_files\windows\eDirectory\x64\NDSonNT>install.exe /
   silent /nopleasewait /template=Response file
   ```

   For example:

   ```
   D:\builds\eDirectory\windows\eDirectory\x64\NDSonNT>install.exe /silent
   /
   nopleasewait /
   template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
   ```

Performing a Silent Configuration

1. Create a new `response.ni` file or edit an existing response file. For more information about the values in the response file, see "Editing the response.ni File" on page 43.
2. Log in with an administrator account to the computer where you want to install the Identity Vault.
3. Open a command prompt with the **Run as administrator** option enabled.
4. At the command line, enter the following command:

   ```
   Windows Drive\Program Files\Common Files\novell>install.exe /silent /
   restrictnoderemove /nopleasewait /template=Response file
   ```

   For example:

   ```
   c:\Program Files\Common Files\novell>install.exe /silent /
   restrictnoderemove /nopleasewait /
   template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
   ```

Performing a Silent Installation Combined with Configuration

Before beginning, review the prerequisites for performing a silent or unattended installation. For more information, see "Prerequisites and Considerations for Installing the Identity Vault" on page 32. Also, create the `response.ni` file to use as a template for the installation.

1. Create a new `response.ni` file or edit an existing response file. For more information about the values in the response file, see "Editing the response.ni File" on page 43.
2. Log in with an administrator account to the computer where you want to install the Identity Vault.
3. Open a command prompt with the **Run as administrator** option enabled.

4 At the command line, enter the following command:

```
Unzipped Location\windows\eDirectory\x64\NDSonNT>install.exe /silent /
nopleasewait /template=Response file
```

For example:

```
D:\builds\eDirectory\windows\eDirectory\x64\NDSonNT>install.exe /silent
/
nopleasewait /
template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
```

Configuring the Identity Vault after Installation

After installing the Identity Vault, you may need to perform certain configuration tasks on the Identity Vault.

- "Adding SecretStore to the Identity Vault Schema" on page 51
- "Configuring the Identity Vault in a Specific Locale" on page 52
- "Managing eDirectory Instances" on page 52

Adding SecretStore to the Identity Vault Schema

You must extend the Identity Vault schema to support SecretStore functionality. The identity applications need SecretStore to connect to the vault.

1 To extend the schema for the Identity Vault, enter the following command:

```
ice -S SCH -f C:\NetIQ\eDirectory\sssv3.sch -D LDAP -s serverIP -d
adminDN
```

For example:

```
ice -S SCH -f C:\NetIQ\eDirectory\sssv3.sch -D LDAP -s 192.168.0.1 -d
cn=admin,o=administrators
```

2 To configure SecretStore on a Windows server, complete the following steps:

2a Navigate to the `C:\NetIQ\eDirectory` directory.

2b Enter the following command:

```
ssscfg.exe -c
```

2c Specify the configuration settings for SecretStore, then close the utility.

2d Run `NDSCons.exe`.

2e In the utility, specify `auto` for the `ssncp.dlm` module.

2f Close the utility.

For more information, see "SecretStore Configuration for eDirectory Server" in the *NetIQ eDirectory Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

Configuring the Identity Vault in a Specific Locale

To configure the Identity Vault in a specific locale, you must export LC_ALL and LANG to that particular locale before performing the configuration. For example, enter the following commands in the ndsconfig utility:

```
export LC_ALL=ja
```

```
export LANG=ja
```

Managing eDirectory Instances

You can create, start, and stop server instances in the Identity Vault. You can also view a list of configured instances.

Listing Identity Vault Instances

You can use the DHost iConsole to view the configuration file path, fully distinguished name and port for the server instance, and the status of the instance (active or inactive) for specified users.

Creating a New Instance in the Identity Vault

Use DHost utility to create a new instance in eDirectory.

Configuring and Deconfiguring an Instance in the Identity Vault

Use DHost utility to configure and deconfigure an instance in the Identity Vault.

Invoking a utility for an Instance in the Identity Vault

You can run utilities, such as DSTrace, against an instance.

1. Navigate to the `C:\NetIQ\eDirectory` directory.
2. Run the `NDSCons.exe`.
3. In the **NetIQ eDirectory Services** console, navigate to the `dstrace.dlm`.
4. Click **Start**.

Starting and Stopping Instances in the Identity Vault

You can start or stop one or more instances that you configured.

To start an instance:

1. Navigate to the `C:\NetIQ\eDirectory` directory.
2. Run the `NDSCons.exe`.
3. Navigate to an instance and click **Start**.

To stop an instance:

1. Navigate to the `C:\NetIQ\eDirectory` directory.
2. Run the `NDSCons.exe`.
3. Navigate to an instance and click **Stop**.

4 Planning to Install the Engine, Drivers, and Plug-ins

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

- "Checklist for Installing the Identity Manager Engine, Drivers, and Plug-ins" on page 55
- "Understanding the Installation Program" on page 56
- "Prerequisites and Considerations for Installing the Identity Manager Engine" on page 56

NOTE: This installation program can also install the Remote Loader. For more information, see "Installing Remote Loader" on page 67.

Checklist for Installing the Identity Manager Engine, Drivers, and Plug-ins

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

	Checklist Items
❑	1. Review the planning information. For more information, see Part I, "Planning to Install Identity Manager," on page 17.
❑	2. Review the hardware and software requirements for the computers that will host the Identity Manager engine. For more information, see "Meeting System Requirements" on page 22.
❑	3. Learn about the options in the installation program. For more information, see "Understanding the Installation Program" on page 56.
❑	4. (Conditional) For a guided installation process (wizard) of the Identity Manager engine, see Section 5, "Installing the Engine, Drivers, and iManager Plug-ins," on page 59.
❑	5. (Conditional) To install the components in a single command, see "Performing a Silent Installation" on page 60.
❑	6. (Conditional) To install the Remote Loader, see "Installing Remote Loader" on page 67.
❑	7. Start the driver instance in the Remote Loader. For more information, see Chapter , "Configuring the Remote Loader and Drivers," on page 72.
❑	8. Install the rest of the Identity Manager components, including the identity applications and Identity Reporting.

Understanding the Installation Program

As a convenience, this installation program bundles several of the components that provide the underlying framework for your Identity Manager solution. You can choose to install all components on the same server, or on individual servers. For more information about server requirements, see the Planning to Install the Engine, Drivers, and Plug-ins for each component, the guide for the individual driver, and the latest Release Notes.

The installation program provides the following options for component installation:

Identity Manager Server

Installs the Identity Manager engine, schema, drivers, and audit components.

Connected System Server (32-bit, 64-bit, .NET)

Installs the Remote Loader service and the driver instances in the loader. The Remote Loader allows you to run Identity Manager drivers on connected systems that do not host the Identity Vault and Identity Manager engine. In the installation program, you can select the drivers that you want to install with the Remote Loader on the connected system

Fanout Agent

Installs the Fan-Out agent for the JDBC Fan-Out driver. The JDBC Fan-Out driver uses the Fan-Out agent to create multiple JDBC Fan-Out driver instances. The Fan-Out agent loads the JDBC driver instances based on the configuration of the connection objects in the Fan-Out driver. For more information, see NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide.

iManager Plug-ins for Identity Manager

Installs the iManager plug-ins that allow you to use iManager to manage Identity Manager drivers that have structured Global Configuration Values (GCVs).

Drivers

Identity Manager drivers synchronize identity information among several types of directories, databases, and business applications and the Identity Vault. You can configure the driver to synchronize the data in a single direction or in both directions.

In the installation program, you can select the drivers that you want to install with the other components. You might want to install some of the drivers on a server that does not host the Identity Manager engine. In this case, you would also need to install the Remote Loader service on that server.

Prerequisites and Considerations for Installing the Identity Manager Engine

Before installing the Identity Manager engine, review the following considerations:

- Before installing the Identity Manager engine, you must install the Identity Vault. Also, the Identity Vault must contain a tree with at least one organizational unit, one user, and an iManager server.

- Install the Identity Manager engine on the same server that hosts the Identity Vault.
- (Conditional) To install the Remote Loader on the same computer as the Identity Manager engine, ensure that you select an operating system that supports both components. For more information about system requirements for the Remote Loader, see "Prerequisites and Considerations for Installing the Remote Loader" on page 67.

5 Installing the Engine, Drivers, and iManager Plug-ins

This section describes the installation process for the Identity Manager engine, drivers, iManager plug-ins, and the Remote Loader. You can install these programs on the same server or separate servers. For example, you might want to a driver on a connected system, rather than on the same server as the Identity Manager engine. In this case, you also would install the Remote Loader on that connected system.

NetIQ provides both a guided installation process and a silent installation.

- "Using the Wizard to Install the Components" on page 59
- "Performing a Silent Installation" on page 60
- "Installing on a Server with Multiple Instances of Identity Vault" on page 62

Using the Wizard to Install the Components

The installation program guides you through the configuration settings for the Identity Manager engine. The installation program automatically defaults to wizard mode.

To prepare for the installation, see "Checklist for Installing the Identity Manager Engine, Drivers, and Plug-ins" on page 55. Also see the Release Notes accompanying the release. To perform an unattended installation, see "Performing a Silent Installation" on page 60.

NOTE: Your choice of performing the installation as an administrator or a non-administrator user should match the method that you used for installing the Identity Vault.

Installing as an Administrative User

This section describes the guided process for using the installation wizard to install the Identity Manager engine as an administrative user. The installation program is located at `\products\idm\windows\setup\idm_install.exe`.

To install the Identity Manager engine as an administrative user:

1. Log in as an administrator on the computer where you want to install the Identity Manager engine.
2. From the directory that contains the installation files, locate and run `idm_install.exe`.
3. Accept the license agreement, and then click **Next**.
4. In the Select Components window, specify the components that you want to install.

   For more information about the options, see "Understanding the Installation Program" on page 56.

5 (Optional) To select specific drivers for the individual components, complete the following steps:

  5a Click **Customize the selected components**, and then click **Next**.

  5b Expand **Drivers** under the component that you want to install.

  5c Select the drivers that you want to install.

6 Click **Next**.

7 In the Activation Notice window, click **OK**. For more information, see "Activating Identity Manager" on page 243.

8 For Authentication, specify a user account and its password with sufficient rights in eDirectory to extend the schema. Specify the user name in the LDAP format. For example, `cn=admin,o=company`.

9 For Pre-Installation Summary, verify the settings.

10 Click **Install**.

11 Activate Identity Manager. For more information, see "Activating Identity Manager" on page 243.

12 To create and configure your driver objects, consult the specific guide for that driver. For more information, see Identity Manager Drivers documentation website.

Performing a Silent Installation

To run a silent installation of Identity Manager, create a properties files with the parameters required to complete the installation. The Identity Manager media includes a sample properties file at `\products\idm\windows\setup\silent.properties`.

To perform a silent installation:

1 In the installation directory, create a properties file or edit the sample `silent.properties` file.

2 In a text editor, specify the following parameters in the file:

METADIRECTORY_SERVER_SELECTED

Specifies whether you want to install the Identity Manager server and drivers. The allowed values are `True` or `False`.

EDITION_INPUT_RESULTS

Specifies the edition of the Identity Manager server. For example, `Advanced Edition`.

EDIR_USER_NAME

Specifies the LDAP distinguished name of the Administrator account for the Identity Vault. For example, `c=admin,o=netiq`. The installation program uses this account to connect the Identity Manager engine to the Identity Vault.

You might need to add this parameter to the sample `silent.properties` file.

EDIR_USER_PASSWORD

Specifies the password for the Administrator account for the Identity Vault. For example, `netiq123`. You might need to add this parameter to the sample `silent.properties` file.

If you do not want to include the password value in the file, leave the field empty. The installation program then reads the value from the `EDIR_USER_PASSWORD` environment variable. Ensure that you have an environment variable for `EDIR_USER_PASSWORD`.

EDIR_IP_ADDRESS

Specifies the IP address for the Identity Vault.

If you have multiple instances of the Identity Vault, specify the address for each instance.

EDIR_NCP_PORT

Specifies the port number of the Identity Vault.

If you have multiple instances of the Identity Vault, specify the port for each instance.

CONNECTED_SYSTEM_SELECTED

Specifies whether you want to install the 32-bit Remote Loader service and drivers. You can install both 32-bit and 64-bit versions on the same server.

X64_CONNECTED_SYSTEM_SELECTED

Specifies whether you want to install the 64-bit Remote Loader service and drivers. You can install both 32-bit and 64-bit versions on the same server.

WEB_ADMIN_SELECTED

Applies when you have previously installed iManager.

Specifies whether you want to install iManager plug-ins.

UTLITIES_SELECTED

Specifies whether you want to install the Utilities and system components for the Remote Loader.

FANOUTAGENT_SELECTED

Specifies whether you want to install the Fan-Out agent for the JDBC driver.

DOT_NET_REMOTELOADER_SELECTED

Specifies whether you want to install the .NET Remote Loader service and drivers on the Windows server.

CUSTOM_SELECTED

Specifies whether you want to customize your driver installation options. The allowed values are `True` and `False`. If you select `False`, all Identity Manager drivers will be installed. If you select `True`, you can selectively install the required drivers by specifying the name of the drivers.

CHOSEN_INSTALL_FEATURE_LIST_SERVER: Specifies the drivers that you want to install with the Engine.

CHOSEN_INSTALL_FEATURE_LIST_REMOTE: Specifies the drivers that you want to install using the Remote Loader.

CHOSEN_INSTALL_FEATURE_LIST_REMOTE64BIT: Specifies the drivers that you want to install using the 64-bit Remote Loader.

CHOSEN_INSTALL_FEATURE_LIST_DOTNETRL: Specifies the drivers that you want to install using the .NET Remote Loader.

USER_MAGIC_FOLDER: Specifies the install location for the 32-bit Remote Loader.

X64_CONNECTED_SYSTEM_LOCATION: Specifies the install location for the 64-bit Remote Loader.

DOT_NET_REMOTELOADER_LOCATION: Specifies the install location for the .NET Remote Loader.

IDM_DRIVER_UTILITIES_DIR: Specifies the install location for the Identity Manager driver utilities.

IDM_FANOUT_AGENT_DIR: Specifies the install location for the FanOut Agent.

3 To run the silent installation, issue the following command from the directory for the properties file:

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

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

```
C:\Program Files (x86)\Novell\Identity
Manager\Identity_Manager_Install_<install-date>.log
```

and

```
%temp%\idmInstall.log
```

Installing on a Server with Multiple Instances of Identity Vault

Identity Manager supports this installation as an administrative user and in a silent mode. This procedure requires you to create a `silent.properties` file for each Identity Vault instance where you want to install Identity Manager.

Perform the following steps to install Identity Manager in the silent mode:

1 Review the prerequisites and system requirements in Chapter 4, “Planning to Install the Engine, Drivers, and Plug-ins,” on page 55.

2 Follow the instructions from “Performing a Silent Installation” on page 60.

2a Ensure that the silent.properties file includes the following settings:

```
EDITION_INPUT_RESULTS=Advanced Edition
EDIR_USER_NAME=cn=admin_name,o=organization_name
EDIR_USER_PASSWORD=identity_vault_password
METADIRECTORY_SERVER_SELECTED=true
CONNECTED_SYSTEM_SELECTED=false
X64_CONNECTED_SYSTEM_SELECTED=false
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
FANOUTAGENT_SELECTED=false
EDIR_NCP_PORT=<ncp_port>
EDIR_NDS_CONF=</path/to/edir/conf>
EDIR_IP_ADDRESS=ip_address_for_identity_vault

# For Customization use the following properties
CUSTOM_SELECTED=true
# engine custom list engine and drivers jdbc and delim
CHOSEN_INSTALL_FEATURE_LIST_SERVER=ENGINE,JDBC,DELIM,additional_val
ue
```

2b You can include the following additional values to customize the engine list:

- Server_DRIVERS
- AD
- EBSHR
- EBSTCA
- EBSUM
- DELIM
- EDIR
- BIEDIR
- JDBC
- JMS
- LDAP
- NXSET
- NOTES
- PS
- REMEDY
- SAPUMJ
- SAPHR
- SAPBL
- SAPPORTAL
- SOAP
- REST
- SFORCE
- SENTREST
- BLACK

- BANNER
- GOOGLE
- AR
- NPUM
- TSS
- RACF
- AFC2
- UAD
- RRSD

6 Installing the Remote Loader

In this section, you will install the Remote Loader, .NET Remote Loader, or the Java Remote Loader and configure driver instances in the loader.

The installation program for the Remote Loader is bundled with the Identity Manager engine. The files are located in the `\products\idm` directory in the Identity Manager installation package. By default, the installation program installs the components in `C:\Netiq`.

NetIQ recommends that you review the installation process before beginning. For more information, see "Checklist for Installing the Remote Loader" on page 65.

NOTE: Before installing the Remote Loader, you must have a good understanding of how Remote Loader works. For more information, see Deciding Whether to Use the Remote Loader in the *NetIQ Identity Manager Driver Administration Guide*.

Planning to Install the Remote Loader

This section provides information that helps you prepare for installing .NET Remote Loader.

- "Checklist for Installing the Remote Loader" on page 65
- "Understanding the Installation Program" on page 66
- "Using 32-bit and 64-bit Remote Loader on the Same Computer" on page 67
- "Prerequisites and Considerations for Installing the Remote Loader" on page 67

Checklist for Installing the Remote Loader

NetIQ recommends that you complete the steps in the following checklist:

	Checklist Items
❏	1. Review the planning information. For more information, see Part I, "Planning to Install Identity Manager," on page 17.
❏	2. Review the hardware and software requirements for the computers that will host the Remote Loader. For more information, see "Meeting System Requirements" on page 22 and "Prerequisites and Considerations for Installing the Remote Loader" on page 67.
❏	3. Ensure that the Identity Manager engine has been installed. For more information, see Chapter 5, "Installing the Engine, Drivers, and iManager Plug-ins," on page 59

	Checklist Items
□	4. (Conditional) To install the Remote Loader on a server that does not host the Identity Manager engine, ensure that you can establish a secure connection to the engine. For more information, see Creating a Secure Connection to the Identity Manager Engine in the *NetIQ Identity Manager Driver Administration Guide*.
□	5. Decide whether you want to install a 32-bit or 64-bit version of the Remote Loader. For more information, see "Using 32-bit and 64-bit Remote Loader on the Same Computer" on page 67.
□	6. Install the Remote Loader: ◆ For a guided installation, see "Using the Wizard to Install the Remote Loader" on page 68. ◆ For a silent installation, see "Performing a Silent Installation of the Remote Loader" on page 69.
□	7. (Conditional) To install the .NET Remote Loader, see "Installing .NET Remote Loader" on page 71.
□	8. To configure a driver instance in the Remote Loader, see one or all of the following sections in the *NetIQ Identity Manager Driver Administration Guide*: ◆ Configuring the Remote Loader for Driver Instances on Windows ◆ Configuring the Java Remote Loader for Driver Instances ◆ Configuring Mutual Authentication with the Identity Manager Engine ◆ Install and configure password synchronization for drivers. For more information, see the individual driver implementation guide in the Identity Manager Drivers Documentation page. ◆ Verifying the Configuration **NOTE:** *NetIQ Identity Manager Driver Administration Guide* provides detailed instructions about configuring the Remote Loader with drivers. You must refer to this guide for such instructions.
□	9. Install the rest of the Identity Manager components, including the identity applications and Identity Reporting.

Understanding the Installation Program

As a convenience, this installation program bundles several of the components that provide the underlying framework for your Identity Manager solution. You can choose to install all components on the same server or on individual servers. In addition to the Remote Loader, you can select the drivers that you want to install on the connected system. The installation kit provides .NET Remote Loader option for Windows operating systems.

Using 32-bit and 64-bit Remote Loader on the Same Computer

By default, the installation program detects the version of the operating system then installs the corresponding version of the Remote Loader. You can install both the 32-bit and 64-bit Remote Loader on a 64-bit operating system:

- If you are upgrading a 32-bit Remote Loader installed on a 64-bit operating system, the process upgrades the 32-bit Remote Loader to the latest version and also installs the 64-bit Remote Loader.
- If you choose to have both a 32-bit and a 64-bit Remote Loader on the same computer, the audit events are generated only with the 64-bit Remote Loader. If a 64-bit Remote Loader is installed before installing a 32-bit Remote Loader, the events are logged to the 32-bit cache.

Prerequisites and Considerations for Installing the Remote Loader

Before installing the Remote Loader, NetIQ recommends that you review the following considerations:

- Install the Remote Loader on a server that can communicate with the managed systems. The driver for each managed system must be available with the relevant APIs.
- You can install the Remote Loader on the same computer where you installed the Identity Manager engine.
- You can install both 32-bit and 64-bit Remote Loader on the same computer.
- You can install Java Remote Loader on platforms that do not support the native Remote Loader.
- (Conditional) To connect Identity Manager to Active Directory, you must install Remote Loader and the driver for Active Directory on a server that is a member server or a domain controller. You do not need to install eDirectory and Identity Manager on the same server as the connected system. The Remote Loader sends all of the events from Active Directory to the Identity Manager server. The Remote Loader then receives any information from the Identity Manager server and passes that to the connected application.

For more information about the Identity Manager Remote Loader, see Deciding Whether to Use the Remote Loader in *NetIQ Identity Manager Driver Administration Guide*.

Installing Remote Loader

The Remote Loader Console uses `rlconsole.exe` to interface with `dirxml_remote.exe`, which is an executable that enables the Identity Manager engine server to communicate with the Identity Manager drivers that are running.

- "Using the Wizard to Install the Remote Loader" on page 68
- "Performing a Silent Installation of the Remote Loader" on page 69
- "Installing Java Remote Loader" on page 69
- "Installing .NET Remote Loader" on page 71

Using the Wizard to Install the Remote Loader

The installation program guides you through the configuration settings for the Remote Loader. This section describes the guided process for using the installation wizard to install the Remote Loader. The installation program is present in the `\products\idm\windows\setup\` directory.

To prepare for the installation, see "Checklist for Installing the Remote Loader" on page 65. Also see the Release Notes accompanying the release. To perform an unattended installation, see "Performing a Silent Installation" on page 60.

NOTE: Your choice of performing the installation as an administrator or a non-administrator user should match the method that you used for installing the Identity Vault.

To install the Remote Loader:

1 Log in to the computer where you want to install Remote Loader.

> **NOTE:** You can install the Java Remote Loader as a non-administrator user.

2 Navigate to the `\products\idm\windows\setup\` directory.

3 Run the `idm_install.exe` program.

4 Accept the license agreement and then click **Next**.

5 In the **Select Components** window, specify the Remote Loader components that you want to install.

For more information about the options, see "Understanding the Installation Program" on page 56.

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 For Authentication, specify a user account and its password with sufficient rights in eDirectory to extend the schema. Specify the user name in the LDAP format. For example, `cn=admin,o=company`.

10 For Pre-Installation Summary, verify the settings.

11 Click **Install**.

12 Activate Identity Manager. For more information, see "Activating Identity Manager" on page 243.

13 Configure the Remote Loader to connect with the drivers and Identity Manager. For more information, see Chapter , "Configuring the Remote Loader and Drivers," on page 72.

14 To create and configure your driver objects, consult the specific guide for that driver. For more information, see Identity Manager Drivers documentation website.

Performing a Silent Installation of the Remote Loader

To run a silent installation of Remote Loader, create a properties files with the parameters required to complete the installation. The Identity Manager media includes a sample properties file. By default, the sample properties file is located at the `\products\idm\windows\setup\` directory.

To perform a silent installation:

1 Log in to the computer where you want to install Remote Loader.

2 Navigate to the `\products\idm\windows\setup\` directory

3 Create a properties file or edit the sample `silent.properties` file.

4 Specify the following parameters in the file:

CONNECTED_SYSTEM_SELECTED

Specifies whether you want to install the 32-bit Remote Loader service and drivers. You can install both 32-bit and 64-bit versions on the same server.

X64_CONNECTED_SYSTEM_SELECTED

Specifies whether you want to install the 64-bit Remote Loader service and drivers. You can install both 32-bit and 64-bit versions on the same server.

UTLITIES_SELECTED

Specifies whether you want to install the Utilities and system components for the Remote Loader.

DOT_NET_REMOTELOADER_SELECTED

Specifies whether you want to install the .NET Remote Loader service and drivers.

5 To perform a silent installation, run the following command from the command prompt:

```
install.exe -i silent -f silent.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 (1.8.0 minimum) 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 To access the installation program, complete one of the following steps:

4a (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the Java Remote Loader installation files, located by default in `products\idm\java_remoteloader`.

4b (Conditional) If you downloaded the Java Remote Loader installation files from the NetIQ Downloads website, complete the following steps:

4b1 Navigate to the `.tgz` file for the downloaded image.

4b2 Extract the contents of the file to a folder on the local computer.

5 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.

6 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.

7 On the target computer, unzip and extract the .tar.gz files.

For example, use 7-Zip or supported software to unzip .tar.gz files.

8 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
```

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

10 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.

11 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*.

12 Launch the Remote Loader using following commands:

12a To specify a Remote Loader password:

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

For example,

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

12b To start the Remote Loader:

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

For example,

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

12c To stop the Remote Loader:

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

For example,

```
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.

For more information about the options, see "Understanding the Installation Program" on page 56.

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.

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. For more information, see Configuring the Remote Loader and Drivers in the *NetIQ Identity Manager Driver Administration Guide*.

7 Installing iManager

This section guides you through the process of installing the required components for iManager. The setup programs can install the following components:

- iManager (server version)
- iManager Workstation (client version)
- Java
- Novell International Cryptographic Infrastructure (NICI)
- Tomcat

The installation files are located in the `\products\iManager\installs\`*`server_platform`*`\` directory within the `.iso` image file for the Identity Manager installation package. By default, the installation program installs the components in `C:\Novell`.

NetIQ recommends that you review the installation process before beginning. For more information, see Chapter , "Planning to Install iManager," on page 73.

Planning to Install iManager

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

- "Checklist for Installing iManager" on page 73
- "Understanding the Server and Client Versions of iManager" on page 74
- "Understanding Installation for iManager Plug-ins" on page 74
- "Prerequisites and Considerations for Installing iManager" on page 75

Checklist for Installing iManager

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

	Checklist Items
☐	1. Review the planning information. For more information, see Part I, "Planning to Install Identity Manager," on page 17.
☐	2. Review the hardware and software requirements for the computers that will host iManager. For more information, see "Meeting System Requirements" on page 22.
☐	3. Understand the difference between iManager and iManager Workstation. For more information, see "Understanding the Server and Client Versions of iManager" on page 74.

	Checklist Items
❑	4. Access the installation files for iManager, located by default in the `\products\iManager\installs\`*`server_platform`*`\` directory within the `.iso` image file for the Identity Manager installation package. Alternatively, download the installation files from the NetIQ Downloads website. Search for iManager products, select the iManager version that you want, then download the `win.zip` file to a directory on your server. For example, `iMan_31_win.zip`.
❑	5. (Optional) To learn more about the process for installing plug-ins, see "Understanding Installation for iManager Plug-ins" on page 74.
❑	6. (Optional) To review actions that you can perform after installing iManager, see "Post-Installation Tasks for iManager" on page 82.
❑	7. To install iManager and iManager Workstation, see the following sections: ◆ For GUI installation, see "Installing iManager Server and Workstation" on page 76 ◆ For a silent installation, see "Installing iManager Silently" on page 81

Understanding the Server and Client Versions of iManager

You must install iManager on a server that can access an eDirectory tree. To install iManager on a workstation instead of a server, you need the client-based version of iManager, the **iManager Workstation**. Use the following guidelines to decide which version fits best in your environment, or whether your eDirectory management policies would benefit from installing both versions:

- If you have a single administrator who always manages eDirectory from the same client workstation, you can take advantage of iManager Workstation. iManager Workstation is fully self-contained and requires little setup. It automatically starts and stops the resources it needs when it loads or unloads. iManager Workstation installs and runs on various Windows client workstations, has no dependencies on server-based iManager, and it can co-exist with any other versions of iManager installed on your network.

  iManager plug-ins do not automatically synchronize between iManager instances. If you have multiple administrators and use customized plug-ins, iManager Workstation and these plug-ins must be installed on each administrator's client workstation.
- If you manage eDirectory from multiple client workstations, or have multiple administrators, install iManager Server so that it is available from any connected workstation. Additionally, customized plug-ins only need to be installed once per iManager Server.

Understanding Installation for iManager Plug-ins

By default, the plug-in modules are not replicated between iManager servers. You must install the plug-in modules that you want on each iManager server.

In a clean install, the setup program preselects the "typical" plug-ins. For an upgrade, only plug-ins that need to be updated are preselected. You can override the default selections and add new plug-ins to download. However, for an upgrade, NetIQ recommends that you do not unselect any plug-in that was pre-selected. As a general rule, you should always upgrade plug-ins that you installed with a previous version of iManager. Also, more recent plug-ins might not be compatible with previous versions of iManager.

The base plug-ins for iManager are available only as part of the complete iManager software download (for example, eDirectory administrative plug-ins). Unless there are specific updates to these plug-ins, you can only download and install them with the entire iManager product.

The installation program uses an XML descriptor file, `iman_mod_desc.xml`, to identify the plug-ins that are available for downloading. The default URL for the file is http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. However, you can point the installation program to an alternative network URL. For example, you might be installing iManager behind a proxy or firewall that prevents the installation program from accessing the default URL.

For instructions about downloading and installing plug-ins, see the steps in one of the following sections:

- **GUI installation**: "Installing iManager Server and Workstation" on page 76
- **Silent installation**: "Installing iManager Silently" on page 81

For more information about customizing the process for downloading and installing plug-ins, see "Downloading and Installing Plug-in Modules" in the *NetIQ iManager Installation Guide*.

Prerequisites and Considerations for Installing iManager

This section provide information for installing server and workstation versions of iManager.

- "General Considerations for Installing iManager" on page 75
- "Considerations for Installing iManager Server" on page 76
- "Considerations for Installing iManager Workstation" on page 76

General Considerations for Installing iManager

Before installing iManager, review the following considerations:

- Identity Manager 4.7 supports eDirectory 9.1. Use iManager 3.1. For more information, see *iManager 3.1 Installation Guide*.
- If you plan to have more than 10 administrators regularly working in iManager at the same time, do not install iManager on the same server as other Identity Manager components.
- If you plan to have only one administrator, you can install iManager on the same server as the Identity Manager engine.
- If the iManager Server setup program detects a previously installed version of iManager, you can stop the installation process or remove the existing iManager, JRE, and Tomcat installations.
- Because iManager Workstation is a self-contained environment, you can install multiple versions on the same workstation, including older versions of Mobile iManager. However, you should not attempt to run them simultaneously. If you need to use different versions, run one version, close it, and then run the other version.
- You cannot run iManager Workstation from a path that includes spaces. For example, `C:\NetIQ\iManager Workstation\working`.
- You must have Administrator access for Windows servers.
- To create a Role-Based Services (RBS) collection in the eDirectory tree, you must have admin-equivalent rights.

- To run the iManager RBS Configuration Wizard, you must have admin-equivalent rights.
- To manage the same eDirectory tree with multiple versions of iManager, you must update your RBS Collection(s) to the latest iManager version.

Considerations for Installing iManager Server

If you are using Microsoft Internet Information Services (IIS) or Apache HTTP Server, you must manually integrate iManager with these web server infrastructures. By default, iManager uses Tomcat.

Considerations for Installing iManager Workstation

Before installing iManager Workstation on your Windows clients, NetIQ recommends that you review the following considerations:

- To enable Internet Explorer to use a proxy server for your LAN, you must specify **Bypass Proxy Server for Local Addresses** under **Tools** > **Internet Options** > **Connections** > **LAN Settings**.
- To run a Novell Client earlier than version 4.91, the NetIQ Modular Authentication Service (NMAS) client must be installed on the workstation before you launch iManager Workstation.
- If you run iManager Workstation from a path where any directory contains `temp` or `tmp` in the name, such as `c:\programs\temp\imanager`, iManager plug-ins do not install. Instead, run iManager Workstation from `C:\imanager` or a non-temporary directory.
- The first time that you run iManager Workstation on a Windows workstation, use an account that is a member of the workstation's Administrators group.

Installing iManager Server and Workstation

This chapter describes the process for installing iManager. To prepare for the installation, review the prerequisites and system requirements provided in "Prerequisites and Considerations for Installing iManager" on page 75.

To review the full installation process, see the "Planning to Install iManager" on page 73.

- "Installing iManager and iManager Workstation" on page 76
- "Installing iManager Silently" on page 81

Installing iManager and iManager Workstation

This section provides the steps for installing iManager and iManager Workstation on Windows servers and clients. To prepare for the installation, review the prerequisites and system requirements:

- **iManager**: "Considerations for Installing iManager Server" on page 76.
- **iManager Workstation**: "Considerations for Installing iManager Workstation" on page 76.
- Also see the Release Notes accompanying the release.

Installing iManager Server

The following procedure describes how to install the server version of iManager on a Windows server using an installation wizard. To perform a silent, unattended installation, see "Installing iManager Silently" on page 81.

If the setup program for iManager Server detects a previously installed version of iManager, it might give you the option to stop the installation process or remove the existing iManager, JRE, and Tomcat installations. When the setup program removes the previously installed version of iManager, it backs up the directory structure to the old *`TOMCAT_HOME`* directory to preserve any previously created custom content.

To install iManager Server:

1 Log in as a user with administrator privileges on the computer where you want to install iManager.

2 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the iManager installation files, located by default in the `\products\iManager\installs\win` directory.

3 (Conditional) If you downloaded the iManager installation files from the NetIQ Downloads website, complete the following steps:

3a Identify the `win.zip` file. For example, `iMan_310_win_x86_64.zip`.

3b Extract the `win.zip` file to a folder on the local computer.

4 Run `iManagerInstall.exe`.

5 (Optional) To view the debug output of the installation program, hold the `Ctrl` key immediately after launching the installation program until a console window appears. For more information about debugging, see "Troubleshooting" in the *NetIQ iManager Administration Guide*.

6 In the iManager welcome window, select a language, and then click **OK**.

7 In the **Introduction** window, and then click **Next**.

8 Accept the License Agreement, and then click **Next**.

9 (Conditional) If your server already has a version of JVM or Tomcat or other supporting components that are installed as part of iManager, in the **Detection Summary** window, complete the following steps:

9a Under **Install the following components**, verify that the versions listed for the components match the versions that you want to install.

9b (Optional) If the setup program does not list the versions that you want to install, browse to the appropriate components in the installation folder.

10 Click **Next**.

11 In the **Get PORT Input** window, specify the port numbers on which Tomcat server must run, and then click **Next**.

By default, the HTTP port and SSL port values are 8080 and 8443, respectively. However, if you have another service or Tomcat server using the default ports, you can specify different ports.

12 Specify the certificate public key algorithm that you want TLS certificate to use, then click **Next**. By default, the public key algorithm is set to **RSA**.

- **RSA:** The certificate uses a 2048-bit RSA key pair. If you select **RSA**, it allows four cipher levels. By default, the cipher level is set to **NONE**.
    - **NONE:** Allows any type of cipher.
    - **LOW:** Allows a 56-bit or a 64-bit cipher.
    - **MEDIUM:** Allows a 128-bit cipher.
    - **HIGH:** Allows ciphers that are greater than 128-bit.
- **ECDSA 256:** The certificate uses a ECDSA key pair with curve secp256r1. If you select **ECDSA 256**, it allows only one cipher level:
    - **SUITEB 128 ONLY:** Allows a 128-bit cipher.

For more information about ciphers, see the NetIQ iManager Administration Guide.

13 (Optional) To use IPv6 addresses with iManager, click **Yes** in the **Enable IPv6** window.

You can enable IPv6 addresses after you install iManager. For more information, see "Configuring iManager for IPv6 Addresses after Installation" on page 85.

14 Click **Next**.

15 In the **Choose Install Folder** window, specify the folder to store the installation files, and then click **Next**.

The default installation location is `C:\Program Files\Novell`.

16 (Optional) To download and install plug-ins as part of the installation, complete the following steps:

16a In the **Select Plug-ins to Download and Install** window, select the required plug-ins.

16b (Optional) To download plug-ins from an different network location, specify an alternative **Network URL**.

When using an alternative URL for downloading plug-ins, you must verify the URL contents, and verify that the plug-in is appropriate for your use. By default, the installation program downloads plug-ins from http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. For more information, see "Understanding Installation for iManager Plug-ins" on page 74.

16c Click **Next**.

16d (Conditional) The setup program might display the following message:

```
No new or updated plug-ins found. All plug-ins are downloaded or
updated or the iManager download server is unavailable.
```

If you see this error, one or more of the following conditions exist:

- There are no updated plug-ins available from the download site.
- There is a problem with your Internet connection. Verify your connection and try again.
- Connection to the Descriptor File (http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml) was not successful. This URL refers to an XML descriptor file of available iManager plug-ins.
- The iManager installation is behind a proxy that does not allow a connection to the above URL.

16e (Optional) To install plug-ins from a local directory, in the Select Plug-ins to Install from Disk window, specify the directory path that contains the appropriate `.npm` plug-in files.

This step allows you to install previously downloaded or custom plug-ins. The default path is `\`*`extracted location`*`\products\iManager\plugins`. However, you can specify any valid path.

16f Click **Next**.

17 (Optional) In the **Get User and Tree Names** window, specify an authorized user and the name of the eDirectory tree that this user will manage.

NOTE

- If eDirectory uses a port other than the default port 524, you can specify the IP address or DNS name of the eDirectory server plus the port number. Do not use `localhost`. For example, to specify an IPv6 address, enter `https://[2001:db8::6]:1080/nps/servlet/webacc?taskId=fw.Startup&forceMaster=true`.
- NetIQ does not recommend leaving these settings blank. If you leave these fields blank, iManager allows any user to install plug-ins and make changes to iManager server settings. You can specify an authorized user after completing the installation process. For more information, see "Specifying an Authorized User for eDirectory" on page 85.
- The installation program does not validate the specified user credentials with eDirectory.

---

18 Click **Next**.

19 Read the Pre-installation summary page, and then click **Install**.

20 When the installation completes, the **Install Complete** window displays relevant messages about the success of the process.

NOTE: Despite a successful installation, the **Install Complet**e window might display the following error message:

```
The installation of iManager version is complete, but some errors
occurred during the install.
Please see the installation log Log file path for details. Press "Done"
to quit the installer.
```

---

21 (Conditional) If the installer displays the error message shown in Step 20, complete the following steps:

21a Note the path to the log file that the error message displays.

21b In the **Install Complete** window, click **Done**.

21c Open the log file.

21d (Conditional) If you find the following error in the log file, you can ignore the error message. The installation was successful, and iManager functions properly.

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class
com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The
process cannot access the file because it is being used by another
process)
```

21e (Conditional) If the log file does not contain the error listed in Step 21d, NetIQ recommends that you retry the installation.

22 Click **Done**.

23 When the initialization of iManager finishes, click the first link in the Getting Started page, an then log in. For more information, see "Accessing iManager" in the *NetIQ iManager Administration Guide*.

Installing iManager Workstation

iManager Workstation is a self-contained environment. You can install multiple versions on the same workstation (including older versions of Mobile iManager). However, you should not attempt to run them concurrently. If you need to use different versions, run one version, close it, and then run the other version.

NOTE: You cannot run iManager Workstation from a path that includes spaces. For example, `C:\NetIQ\iManager Workstation\working`.

To install iManager Workstation:

1 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the iManager installation files, located by default in the `\products\iManager\installs\win\` directory.

2 (Conditional) If you downloaded the iManager installation files from the NetIQ Downloads website, complete the following steps:

2a Identify the `win.zip` file. For example, `iMan_31_workstation_win.zip`.

2b Extract the `win.zip` file to a folder on the local computer.

3 From the `imanager\bin` folder, run the `iManager.bat` file.

4 In the iManager login window, specify the credentials for an authorized user and the eDirectory tree that this user manages.

For more information about accessing iManager, see "Accessing iManager" in the *NetIQ iManager Administration Guide*.

5 (Optional) To enable IPv6 addresses, complete the following steps:

1. Open the `*User_Install_Directory*\Tomcat\conf\catalina.properties` file.
2. Set the following configuration entries in the `catalina.properties` file:

```
java.net.preferIPv4Stack=false
java.net.preferIPv4Addresses=true
```

3. Restart the Tomcat service.

Installing iManager Silently

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, InstallAnywhere uses information from a default `install.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process.

To prepare for the installation, review the prerequisites and system requirements:

- **iManager Server**: "Considerations for Installing iManager Server" on page 76.
- **iManager Workstation**: "Considerations for Installing iManager Workstation" on page 76.
- Also see the Release Notes accompanying the release.

Editing the Properties File for a Customized Silent Installation

For more control over which modules are installed, you can customize the silent installation process.

1 Open the `install.properties` file, located by default in the *`products/`*`iManager` directory within the `.iso` image file for the Identity Manager installation package for each operating system environment directory.

> **NOTE:** If you previously installed the current version of iManager on a server, you can use the `installer.properties` file that setup program generated. The file, located by default in the `log` directory, contains the values that you specified during the installation.

2 In the properties file, add the following parameters and values:

`$PLUGIN_INSTALL MODE$`

Specifies the property that controls whether plug-ins are installed. Add one of the following values:

- `DISK` - (default) instructs the setup program to install the plug-ins from the local disk.
- `NET` - instructs the setup program to install the plug-ins from the network.
- `BOTH` - instructs the setup program to install the plug-ins from both disk and network.
- `SKIP` - does not install the plug-ins.

`$PLUGIN_DIR$`

Specifies an alternate path to plug-ins located on the local disk. The default path is `\`*`installer_root_directory`*`\iManager\installs\`*`platform path`*`\plugin`.

The installation program installs all modules in the plug-in directory, except for subdirectories.

`$PLUGIN_INSTALL_URL$`

Specifies the network URL where the installation program can download the plug-ins, by default http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. If you specify an alternative URL, you must verify the URL contents, and verify that the plug-in is appropriate for your use. For more information, see "Understanding Installation for iManager Plug-ins" on page 74.

$LAUNCH_BROWSER$

Specifies whether the installation program launches the `gettingstarted.html` file launches once the installation process completes.

$USER_INSTALL_DIR$

Specifies the path where you want iManager to be installed.

USER_INPUT_ENABLE_IPV6

Specifies whether to enable iManager to use IPv6 addresses. By default, the installation program sets this value to `yes`.

3 For each plug-in module that you want to download and install, specify the module ID and version from the `MANIFEST.MF` file, located in the `META-INF/` folder of the `.npm` (plug-in module). For example:

```
$PLUGIN_MODULE_ID_1$=eDirectoryBackupAndRestore

$PLUGIN_VERSION_1$=2.7.20050517

$PLUGIN_MODULE_ID_2$=ldap

$PLUGIN_VERSION_2$=2.7.20050517
```

NOTE

- If you do not specify any modules, the program installs the most commonly installed modules, tagged as "selected" in the `iman_mod_desc.xml` files on the download website.
- If you do not define a version for a module, the setup program installs any module that matches the `.npm` name.

Running a Silent Installation for iManager

You can silently install iManager using the default values in the `install.properties` file, located by default in the `\`*`products`*`\iManager` directory within the `.iso` image file for the Identity Manager installation package for each operating system environment directory. The `\`*`products`*`\iManager` directory should also contain the installation executable file.

1 In a console window, go to the directory containing the `install.properties` file that you downloaded.

2 On the command line, enter one of the following command:

```
iManagerInstall.exe -i silent
```

Post-Installation Tasks for iManager

After you install iManager, you can modify the configuration settings, such as enabling IPv6 addressing or changing the authorized user for an eDirectory tree. Also, NetIQ recommends that you replace the self-signed certificates that the installation process created.

- "Replacing the Temporary Self-Signed Certificates for iManager" on page 83
- "Configuring iManager for IPv6 Addresses after Installation" on page 85
- "Specifying an Authorized User for eDirectory" on page 85

Replacing the Temporary Self-Signed Certificates for iManager

Standalone iManager installations include a temporary, self-signed certificate for use by Tomcat. It has an expiration date of one year. NetIQ provides this certificate to help you get your system up and running so you can securely use iManager immediately after you install the product. NetIQ and OpenSSL do not recommend using self-signed certificates except for testing purposes. Instead, you should replace the temporary certificate with a secure one.

Tomcat stores the self-signed certificate in a keystore that uses Tomcat (JKS) format file. Normally, you would import a private key to replace the certificate. However, the `keytool` that you use to modify the Tomcat keystore cannot import a private key. The tool only uses a self-generated key.

This section explains how to generate a public/private key pair in eDirectory using NetIQ Certificate Server and to replace the temporary certificate. If you are using eDirectory, you can use NetIQ Certificate Server to securely generate, track, store, and revoke certificates with no further investment.

Replacing the iManager Self-Signed Certificates

This section describes how to create a keypair in eDirectory and export the Public, Private, and Root Certificate Authority (CA) keys with a PKCS#12 file. This includes modifying Tomcat's `server.xml` configuration file to use the PKCS12 directive and point the configuration to an actual P12 file rather than use the default JKS keystore.

This process uses the following files:

- `C:\Program Files\Novell\Tomcat\conf\ssl\.keystore`, which holds the temporary keypair
- `C:\Program Files\Novell\jre\lib\security\cacerts`, which holds the trusted root certificates
- `C:\Program Files\Novell\Tomcat\conf\server.xml`, which is used for configuring Tomcat's use of certificates

To replace the self-signed certificates:

1 To create a new certificate, complete the following steps:

   1a Log in to iManager.

   1b Click **NetIQ Certificate Server** > **Create Server Certificate**.

   1c Select the appropriate server.

   1d Specify a nickname for the server.

   1e Accept the rest of the certificate defaults.

2 To export the server certificate, complete the following steps:

   2a In iManager, select **Directory Administration** > **Modify Object**.

   2b Browse to and select the Key Material Object (KMO) object.

   2c Click **Certificates** > **Export**.

   2d Specify a password.

   2e Save the server certificate as a PKCS#12 (`.pfx`).

3 To convert the `.pfx` file to a `.pem` file, complete the following steps:

NOTE: OpenSSL is not installed by default. However, you can download a version from the OpenSSL website.

3a Enter a command, such as `openssl pkcs12 -in newtomcert.pfx -out newtomcert.pem`.

3b Specify the same password for the certificate that you specified in Step 2.

3c Specify a password for the new `.pem` file.

You can use the same password, if desired.

4 To convert the `.pem` file to a `.p12` file, complete the following steps:

4a Enter a command, such as `openssl pkcs12 -export -in newtomcert.pem -out newtomcert.p12 -name "New Tomcat"`.

4b Specify the same password for the certificate that you specified in Step 3.

4c Specify a password for the new `.p12` file.

You can use the same password, if desired.

5 Copy the `.p12` file to the Tomcat certificate location, by default `C:\Program Files\Novell\Tomcat\conf\ssl\`.

6 Stop the Tomcat Service by using the `services.msc` startup script.

7 To ensure that Tomcat uses the newly created `.p12` certificate file, add `keystoreType`, `keystoreFile`, and `keystorePass` variables to the Tomcat `server.xml` file. For example:

```
<Connector className="org.apache.coyote.http11.Http11AprProtocol"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory
className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
 clientAuth="false" protocol="TLS" keystoreType="PKCS12"
 keystoreFile="C:\Program Files\Novell\Tomcat\conf\ssl\newtomcert.p12"
keystorePass="password" />
```

Or,

```
<Connector className="org.apache.coyote.http11.Http11NioProtocol"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory
className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
 clientAuth="false" protocol="TLS" keystoreType="PKCS12"
 keystoreFile="C:\Program Files\Novell\Tomcat\conf\ssl\newtomcert.p12"
keystorePass="password" />
```

When setting the keystore type to PKCS12, you must specify the entire path to the certificate file, as Tomcat will no longer default to using the Tomcat home path.

8 Start the Tomcat service by using the `services.msc` startup script.

Configuring iManager for IPv6 Addresses after Installation

After installing iManager, you can enable iManager to use IPv6 addresses.

1. Open the `catalina.properties` file in the installation directory, located by default *`installation_directory`*`\Tomcat\conf`.
2. Set the following configuration entries in the properties file:

   ```
   java.net.preferIPv4Stack=false
   ```

   ```
   java.net.preferIPv4Addresses=true
   ```

3. Restart Tomcat.

Specifying an Authorized User for eDirectory

After installing iManager, you can modify the credentials for the authorized user and the appropriate eDirectory tree name that this user manages. For more information, see "iManager Authorized Users and Groups" in the *NetIQ iManager Administration Guide*.

1 Log in to iManager.

2 In the Configure view, select **iManager Server** > **Configure iManager** > **Security**.

3 Update the user credentials and tree name.

III Installing Identity Applications

This section guides you through the process of installing the components and framework required for the identity applications:

- Identity Applications Administration
- Identity Applications Dashboard
- Role and Resource Service driver
- User Application
- User Application driver

By default, the installation program installs these components in `C:\NetIQ\idm\apps`.

The identity applications require access to other Identity Manager components during and after installation. NetIQ recommends that you review the installation process before beginning. For more information, see "Planning to Install the Identity Applications" on page 115.

8 Installing PostgreSQL and Tomcat for Identity Manager

In this section, you will install the following application server and database programs that are used by most of the Identity Manager components:

- Apache Tomcat
- PostgreSQL

The installation files are located in the `\products\CommonApplication\` directory in the Identity Manager installation package. By default, the installation program installs the applications in `C:\NetIQ\idm\apps\`.

NetIQ recommends that you review the installation process before beginning. For more information, see "Checklist for Installing Tomcat and PostgreSQL" on page 89.

Planning to Install PostgreSQL and Tomcat

From Identity Manager 4.6, NetIQ supports only Apache Tomcat as an application server. If your company provides a supported version of Tomcat, you can use it with Identity Manager.

Alternatively, NetIQ bundles Tomcat and PostgreSQL in the same installation program for your convenience. This installer lets you install these applications without downloading them separately. NetIQ does not provide updates for these components, or administration, configuration, or tuning information beyond what is outlined in the NetIQ Identity Manager documentation.

- "Checklist for Installing Tomcat and PostgreSQL" on page 89
- "Understanding the Installation Process for PostgreSQL and Tomcat" on page 90
- "Prerequisites for Installing PostgreSQL" on page 91
- "Prerequisites for Installing Tomcat" on page 91
- "System Requirements for PostgreSQL" on page 92
- "System Requirements for Tomcat" on page 92

Checklist for Installing Tomcat and PostgreSQL

NetIQ recommends that you complete the steps in the following checklist:

	Checklist Items
☐	1. Review the planning information. For more information, see Part I, "Planning to Install Identity Manager," on page 17.

	Checklist Items
□	2. Review the hardware and software requirements for the computers that will host the Identity Vault. For more information, see the following sections: ◆ “Meeting System Requirements” on page 22. ◆ “Prerequisites for Installing Tomcat” on page 91 ◆ “Prerequisites for Installing PostgreSQL” on page 91
□	3. Decide whether you should install NetIQ Sentinel before installing Tomcat or PostgreSQL. For more information, see “Recommended Installation Scenarios and Server Setup” on page 21. **NOTE:** Sentinel installation is supported only on a Linux server. To install Sentinel, you must have a Linux server in your environment.
□	4. Install the applications: ◆ For a guided installation, see “Using the Wizard to Install PostgreSQL and Tomcat” on page 92. ◆ For a silent installation, see “Silently Installing Tomcat and PostgreSQL for Identity Manager” on page 94.
□	5. Install the rest of the Identity Manager components.

Understanding the Installation Process for PostgreSQL and Tomcat

You can choose to install one or both of the applications. For example, you might not need PostgreSQL because you already have a supported version of the application on the server. The following considerations apply to the individual installations:

PostgreSQL

The installation process installs the database for the identity applications and creates an administrative user called `idmadmin` to own the database. However, the installation does not create the schema in the database for the identity applications. Schema information gets added when you install the identity applications.

If you already have a supported version of PostgreSQL running on the server, the installation program prompts you for the password for the default `postgres` user. The program then creates the `idmadmin` user and assigns it the same password as for `postgres`.

At the end of the process, the installation program starts the database instance. The instance must be running when you install other Identity Manager components that use the database, such as the User Application.

You are not required to use PostgreSQL for the database for identity applications.

Tomcat

The installation process creates the IDM Apps Tomcat Service. To support the Tomcat application server, the installation program also installs Apache ActiveMQ and Oracle JRE. These items help Tomcat send email notifications.

The installation program does not start Tomcat upon completion. Tomcat must be stopped before you install other Identity Manager components, such as Identity Reporting.

Prerequisites for Installing PostgreSQL

Review the following considerations before planning the PostgreSQL installation:

- You can install the version of PostgreSQL bundled with Identity Manger in an environment that runs an older version of the database program. To ensure that the new installation does not overwrite the previous version, specify a different directory for the files.
- The identity applications apply some prerequisites to the database they use, such as PostgreSQL. For more information, see "Prerequisites for Installing the Database for the Identity Applications" on page 120.
- You cannot install more than one version of PostgreSQL because the service account for PostgreSQL does not handle both instances. Uninstall the old version before installing this version of PostgreSQL.

Prerequisites for Installing Tomcat

Review the following considerations before planning the Tomcat installation:

- You can install Tomcat and PostgreSQL on the same server or on separate servers.
- The installation process installs supported versions of Oracle JRE and Apache ActiveMQ.
- The installation process also installs the files required for the Apache Log4j service to audit Tomcat events.
- You can use your own Tomcat installation program instead of the one provided in the Identity Manager installation kit. However, to use the Apache Log4j service with your version of Tomcat, ensure that you have the appropriate files installed. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 98. This requirement applies to using Tomcat for OSP, the identity applications, and Identity Reporting.
- To have guaranteed delivery of email notifications with ActiveMQ, install MQServer.
- The identity applications apply some prerequisites to the Tomcat application server on which they run. For more information, see "Prerequisites and Considerations for the Application Server" on page 119.
- The installation process sets the JRE location in the `setenv.bat` file, located by default in the `c:\NetIQ\idm\apps\tomcat\bin` directory. When you install the identity applications and Identity Reporting on Tomcat, the process updates the `JAVA_OPTs` or `CATALINA_OPTS` entries in the `setenv.bat` file.

System Requirements for PostgreSQL

PostgreSQL has the same computer requirements as for the identity applications. For more information, see "Meeting System Requirements" on page 22. Also see the release notes for the latest version of Identity Manager and the PostgreSQL documentation.

System Requirements for Tomcat

Tomcat has the same computer requirements as for the identity applications. For more information, see "Meeting System Requirements" on page 22. Also see the release notes for the latest version of Identity Manager and the Apache documentation.

Installing PostgreSQL and Tomcat

This section guides you through the process of installing Tomcat and PostgreSQL.

- "Using the Wizard to Install PostgreSQL and Tomcat" on page 92
- "Silently Installing Tomcat and PostgreSQL for Identity Manager" on page 94

Using the Wizard to Install PostgreSQL and Tomcat

The following procedure describes how to install Tomcat and PostgreSQL on a Windows platform using a guided process. To perform a silent, unattended installation, see "Silently Installing Tomcat and PostgreSQL for Identity Manager" on page 94.

To prepare for the installation, review the considerations and system requirements listed in the following sections:

- "Prerequisites for Installing Tomcat" on page 91
- "Prerequisites for Installing PostgreSQL" on page 91
- Release Notes accompanying the release

NOTE: Whether you install PostgreSQL or use an existing version of PostgreSQL, you must specify passwords for the database. However, this installation program does not support passwords that include a " or $ character. To use these special characters, change the password after you complete the installation process.

To perform a guided installation:

1. Log in as an administrator to the computer where you want to install the applications.
2. Ensure that the planned installation path does not include directories with any of the following names:
    - tomcat
    - postgres
    - activemq
    - jre

NOTE: While installing Standard Edition, you must install ActiveMQ. Otherwise, the Reporting page does not load after you log in to Identity Reporting. Alternatively, copy the `activemq-all-5.15.2 jar` file into `C:\NetIQ\idm\apps\tomcat\lib` directory after completing the PostgreSQL installation and then restart Tomcat.

3. (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to `\products\CommonApplication\postgre_tomcat_install` directory containing the installation files.
4. (Conditional) If you downloaded the installation files from the NetIQ Downloads website, complete the following steps:

   4a Navigate to the `win.zip` file for the downloaded image.

   4b Extract the contents of the file to a directory on the local computer.
5. From the directory that contains the installation files, run `TomcatPostgreSQL.exe`.
6. In the installation program, specify the language that you want to use for installation, and then click **OK**.
7. Review the introductory information, and then click **Next**.
8. Accept the License Agreement, and then click **Next**.
9. Specify whether you want to install Tomcat, PostgreSQL, or both.
10. To complete the guided process, specify values for the following parameters:

    - **Tomcat parent folder**

      Applies only when installing Tomcat.

      Specifies the directory where you want to install the Tomcat files.
    - **Tomcat details**

      Applies only when installing Tomcat.

      Represents the ports needed for Tomcat.

      Tomcat shutdown port

      Specifies the port that you want to use for cleanly shutting down all webapps and Tomcat. The default is 8005.

      Tomcat http port

      Specifies the port that you want the Tomcat server to use for communication with client computers. The default is 8080. To use SSL, the default is 8443.

      Tomcat redirect port

      (Conditional) When you do not use TLS/SSL protocols, specifies the port to which the application server redirects requests that require SSL transport. The default value is 8443.

      Tomcat ajp port

      (Optional) Specifies the port that you want the application server to use for communication with a web connector using the AJP protocol instead of `http`. The default value is 8009.

      Use this parameter when you want the application server to manage the static content contained in the web application, and/or utilize the application server’s SSL processing.

- **PostgreSQL parent folder**

  Applies only when installing PostgreSQL.

  Represents the directory where you want to install the PostgreSQL files.

- **PostgreSQL details**

  Applies only when installing PostgreSQL.

  Represents the settings for the PostgreSQL database for the identity applications.

  NOTE: If you already have a supported version of PostgreSQL running on the server, the installation program prompts you for the password for the default `postgres` user. The program then creates the `idmadmin` user and assigns it the same password as for `postgres`.

  This installation program does not support passwords that include a " or $ character.

  Database name

  Specifies the name of the database. The default value is `idmuserappdb`.

  Database admin

  Specifies the `idmadmin` account, which is a database administrator that can create database tables, views, and other artifacts.

  This account is not the same as the default postgres user.

  Password for admin user

  Specifies the password for the database administrator and the default `postgres` user.

  This installation program does not support passwords that include a " or $ character.

  PostgreSQL port

  Specifies the port of the server that hosts the Postgres database. The default value is 5432.

11 Review the pre-installation summary.

12 Start the installation process.

13 When the installation process completes, click *Done*.

Silently Installing Tomcat and PostgreSQL for Identity Manager

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, InstallAnywhere uses information from a default `silent.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process. For a guided installation, see "Using the Wizard to Install PostgreSQL and Tomcat" on page 92.

To prepare for the installation, review the considerations and system requirements listed in the following sections:

- "Prerequisites for Installing Tomcat" on page 91
- "Prerequisites for Installing PostgreSQL" on page 91
- "Safeguarding the Passwords for a Silent Installation" on page 95
- Release Notes accompanying the release

Safeguarding the Passwords for a Silent Installation

If you do not want to specify the passwords in the `postgresq_tomcat-silent.properties` file for the installation, you can set the passwords in the environment instead. In this case, the silent installer will read the passwords from the environment, rather than from the `postgresq_tomcat-silent.properties` file. This can provide some additional security.

You must specify the following passwords for the installation:

- NETIQ_DB_PASSWORD
- NETIQ_DB_PASSWORD_CONFIRM

Use the `set` command. For example:

```
set NETIQ_DB_PASSWORD_CONFIRM=myPassWord
```

The installation program does not support passwords that include a " for $ character. To use these special characters, change the password after installing PostgreSQL.

Silently Installing Tomcat and PostgreSQL

1. Log in to the computer where you want to install the applications.
2. (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to `\products\CommonApplication\postgre_tomcat_install` directory containing the installation files.
3. (Conditional) If you downloaded the installation files from the NetIQ Downloads website, complete the following steps:

   3a Navigate to the `win.zip` file for the downloaded image.

   3b Extract the contents of the file to a directory on the local computer.

4. To specify the installation parameters, complete the following steps:

   4a Ensure that the `postgresq_tomcat-silent.properties` file is located in the same directory as the execution file for installation.

   4b In a text editor, open the `postgresq_tomcat-silent.properties` file.

   4c Specify the parameter values. For a description of the parameters, see Step 10 on page 93.

   4d Save and close the file.

5. To launch the installation process, enter the following command:

   ```
   TomcatPostgreSQL -i silent -f postgresq_tomcat-silent.properties
   ```

   NOTE: If the `postgresq_tomcat-silent.properties` file resides in a different directory from the installation script, you must specify the full path to the file. The script unpacks the necessary files to a temporary directory and then launches the silent installation.

9 Installing the Single Sign-on Component

In this section, you will install One SSO Provider (OSP) to support single sign-on access to the identity applications and Identity Reporting.

The installation files are located in the `products\CommonApplication\osp_install` directory in the Identity Manager installation package. By default, the installation program installs the components in `C:\NetIQ\idm\apps\osp`.

NetIQ recommends that you review the installation process before beginning.

Planning to Install Single Sign-on for Identity Manager

This section provides information prerequisites, considerations, and system setup that are needed to install One SSO Provider (OSP).

- “Checklist for Single Sign-on Component” on page 97
- “Prerequisites for Installing One SSO Provider” on page 98
- “System Requirements for One SSO Provider” on page 98
- “Using the Apache Log4j Service to Log Sign-on” on page 98

Checklist for Single Sign-on Component

NetIQ recommends that you complete the steps in the following checklist:

	Checklist Items
□	1. Review the planning information. For more information, see Part I, “Planning to Install Identity Manager,” on page 17.
□	2. Review the hardware and software requirements for the computers that will host OSP. For more information, see “Meeting System Requirements” on page 22.
□	3. Ensure that Tomcat has been installed. For more information, see “Installing PostgreSQL and Tomcat” on page 92.
□	4. (Conditional) To use the Apache Log4j service to record events in Tomcat, ensure that you have the appropriate files. For more information, see “Using the Apache Log4j Service to Log Sign-on” on page 98.
□	5. Install OSP: • For a guided installation, see “Using the Wizard to Install One SSO Provider” on page 99. • For a silent installation, see “Silently Installing One SSO Provider” on page 102.

	Checklist Items
❑	6. Install Self Service Password Reset (SSPR) to manage user passwords for Identity applications. For more information, see Section 10, "Installing the Password Management Component," on page 105.
❑	7. Install and configure the identity applications to use single sign-on access. For more information, see "Installing the Identity Applications" on page 127.

Prerequisites for Installing One SSO Provider

The following Identity Manager components require OSP for user authentication:

- Identity Applications
- Identity Reporting

Before installing OSP, NetIQ recommends that you review the following considerations:

- To run OSP, you can use your own Tomcat installation program instead of the one provided in the Identity Manager installation kit. However, to use the Apache Log4j service with your version of Tomcat, ensure that you have the appropriate files installed. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 98.
- OSP requires trust certificates to ensure that the identity applications and reporting can communicate with the authentication server. The installation process automatically creates a certificate for TLS/SSL in the `osp.jks` file. You can also have the process create the Trusted Root Certificate for a SAML Assertion to eDirectory.

  NOTE: These certificates expire two years after their creation date. You must create new certificates when the original ones expire. For more information, see "Authentication Server" on page 175 and Configuring Single Sign-on Access in Identity Manager in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

System Requirements for One SSO Provider

OSP requires Apache Tomcat application server. The version of Tomcat must be the same as required for the identity applications.

All other server requirements match the server requirements for the identity applications. For more information, see "Prerequisites and Considerations for Installing the Identity Applications" on page 117 and the most recent Release Notes for this version.

Using the Apache Log4j Service to Log Sign-on

You can use either the Apache Log4j or java.util.logging service to record events that occur in Tomcat. The Tomcat installer in the Identity Manager installation kit includes the files that you need for Log4j. However, if you install your own version of Tomcat, you need the following files to use the Apache logging service:

- `log4j-1.2.16.jar`

- tomcat-juli-adapters.jar
- tomcat-juli.jar

To add the files to your Tomcat installation, complete the following steps:

1. Download the "JULI" files for Tomcat v8.5.x from the Apache website:
   - tomcat-juli.jar
   - tomcat-juli-adapters.jar
2. Download the log4j-1.2.16.jar file from the Apache website.
3. Place the following files in the $TOMCAT_HOME\lib directory:
   - log4j-1.2.16.jar
   - tomcat-juli-adapters.jar
4. Place the tomcat-juli.jar file in the $TOMCAT_HOME\bin directory.
5. Specify a value for -Dlog4j.configuration in CATALINA_OPTS or create a log4j.properties file in the $TOMCAT_HOME\lib directory.

Installing Single Sign-on for Identity Manager

- "Using the Wizard to Install One SSO Provider" on page 99
- "Silently Installing One SSO Provider" on page 102
- "Configuring Single Sign-on Access" on page 103

Using the Wizard to Install One SSO Provider

The following procedure describes how to install OSP on a Windows platform using an installation wizard. To perform a silent, unattended installation, see "Silently Installing One SSO Provider" on page 102. To prepare for the installation, review the prerequisites and system requirements listed in "Checklist for Single Sign-on Component" on page 97.

1. Log in as an administrator to the server where you want to install OSP.
2. Stop the Tomcat server.
3. (Conditional) If you have the .iso image file for the Identity Manager installation package, navigate to the directory containing the OSP installation files, located by default in the products\CommonApplication\osp_install directory.
4. (Conditional) If you downloaded the OSP installation files, complete the following steps:

   4a Navigate to the win.zip file for the downloaded image.

   4b Extract the contents of the file to a directory on the local computer.
5. From the directory that contains the installation files, run the osp-install-win.exe file.
6. Read and accept the license agreement, and then click **Next**.
7. Specify a path for the installed files.

8 Complete the guided process, using the following parameters:

- **Tomcat details**

  Represents the home directory for the Tomcat server. For example, `C:\NetIQ\idm\apps\tomcat\`. The installation process adds some files for OSP to this folder.

- **Tomcat Java home**

  Represents the home directory for Java on the Tomcat server. For example, `C:\NetIQ\idm\jre`. The installation process adds some files for OSP to the directory.

- **Application address**

  Represents the settings of the URL that users need to connect to OSP on the Tomcat server. For example, `https://myserver.mycompany.com:8543`.

  Protocol

  Specifies whether you want to use *http* or *https*. To use Secure Sockets Layer (SSL) for communications, specify `https`.

  Host Name

  Specifies the DNS name or IP address of the server where you are installing OSP. Do not use `localhost`.

  Port

  Specifies the port that you want the server to use for communication with client computers.

- **Login Screen Customization**

  Specifies the custom name that you want to display on user login screen. The default value is **Identity Access**.

  (Conditional) When you upgrade OSP, the login screen name automatically changes to **Identity Access**.

  NOTE: Only `Latin1 Standard character set` is supported.

- **Authentication details**

  Represents the requirements for connecting to the authentication server which contains the list of users who can log in to the application.

  LDAP host

  Specifies the DNS name or IP address of the LDAP authentication server. Do not use `localhost`.

  LDAP port

  Specifies the port that you want the LDAP authentication server to use for communication with Identity Manager. For example, specify 389 for a non-secure port or 636 for SSL connections.

  Use SSL

  Specifies whether you want to use Secure Sockets Layer protocol for connections between the Identity Vault and the authentication server.

JRE Trust store (cacerts) file

Applies only when you want to use SSL for the LDAP connection.

Specifies the path to the certificate. For example, `C:\NetIQ\idm\apps\jre\lib\security\cacerts`.

JRE Trust store password

Applies only when you want to use SSL for the LDAP connection.

Specifies the password for the `cacerts` file.

Admin DN

Applies only when installing a new authentication server.

Specifies the DN for an administrator account of the LDAP authentication server. For example, `cn=admin,ou=sa,o=system`.

Admin password

Applies only when installing a new authentication server.

Specifies the password for the administrator account of the LDAP authentication server.

User container

Applies only when installing a new authentication server.

Specifies the container in the LDAP authentication server where you store the user accounts that can log in to Access Review. For example, `o=data`.

Admin container

Applies only when installing a new authentication server.

Specifies the container in the LDAP authentication server where you store the administrator accounts. For example, `ou=sa,o=system`.

Identity Vault

Specifies your Identity Vault.

Keystore Password

Applies only when installing a new authentication server.

Specifies the password that you want to create for the new keystore for the LDAP authentication server.

The password must be a minimum of six characters.

- **Auditing details (OSP)**

Represents the settings for auditing OSP events that occur in the authentication server.

(Conditional) *Enable auditing for OSP*

Specifies whether you want to send OSP events to an auditing server.

If you select this setting, also specify the location for the audit log cache.

Audit log cache folder

Applies only when you enable auditing for OSP.

Specifies the location of the cache directory that you want to use for auditing. For example, `C:\NetIQ\idm\naudit\jcache`.

Specify existing certificate / Generate a certificate

Indicates whether you want to use an existing certificate for the NAudit server or create a new one.

Enter Public key

Applies only when you want to use an existing certificate.

Lists the custom public key certificate that you want the NAudit service to use to authenticate audit messages.

Enter RSA Key

Applies only when you want to use an existing certificate.

Specifies the path to the custom private key file that you want the NAudit service to use to authenticate audit messages.

9 To install SSPR, continue to Chapter 10, “Installing the Password Management Component,” on page 105.

For more information about configuring forgotten password management, see “Configuring Forgotten Password Management” on page 156.

Silently Installing One SSO Provider

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

1 Log in as an administrator to the computer where you want to install the components.

2 Stop Tomcat.

3 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the OSP installation files, located by default in the `osp` directory.

4 (Conditional) If you downloaded the installation files from the NetIQ Downloads website, complete the following steps:

4a Navigate to the `.zip` file for the downloaded image.

4b Extract the contents of the file to a folder on the local computer.

5 Copy the `osp.configure.properties` file on to the location where you have write access and edit this file.

For more information about the settings for installation, see Step 7 and Step 8 on page 100.

6 To run the silent installation, issue the following command:

```
osp-install-win.exe -i silent -f path_to_silent.properties_file
```

In this command, specify the absolute path of the file. For example:

```
osp-install-win.exe -i silent -f
c:\NetIQ\idm\apps\osp\osp.silent.properties
```

7 Install SSPR. For more information, see Chapter 10, “Installing the Password Management Component,” on page 105.

Configuring Single Sign-on Access

You need to perform some actions to configure single sign-on access immediately after installing OSP. However, the final configuration process requires that first you install the identity applications. For more information, see Configuring Single Sign-on Access in Identity Manager in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

NOTE: While configuration the One SSO Provider in silent mode, ensure to specify the correct path for install, Java, Tomcat and SSL Keystore folders in the `osp.silent.properties` file. For example,

Install Folder: `USER_INSTALL_DIR=C:\NetIQ\idm\apps\osp`

Tomcat Folder: `NETIQ_TOMCAT_HOME=C:\NetIQ\idm\apps\tomcat`

Windows: `NETIQ_TOMCAT_HOME=C:\NetIQ\idm\apps\tomcat`

Java Folder: `NETIQ_JAVA_HOME=C:\NetIQ\idm\apps\jre`

SSL Keystore Folder:
`NETIQ_SSL_KEYSTORE_FILE=C:\NetIQ\idm\apps\jre\lib\security\cacerts`

10 Installing the Password Management Component

In this section, you will install Self Service Password Reset (SSPR) that helps you configure Identity Manager to allow users to reset their passwords.

SSPR integrates with the identity applications, identity reporting, and OSP to ensure that users who need to modify their passwords get directed to the appropriate web pages without performing any additional actions. After users complete their self-service activities, SSPR redirects users to the application that they original attempted to access.

NOTE: Identity Manager 4.6 and above version uses SSPR as a primary Password Management Tool.

Identity Manager does not require SSPR. You can use an alternative method for resetting user passwords.However, you might need to modify some configuration settings for Identity Manager. For more information, see "Configuring Forgotten Password Management" on page 156.

The installation files are located in the `\products\CommonApplication\sspr_install` directory. By default, the installation program installs the SSPR components in `C:\NetIQ\idm\apps\sspr`.

NetIQ recommends that you review the installation process before beginning.

Planning to Install Password Management for Identity Manager

This section provides information prerequisites, considerations, and system setup that are needed to install Self Service Password Reset (SSPR).

- "Checklist for Installing Password Management Components" on page 105
- "Prerequisites for Installing Self Service Password Reset" on page 106
- "System Requirements for Self Service Password Reset" on page 106
- "Using the Apache Log4j Service for Password Event" on page 106

Checklist for Installing Password Management Components

NetIQ recommends that you complete the steps in the following checklist:

	Checklist Items
❑	1. Review the planning information. For more information, see Part I, "Planning to Install Identity Manager," on page 17.

	Checklist Items
❑	2. Review the hardware and software requirements for the computers that will host the Identity Vault. For more information, see “Meeting System Requirements” on page 22.
❑	3. Ensure that Tomcat has been installed. For more information, see “Installing PostgreSQL and Tomcat” on page 92.
❑	4. (Conditional) To use the Apache Log4j service to record events in Tomcat, ensure that you have the appropriate files. For more information, see “Using the Apache Log4j Service to Log Sign-on” on page 98.
❑	5. Install SSPR: ◆ For a guided installation, see “Using the Wizard to Install Self Service Password Request” on page 107. ◆ For a silent installation, see “Silently Installing Self Service Password Reset” on page 110.
❑	6. Install and configure the identity applications to use single sign-on access and password management. For more information, see “Installing the Identity Applications” on page 127.

Prerequisites for Installing Self Service Password Reset

Your installation of NetIQ Self Service Password Reset (SSPR) should match the server requirements for the identity applications, with the following considerations:

- SSPR requires TSL/SSL protocol for communication.
- SSPR requires a supported version of the Tomcat application server. For more information, see “Prerequisites for Installing Tomcat” on page 91 and the most recent Release Notes for this version.
- NetIQ recommends that you review the prerequisites and requirements listed in the *NetIQ Self Service Password Reset Administration Guide*.

System Requirements for Self Service Password Reset

SSPR requires Apache Tomcat application server. The version of Tomcat must be the same as required for the identity applications.

All other server requirements match the server requirements for the identity applications. For more information, see “Prerequisites and Considerations for Installing the Identity Applications” on page 117 and the most recent Release Notes for this version.

Using the Apache Log4j Service for Password Event

You can use either the Apache Log4j or java.util.logging service to record events that occur in Tomcat. The Tomcat installer in the Identity Manager installation kit includes the files that you need for Log4j. However, if you install your own version of Tomcat, you need the following files to use the Apache logging service:

- `log4j-1.2.16.jar`

- tomcat-juli-adapters.jar
- tomcat-juli.jar

To add the files to your Tomcat installation, complete the following steps:

1. Download the "JULI" files for Tomcat v8.5.x from the Apache website:
   - tomcat-juli.jar
   - tomcat-juli-adapters.jar
2. Download the log4j-1.2.16.jar file from the Apache website.
3. Place the following files in the $TOMCAT_HOME\lib directory:
   - log4j-1.2.16.jar
   - tomcat-juli-adapters.jar
4. Place the tomcat-juli.jar file in the $TOMCAT_HOME/bin directory.
5. Specify a value for -Dlog4j.configuration in CATALINA_OPTS or create a log4j.properties file in the $TOMCAT_HOME\lib directory.

Installing Password Management for Identity Manager

This section describes the installation process for SSPR. You can install these programs on the same server where OSP component is installed or on the separate server.

- "Using the Wizard to Install Self Service Password Request" on page 107
- "Silently Installing Self Service Password Reset" on page 110
- "Post-Installation Tasks" on page 111

NOTE: If you use the legacy forgot password method, you do not need to install SSPR.

Using the Wizard to Install Self Service Password Request

The following procedure describes how to install SSPR on a Windows platform using an installation wizard. To perform a silent, unattended installation, see "Silently Installing Self Service Password Reset" on page 110. To prepare for the installation, review the prerequisites and system requirements listed in "Checklist for Installing Password Management Components" on page 105.

1. Log in as an administrator to the server where you want to install SSPR.
2. Stop the Tomcat server.
3. (Conditional) If you have the .iso image file for the Identity Manager installation package, navigate to the directory containing the SSPR installation files, located by default in the products\CommonApplication\sspr_install directory.
4. (Conditional) If you downloaded the SSPR installation files, complete the following steps:

   4a Navigate to the win.zip file for the downloaded image.

   4b Extract the contents of the file to a directory on the local computer.
5. From the directory that contains the installation files, run the sspr-install-win.exe file.
6. Read and accept the license agreement, and then click **Next**.

7 Specify a path for the installed files.

8 Complete the guided process, using the following parameters:

- **Tomcat details**

  Represents the home directory for the Tomcat server. For example, `C:\NetIQ\idm\apps\tomcat`. The installation process adds some files for SSPR to this folder.

- **Tomcat connection**

  Represents the settings of the URL that users need to connect to SSPR on the Tomcat server. For example, `https://myserver.mycompany.com:8080`.

  NOTE: You must also select **Connect to an external authentication server** and specify values for the external server if the following considerations are true:

  - You are installing SSPR.
  - OSP runs on a different instance of the supported application server than SSPR does.

  Protocol

  Specifies whether you want to use *http* or *https*. To use Secure Sockets Layer (SSL) for communications, specify `https`.

  Host Name

  Specifies the DNS name or IP address of the server where you are installing SSPR. Do not use `localhost`.

  Port

  Specifies the port that you want the server to use for communication with client computers.

  Connect to an external authentication server

  Specifies whether a different instance of Tomcat hosts the authentication server (OSP). The authentication server contains the list of users who can log in to SSPR.

  If you select this setting, also specify values for the authentication server's **Protocol**, **Host name**, and **Port**.

- **Tomcat Java home**

  Represents the home directory for Java on the Tomcat server. For example, `C:\NetIQ\idm\jre`. The installation process adds some files for OSP to the directory.

- **Authentication details**

  Represents the requirements for connecting to the authentication server which contains the list of users who can log in to the application.

  LDAP host

  Specifies the DNS name or IP address of the LDAP authentication server. Do not use `localhost`.

  LDAP port

  Specifies the port that you want the LDAP authentication server to use for communication with Identity Manager. For example, specify 389 for a non-secure port or 636 for SSL connections.

Use SSL

Specifies whether you want to use Secure Sockets Layer protocol for connections between the Identity Vault and the authentication server.

JRE Trust store (cacerts) file

Applies only when you want to use SSL for the LDAP connection.

Specifies the path to the certificate. For example, `C:\NetIQ\idm\apps\jre\lib\security\cacerts`.

JRE Trust store password

Applies only when you want to use SSL for the LDAP connection.

Specifies the password for the `cacerts` file.

Admin DN

Applies only when installing a new authentication server.

Specifies the DN for an administrator account of the LDAP authentication server. For example, `cn=admin,ou=sa,o=system`.

Admin password

Applies only when installing a new authentication server.

Specifies the password for the administrator account of the LDAP authentication server.

User container

Applies only when installing a new authentication server.

Specifies the container in the LDAP authentication server where you store the user accounts that can log in to Access Review. For example, `o=data`.

Admin container

Applies only when installing a new authentication server.

Specifies the container in the LDAP authentication server where you store the administrator accounts for Access Review. For example, `ou=sa,o=system`.

Keystore Password

Applies only when installing a new authentication server.

Specifies the password that you want to create for the new keystore for the LDAP authentication server.

The password must be a minimum of six characters.

- **SSPR details**

  Represents the settings required for configuring SSPR.

  Configuration password

  Specifies the password that you want to create for an administrator to use to configure SSPR.

  By default, SSPR does not have a configuration password. Without the password, any user who can log in to SSPR can also modify the configuration settings.

SSPR redirect URL

Specifies the absolute URL to which the client will redirect when actions such as password changes or challenge questions have been completed in SSPR. For example, forward to the Dashboard.

Use the following format: `protocol://server:port/path`. For example, `http://`*`idm_userapp_server_ip`*`:`*`port_no`*`/idmdash/#/landing`.

- **Authentication server details**

  Represents the password that you want to create for the SSPR service to use when connecting to the OSP client on the server. Also referred to as the client secret.

  To modify this password after installation, use the RBPM Configuration utility.

- **Auditing details (SSPR)**

  Represents the settings for auditing SSPR events that occur in the authentication server.

  (Conditional) *Enable auditing for SSPR*

  Specifies whether you want to send SSPR events to an auditing server.

  If you select this setting, also specify the settings for the syslog server.

  Syslog host name

  Applies only when you enable auditing for SSPR.

  Specifies the DNS or IP address of the server that hosts the syslog server. Do not use `localhost`.

  Syslog port

  Applies only when you enable auditing for SSPR.

  Specifies the port of the server that hosts the syslog server.

9 To configure the identity applications and Identity Reporting to use SSPR, continue to Chapter 11, “Installing Identity Applications,” on page 115.

10 In Configuration Update Utility, update the SSO clients Parameters. For more information see, “Self Service Password Reset” on page 181.

For more information about configuring forgotten password management, see “Configuring Forgotten Password Management” on page 156.

Silently Installing Self Service Password Reset

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

1 Log in as an administrator to the computer where you want to install the components.

2 Stop Tomcat.

3 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the SSPR installation files, located by default in the `sspr` directory.

4 (Conditional) If you downloaded the installation files from the NetIQ Downloads website, complete the following steps:

4a Navigate to the `.zip` file for the downloaded image.

4b Extract the contents of the file to a folder on the local computer.

5. Edit the `sspr-silent.properties` file for the SSPR installation, located by default in the same directory as the installation scripts.

   For more information about the settings for installation, see Step 7 on page 108 and Step 8 on page 108.

6. To run the silent installation, issue the following command:

   ```
   sspr-install-win.exe -i silent -f path_to_silent.properties_file
   ```

7. In Configuration Update Utility, update the SSO clients Parameters. For more information see, "Self Service Password Reset" on page 181.

Post-Installation Tasks

Post-installation tasks generally include the following tasks:

- "Ensuring Error-Free Installation" on page 111
- "Assigning the Universal Password Policy to a User Container" on page 112
- "Granting Rights to pwmResponseSet Attributes" on page 113

Ensuring Error-Free Installation

After you install SSPR, you can modify the configuration settings, such as change administrator permission of the LDAP group DN for the default profile or change the forward URL. Also, NetIQ recommends that you verify the URLs that the installation process created and change them if needed.

1. To open the SSPR login page, enter the following URL on your browser:

   `protocol://server:port/web-context`

   For example,

   `http://192.168.0.1:8080/sspr/`

2. On the top-right corner of the SSPR login page, select **Configuration Editor** from the list.

3. Specify the configuration password and click **Sign In**.

4. From the tree view, select **Default Settings** and ensure that **NetIQ IDM/OAuth Integration** is selected in the **LDAP Vendor Default Settings** list.

5. From the tree view, click **LDAP > LDAP Directories > default > Connection > LDAP Certificates**, then click **Import From Server** to import the certificates.

   (Conditional) Click **Test LDAP Profile** on the same page to ensure that all configured LDAP servers are reachable.

6. From the tree view, click **Modules > Authenticated > Administration** and ensure that the administrator permissions are assigned to the LDAP group DN for the default profile.

   If you are performing a fresh installation of SSPR, the list will be empty. You need to create a new group in iManager and add the `admin` user to the group.

7. From the tree view, click **Settings > Application > Application**, and ensure that the **Forward URL** is set to `http://<Server:Port>/idmdash/#/landing`.

   For example, `http:/192.168.0.1:8080/idmdash/#/landing`.

8 From the tree view, click **Settings > UserInterface > Look & Feel** and change **Interface Theme** to **Micro Focus (mdefault)** if not already specified.

9 From the tree view, click **Settings > Single Sign On (SSO) Client > OAuth** and verify the values are correctly specified for the following parameters:

OAuth Login URL

> Specifies the URL for OAuth server login. When user logs in, this URL to redirects the users for authentication with OSP.
>
> For example, `http://192.168.0.1:8080/osp/a/idm/auth/oauth2/grant`

OAuth Code Resolve Service URL

> Specifies the URL for OAuth Code Resolve Service. SSPR uses this web service URL to resolve the artifact that the OAuth identity server returns.
>
> For example, `http://192.168.0.1:8080/osp/a/idm/auth/oauth2/authcoderesolve`

OAuth Profile Service URL

> Specifies the URL for the web service that the Identity Manager provides to return attribute data from the user.
>
> For example, `http://192.168.0.1:8080/osp/a/idm/auth/oauth2/getattributes`

OAUTH Web Service Server Certificate

> (Conditional) If HTTPS is enabled, import the certificate for the OAuth web service server.

OAuth Client ID

> Specifies the client ID of the OAuth client. For example, `sspr`.

OAuth Shared Secret

> Specifies a password for the OAuth shared secret. This password is shared between OSP and SSPR applications.

OAuth User Name/DN Login Attribute

> Specifies the attribute of the user that SSPR uses to request OAuth server to authenticate user locally. For example, `name`.

10 Click 💾 from the top-right corner of the page to save your configuration.

11 On the top right corner of the SSPR login page, select **Configuration Manager** from the list.

12 Click **Restrict Configuration**.

Assigning the Universal Password Policy to a User Container

To assign the Universal Password policy to a user container:

1 Log in to iManager.

2 Select **Roles and Tasks > Password Policies**, then choose the password policy.

3 To select a user with administrative rights:

   3a Click **Universal Password > Configuration Options > Universal Password Retrieval**.

   3b Select **Allow admin to retrieve passwords** or **Allow the following to retrieve passwords** and click **OK**.

   For example, `cn=uaadmin,ou=sa,o=data`

4 Click **Policy Assignment** and assign `container` to the container where the user resides.

   For example, `o=data` or administrative users.

Granting Rights to pwmResponseSet Attributes

Users with authenticated rights perform operations based on the permissions associated with the user’s connection. Authenticated users need the following rights for their own user entry:

- Browse rights to [Entry Rights]
- Read, Compare, and Write rights to pwmResponseSet

To grant rights to pwmResponseSet attribute, perform the following steps:

1 Log in to iManager.

2 Click .

3 Click **iManager Server** > **Configure iManager**.

4 Click **Misc** > **Enable [this]**.

5 Click 🔍.

6 From the **Tree** view, select the top level container of all users in the directory.

7 Click the **current level** check box and then click **Actions** > **Modify Trustees**.

8 Click **[This]** from the list and then click **Add Trustee**.

9 Click **Apply**.

10 Click **Assigned Rights** for **[This]** trustee.

11 Click **Add Property** and then select the **Show all properties in schema** check box.

12 Select **pwmResponseSet** from the list.

   Ensure that Write, Compare, Read, and Inherited options are selected.

13 Click **Done**.

11 Installing Identity Applications

This section guides you through the process of installing the components and framework required for the identity applications:

- Identity Applications Administration
- Identity Applications Dashboard
- Role and Resource Service driver
- User Application
- User Application driver

By default, the installation program installs these components in `C:\NetIQ\idm\apps`.

The identity applications require access to other Identity Manager components during and after installation. NetIQ recommends that you review the installation process before beginning. For more information, see "Planning to Install the Identity Applications" on page 115.

Planning to Install the Identity Applications

The identity applications installation includes the following components:

- Identity Manager Dashboard
- Identity Manager Administration Console
- User Application
- Role and Resource Service driver (RRSD)
- User Application driver (UAD)

The installation does not include the two drivers required for the identity applications: User Application driver and Roles and Resource Services driver.

NOTE: Technically Identity Reporting could be considered an identity application because the component also uses SSPR and OSP, and you modify the settings with the RBPM configuration utility. However, Identity Reporting has its own installation program, can be installed on a separate server, and uses a different database.

- "Checklist for Installing the Identity Applications" on page 116
- "Understanding the Installation Program for the Identity Applications" on page 117
- "Prerequisites and Considerations for Installing the Identity Applications" on page 117

Checklist for Installing the Identity Applications

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

	Checklist Items
□	1. Review the planning information. For more information, see Part I, "Planning to Install Identity Manager," on page 17.
□	2. Review the hardware requirements, software requirements, and considerations for installing the identity applications and their supporting framework. For more information, see the following sections: ◆ Meeting System Requirements. ◆ Prerequisites and Considerations for Installing the Identity Applications
□	3. Decide whether you should install an Sentinel before installing the identity applications. For more information, see "Recommended Installation Scenarios and Server Setup" on page 21.
□	4. Ensure that the Identity Manager engine has been installed. For more information about installing the engine, see Chapter 4, "Planning to Install the Engine, Drivers, and Plug-ins," on page 55.
□	5. Create a User Application Administrator account in the Identity Vault. For more information, see "Assigning Rights to Identity Vault Administrator and User Application Administrator Account" on page 121.
□	6. Install and configure a database for the identity applications on the local computer or a connected server. ◆ To learn about the database, see "Prerequisites for Installing the Database for the Identity Applications" on page 120. ◆ To install the database, see "Configuring the Database for the Identity Applications" on page 123.
□	7. Prepare an application server on the local computer or in a cluster. ◆ To understand the requirements, see "Prerequisites and Considerations for the Application Server" on page 119. ◆ To prepare the cluster, see "Preparing Your Environment for the Identity Applications" on page 125. ◆ To install an application server, see "Preparing Your Environment for the Identity Applications" on page 125.
□	8. (Conditional) To use the Apache Log4j service to record events in Tomcat, ensure that you have the appropriate files. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 98.
□	9. Review the contents of the identity applications installation kit to determine which files are needed for your environment. For more information, see "Understanding the Installation Program for the Identity Applications" on page 117.
□	10. Install the identity applications. For more information, see "Installing the Identity Applications" on page 127.

	Checklist Items
❑	11. Create and deploy the User Application driver and the Roles and Resource Service driver. For more information, see "Creating and Deploying the Drivers for the Identity Applications" on page 147.
❑	12. To perform the final tasks in the installation process, see "Completing the Installation of the Identity Applications" on page 150.
❑	13. Ensure that you have configured the identity applications and single sign-on settings correctly. For more information, see Verifying Single Sign-on Access for the Identity Applications in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.
❑	14. (Optional) To begin using the identity applications, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Understanding the Installation Program for the Identity Applications

The installation files for the identity applications are located in the `\products\UserApplication\` directory of the installation package.

The installation program (`IdmUserApp.exe`) does the following:

- Designates an existing version of an application server to use.
- Designates an existing version of a database to use. The database stores identity application data and configuration information.
- Configures the JDK's certificates file so that the identity application (running on Tomcat) can communicate securely with the Identity Vault and the User Application driver.
- Configures and deploys the Java web application archive (WAR) file for the User Application to Tomcat.
- Enables logging through Sentinel auditing clients if you choose to do so.
- Enables you to import an existing master key to restore a specific installation of the identity applications and to support clusters.

Prerequisites and Considerations for Installing the Identity Applications

NetIQ recommends that you review the prerequisites and computer requirements for the identity applications before you begin the installation process. For more information about configuring the User Application environment, see *NetIQ Identity Manager - User's Guide to the Identity Applications*.

- "Installation Considerations for the Identity Applications" on page 118
- "Prerequisites and Considerations for the Application Server" on page 119
- "Prerequisites for Installing the Database for the Identity Applications" on page 120

Installation Considerations for the Identity Applications

The following considerations apply to the installation of the identity applications.

- Require a supported version of the following Identity Manager components:
  - Designer
  - Identity Vault
  - Identity Manager engine
  - Remote Loader
  - One SSO Provider

  For more information about required versions and patches for these components, see the latest Release Notes.
- Ensure that the Identity Vault includes the created and deployed User Application and Roles and Resources service drivers. For more information, see "Creating and Deploying the Drivers for the Identity Applications" on page 147.
- Install the following framework items before installing the identity applications:
  - An application server on the local computer. For more information, see "Prerequisites and Considerations for the Application Server" on page 119.
  - A database on the local computer or a connected server. For more information, see "Prerequisites for Installing the Database for the Identity Applications" on page 120.
- (Optional) NetIQ recommends that you enable Secure Sockets Layer (SSL) protocol for communication among the Identity Manager components. To use SSL protocol, you must enable SSL in your environment and specify **https** during the installation. For information about enabling SSL, see Configuring Security in the Identity Applications in the *NetIQ Analyzer for Identity Manager Administration Guide*.
- Create the User Application driver before creating the Role and Resource driver. The Role and Resource driver references the role vault container (`RoleConfig.AppConfig`) in the User Application driver.
- You cannot use the Role and Resource Service Driver with the Remote Loader because the driver uses jClient.
- Set the `JAVA_HOME` environment variable to point to the JDK that you plan to use with the identity applications. To override `JAVA_HOME`, manually specify the path during the installation.
- The installation process places the program files in the `C:\NetIQ\idm` directory by default.

  If you plan to install the User Application in a non-default location, the new directory must exist and is writable.
- Each User Application instance can service only one user container. For example, you can add users to, search, and query only the container associated with the instance. Also, a user container association with an application is meant to be permanent.
- (Conditional) If you plan to use external password management, your environment must meet the following requirements:
  - Enable Secure Sockets Layer (SSL) protocol for Tomcat on which you deploy the identity applications and the `IDMPwdMgt.war` file.
  - Ensure that the SSL port is open on your firewall.

For more information about enabling SSL for Tomcat, see Updating the SSL Settings for Self Service Password Reset in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*..

For more information about the `IDMPwdMgt.war` file, see "Configuring Forgotten Password Management" on page 156.

- (Optional) To retrieve authorizations from managed systems, install one or more of the Identity Manager drivers.
  - You must use drivers supported by Identity Manager 3.6.1, 4.0, or later. For more information about installing the drivers, see the appropriate driver guides in the NetIQ Identity Manager Drivers documentation website.
  - To manage the drivers, you must have previously installed Designer or the appropriate plug-ins for iManager. For more information, see "Understanding Installation for iManager Plug-ins" on page 74.

Prerequisites and Considerations for the Application Server

The identity applications require that Tomcat be installed with the following considerations:

- Tomcat must be running with the Java Development Kit (JDK) or Java Runtime Environment (JRE). For more information about supported versions, see the NetIQ Identity Manager Technical Information website.
- Set the `JAVA_HOME` environment variable to point to the JDK that you plan to use with the User Application. To override `JAVA_HOME`, manually specify the path during the installation.
- (Conditional) You can use your own Tomcat installation program instead of the one provided in the Identity Manager installation kit. However, to use the Apache Log4j service with your version of Tomcat, ensure that you have the appropriate files installed. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 98.
- (Conditional) To preserve documents that you digitally sign, you must install the identity applications on a Tomcat application server and use Novell Identity Audit. Digital signature documents are not stored with workflow data in the User Application database, but are stored in the logging database. You must also enable logging to preserve these documents. For more information, see Setting Up Logging in the Identity Applications in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.
- (Conditional) In environments where you log a large amount of user data or your directory-server contains a large number of objects, you might want more than one application server with a deployment of the identity applications. For more information about configuring for optimal performance, see Tuning the Performance of the Applications in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.
- (Conditional) If you use a Tomcat application server, do not start the server until after you complete the installation process.
- (Conditional) To use external password management, you must do the following to enable the Secure Sockets Layer (SSL) protocol:
  - Enable SSL for Tomcat on which you deploy the identity applications and the `IDMPwdMgt.war` file.
  - Ensure that the SSL port is open on your firewall.

For more information about the `IDMPwdMgt.war file`, see Configuring Forgotten Password Management and the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

- The installation process does not modify the `JAVA_HOME` or `JRE_HOME` entries on a Tomcat server. By default, the convenience installer for Tomcat places the `setenv.bat` file in the `C:\NetIQ\idm\apps\tomcat\bin\` directory. The installation also configures the JRE location in the file.

Prerequisites for Installing the Database for the Identity Applications

The database stores the identity applications data and configuration information.

Before installing the database instance, review the following prerequisites:

- To configure a database for use with Tomcat, you must create a JDBC driver. The identity applications use standard JDBC calls to access and update the database. The identity applications use a JDBC data source file bound to the JNDI tree to open a connection to the database.
- You must have an existing data source file that points to the database. The installation program for the User Application creates a data source entry for Tomcat in `server.xml` and `context.xml` which points to the database.
- Ensure that you have the following information:
  - Host and port of the database server.
  - Name of the database to create. The default database for the identity applications is `idmuserappdb`.
  - Database username and password. The database username must represent an Administrator account or must have enough permissions to create tables in the Database Server. The default administrator for the User Application is `idmadmin`.
  - The driver `.jar` file provided by the database vendor for the database that you are using. NetIQ does not support driver JAR files provided by third-party vendors.
- The database instance can be on the local computer or a connected server.
- The database character set must use Unicode encoding. For example, UTF-8 is an example of a character set that uses Unicode encoding, but Latin1 does not use Unicode encoding. For more information about specifying the character set, see "Configuring the Character Set" on page 125 or "Configuring an Oracle Database" on page 123.
- The case-sensitive collation might cause a duplicate key error during migration. Check the collation and correct it, then re-install the identity applications.
- (Conditional) By default, the identity applications installation program accepts only Oracle System ID when using Oracle for the database. To access the database by using a service name instead of Oracle System ID, you must perform certain post-installation actions as described in "Accessing the Oracle Database Using Oracle Service Name" on page 150.
- (Conditional) To use the same database instance both for auditing purposes and for the identity applications, NetIQ recommends installing the database on a separate dedicated server from the server that hosts Tomcat running the identity applications.

- (Conditional) If you are migrating to a new version of the identity applications, you must use the same database that you used for the previous installation.
- The only supported collation for MS SQL is SQL_Latin1_General_CP1_CI_AS.

NetIQ supports clustering database servers with certain considerations. For more information, see "Prerequisites for Installing the Database for the Identity Applications" on page 120.

Assigning Rights to Identity Vault Administrator and User Application Administrator Account

The Identity Vault Administrator is a user who has rights to configure the Identity Vault. This is a logical role that can be shared with other administrative user types.

The Identity Vault Administrator needs the following rights:

- Supervisor rights to the User Application driver and all the objects it contains. You can accomplish this by setting the rights at the driver container level and making them inheritable.
- Supervisor Entry rights to any of the users that are defined through the directory abstraction layer user entity definition. This should include Write attribute rights to objectClass and any of the attributes associated with the `DirXML-EntitlementRecipient`, `srvprvEntityAux` and `srvprvUserAux` auxiliary classes.
- Supervisor rights to the container object `cn=DefaultNotificationCollection`, `cn=Security`. This object persists email server settings used for automated provisioning emails. It can contain SecretStore credentials for authenticating to the email server itself.
- Supervisor rights to the container object `cn=Authorized Login Methods`, `cn=Security`. During the User Application installation the SAML Assertion object is created in this container.
- Ensure that you have supervisor rights to the `cn=Security` container before you install user application. During the User Application installation, the container `cn=RBPMTrustedRootContainer` is created under the `cn=Security` container.

  Alternatively, manually create the `cn=RBPMTrustedRootContainer`,`cn=Security` container (create an object called `Trusted Root Container` with object class `NDSPKI:Trusted Root` inside the `Security` container), and then assign supervisor rights to the container.

You must manually create a User Application Administrator account in the Identity Vault for the Roles Based Provisioning Module to install correctly. The User Application Administrator account must be a trustee of the top container and must have Supervisor rights to the container.

When you create the User Application Administrator account, you must assign a password policy to this new user account. For more information, see "Creating Password Policies" in the *Password Management Administration Guide*.

To create the permissions for the User Application Administrator account, you must create an LDAP Data Interchange Format (LDIF) file specific to your environment. Use the following example LDIF for reference.

```
 dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 1#subtree#[Root]#[Entry Rights]
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#description
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#directReports
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#mail
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#manager
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#photo
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvQueryList
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvUserPrefs
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#telephoneNumber
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#title

dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 17#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[Entry Rights]
ACL: 35#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[All Attributes Rights]
```

NOTE: Copying the content as is might insert some hidden special characters in the file. If you receive a `ldif_record() = 17` error message when you add these attributes to the Identity Vault, insert an extra space between the two DNs.

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 Technical Information website. For more information about considerations for the User Application database, see "Prerequisites for Installing the Database for the Identity Applications" on page 120.

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 123
- "Configuring a PostgreSQL Database" on page 124
- "Configuring a SQL Server Database" on page 124

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 PostgreSQL Database

For your convenience, NetIQ provides an installation program for PostgreSQL, which fully supports the framework services and applications within Identity Manager. The installation program guides you through the configuration process. For more information, see "Installing PostgreSQL and Tomcat" on page 92.

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.

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.

Preparing Your Environment for the Identity Applications

The Identity Applications benefit from higher availability when you run them in a cluster. In addition, they support HTTP session replication and session failover. This means that 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.

This section provides instructions for preparing your environment, including a cluster environment, to function with the identity applications. You must complete the steps in this chapter in conjunction with the instructions in "Using the Guided Process to Install the Identity Applications" on page 128.

- "Specifying a Location for the Permission Index" on page 125
- "Preparing Your Application Server for the Identity Applications" on page 126

Specifying a Location for the Permission Index

When you start the Tomcat server, the process creates a permission index for Identity Applications. If you do not specify a location for the index, the installation creates a folder in a temporary directory. For example: `C:\NetIQ\idm\apps\tomcat\temp\permindex` on Tomcat.

In a test environment, the location usually does not matter. However, in a production or staging environment, you might not want to place the permission index in a temporary directory.

To specify a location for the index:

1. Stop Tomcat.
2. In a text editor, open the `ism-configuration.properties` file.
3. At the end of the file, add the following text:

```
com.netiq.idm.cis.indexdir = path\permindex
```

For example:

```
com.netiq.idm.cis.indexdir = C:\NetIQ\idm\apps\tomcat\temp\permindex
```

4. Save and close the file.
5. Delete the existing `permindex` folder in the temporary directory.
6. Start Tomcat.

To enable permission index for clustering, see “Enabling the Permission Index for Clustering” on page 344.

Preparing Your Application Server for the Identity Applications

You should prepare Tomcat that will run the identity applications. For your convenience, NetIQ provides Apache Tomcat in the installation kit. For more information about using the applications in a cluster environment, also see “Preparing a Cluster for the Identity Applications” on page 331.

The `.iso` for installing Identity Manager includes a program for installing Tomcat (and optionally PostgreSQL). For more information, see “Installing PostgreSQL and Tomcat” on page 92.

You can use your own Tomcat installation program instead of using the convenience installer provided in the installation package. However, if you do use a different installation program, there are additional steps you must perform for Tomcat to function correctly with the Identity Applications.

Before you start the installation process, ensure that the versions of the components you are installing are supported with this version of the Identity Applications. For more information, see “Prerequisites and Considerations for Installing the Identity Applications” on page 117.

1. Install Apache Tomcat as a service on your server.

   For more information, see Tomcat Setup.
2. Install the following components on the same server where you installed Tomcat.
   - **Java Runtime Environment (JRE):** For more information, see the Java Platform Installation Guide.
   - **Apache ActiveMQ:** For more information, see ActiveMQ.
   - **PostgreSQL:** For more information, see PostgreSQL Manuals.
3. Copy the `activemq-all-5.15.2 jar` file to the *`C:\NetIQ\idm\apps\activemq`* folder.
4. Copy the following files to the *`C:\NetIQ\idm\apps\tomcat\bin`* folder for logging.
   - `log4j.jar`
   - `log4j.properties`
   - `tomcat-juli-adapters.jar`
5. Set the following properties in the `setenv.bat` file.

```
JAVA_HOME
JRE_HOME
PATH (set Java path)
JAVA_OPTS="-Xms1024m -Xmx1024m"
```

6 Copy the `postgresql-9.4.1212jdbc42.jar` file to the `C:\NetIQ\idm\apps\tomcat\bin` folder.

7 (Conditional) In a cluster environment, open the `server.xml` file located by default in the `\TOMCAT_INSTALLED_HOME\conf\` directory in the first node of the cluster and uncomment this line:

```
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
```

Do this for all nodes in the cluster.

For advanced Tomcat clustering configuration, follow the steps from Apache Tomcat Documentation.

Installing the Identity Applications

This chapter provides instructions for installing and configuring an application server for the User Application and RBPM. You must have the correct version of the Java environment for your application server.

For more information about the requirements for Tomcat and Java, see the NetIQ Identity Manager Technical Information website.

- "Checklist for Installing the Identity Applications" on page 127
- "Using the Guided Process to Install the Identity Applications" on page 128
- "Silently Installing the Identity Applications" on page 134
- "Post-Installation Steps" on page 140
- "Disabling the Prevent HTML Framing Setting for Integrating Identity Manager with SSPR" on page 144
- "Verifying the User Properties" on page 144
- "Configuration and Usage Considerations for the Identity Applications" on page 145
- "Starting the Identity Applications" on page 146

Checklist for Installing the Identity Applications

Use the following checklist to guide you through the process of installing the identity applications.

	Checklist Items
□	1. Install a supported version of your application server and Java development kit or runtime environment. For more information, see the NetIQ Identity Manager Technical Information website.
□	2. Ensure that Tomcat has the correct settings. For more information, see "Preparing Your Environment for the Identity Applications" on page 125.
□	3. Configure a data source file and JDBC provider for the database.
□	4. Install the identity applications. For more information, see "Using the Guided Process to Install the Identity Applications" on page 128.

	Checklist Items
☐	5. Configure Tomcat for the identity applications. For more information, see "Post-Installation Steps" on page 140.
☐	6. Deploy and start the identity applications. For more information, see "Starting the Identity Applications" on page 146.

Using the Guided Process to Install the Identity Applications

The following procedure describes how to install the identity applications using an installation wizard.

To prepare for the installation, review the activities listed in "Checklist for Installing the Identity Applications" on page 127. Also see the Release Notes accompanying the release.

NOTE

- The installation program does not save the values that you enter as you progress through the windows in the wizard. If you click **Previous** to return to an earlier window, you must re-enter the configuration values.
- The installation program creates the *novlua* user account and sets the permissions in Tomcat to this user. For example, the `services.msc` script uses this user account to run Tomcat.

To install with the guided process:

1. Log in as an administrative user to the computer where you want to install the identity applications.
2. Stop Tomcat.
3. (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the installation files, located by default in the `products\UserApplication\` directory.
4. (Conditional) If you downloaded the installation files, complete the following steps:

   4a Navigate to the `win.zip` file for the downloaded image.

   4b Extract the contents of the file to a directory on the local computer.
5. From the directory that contains the installation files, run the `IdmUserApp.exe` file.
6. Complete the guided process, using the following parameters:
   - **Application Server Platform**

     Represents Tomcat for running the Identity Applications. Tomcat must already be installed.
   - **Installation Folder**

     Represents the path to a directory where the installation program creates the application files.
   - **Database Platform**

     Represents the platform of the User Application database. The database software must already be installed. However, you do not need to create the database schema during installation.

For your convenience, NetIQ provides PostgreSQL.

- **Database Host and Port**

  Represents the settings for the server that hosts the User Application database.

  NOTE: In a cluster environment, you must specify the same database settings for each member in the cluster.

  Host

  Specifies the name or IP address of the server.

  Port

  Specifies the port that you want the server to use for communication with the User Application.

- **Database Username and Password**

  Represents the settings for running the User Application database.

  NOTE

  - If you installed PostgreSQL as part of the installation for this version of Identity Manager, the installation process already created the database and database administrator. By default, the installed database is `idmuserappdb` and the database user is `idmadmin`. Specify the same values that you used for the PostgreSQL installation.
  - In a cluster environment, you must specify the same database name, username, and password for each member in the cluster.

  Database Name or SID

  Specifies the name of the database according to the database platform. By default, the database name is `idmuserappdb`.

  - For a PostgreSQL or SQL Server database, specify the name.
  - For an Oracle database, specify the Security Identifier (SID) that you created with the database instance.

  Database Username

  Specifies the name of an account that allows the User Application to access and modify data in the databases.

  Database Password

  Specifies the password for the specified username.

  Database Driver JAR File

  Specifies 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.

- **Database Administrator**

  Optional

Represents the name and password for the database administrator.

This field automatically lists the same user account and password that you specified for Database Username and Password. To use that account, do not make any changes.

Database administrator

(Optional) Specifies the account for a database administrator that can create database tables, views, and other artifacts.

Password

(Optional) Specifies the password for the database administrator.

- **Create Database Tables**

  Indicates whether you want to configure your new or existing database as part of the installation process, or afterward.

  Create Tables Now

  The installation program creates the database tables as part of the installation process.

  Create Tables at Application Startup

  The installation program leaves instructions to create the tables when the User Application starts for the first time.

  Write SQL to File

  Generates a SQL script that the database administrator can run to create the databases. If you choose this option, you must also specify a name for **Schema File**. The setting is in the **SQL Output File** configuration.

  You might select this option if you do not have permissions to create or modify a database in your environment. For more information about generating the tables with the file, see "Manually Creating the Database Schema" on page 151.

- **New Database or Existing Database**

  Specifies whether you want to use existing, empty databases or create new tables in the existing database. Use the following considerations:

  - New Database

    If the database used is new, click **New Database.** Ensure that a database exists before selecting this option.

  - Existing Database

    If database is existing and it has User Application tables from a previous installation, select **Existing Database.**

    If the existing database runs on an Oracle platform, you must prepare Oracle before updating the schema.

  After selecting the database type, you need to specify, as to when the database tables should be created. The Create Database Tables screen gives you the option to create tables at installation time or at application startup. Alternatively, you can create a schema file at installation time, which the Database Administrator would use to create the tables later.

  If you want to generate a schema file, select the Write SQL to File button and provide a name for the file in the Schema Output File field.

- **Test Database Connection**

Specifies whether you want the installer to connect to the database for creating tables directly or for creating the `.sql` file.

The installation program attempt the connection when you click **Next** or press **Enter**.

NOTE: You can continue with installation if the database connection fails. However, after installation, you must manually create the tables and connect to the database. For more information, see "Manually Creating the SQL File to Generate the Database Schema" on page 151.

- **Java Install**

  Represents the path to the JRE file used to launch the installation program. For example, `C:\NetIQ\idm\jre`.

- ***Application_Server* Configuration**

  Represents the path to the installation files for Tomcat. For example, `C:\NetIQ\idm\jre`. The installation process adds some files to this folder.

- **IDM Configuration**

  Represents the settings for the identity application context used in URLs and for the workflow engine.

  Application Context

  > Specifies a name that represents the Tomcat configuration, the application WAR file, and the name in the URL context.
  >
  > The installation script creates a server configuration, then names the configuration according to the name that you created when installing Tomcat. For example, `IDMProv`.
  >
  > **IMPORTANT:** NetIQ recommends that you make a note of the specified **Application Context**. You will use this application name in the URL when you start the identity applications from a browser.

- **Select Audit Logging Type**

  Indicates whether you want to enable CEF or Sentinel Log Management for IGA. Specify **Yes** or **No**.

- **Audit Logging**

  Applies only when you specify Yes for Select Audit Logging Type.

  Indicates the type of logging that you want to enable.

  For more information about setting up logging, see the *User Application Administration Guide.*

  Sentinel Log Management for IGA

  > Enables logging through a Novell or NetIQ client for the User Application.
  >
  > ---
  >
  > **NOTE:** If you choose this option, you must also specify the hostname or IP address for the client server and the path to the log cache.
  >
  > ---

  CEF

  > Enables the User Application to log events through CEF.

NOTE: If you choose this option, you must also specify the hostname or IP address for the syslog server and the syslog port.

- **Security - Master Key**

  Indicates whether you want to import an existing master key. The User Application uses the master key to access encrypted data. Specify **Yes** or **No**.

  You might want to import the master key in the following situations:

  - After installing the first instance of the identity applications in a cluster. Every instance of the User Application in a cluster must use the same master key. For more information, see "Using the Same Master Key for Each User Application in the Cluster" on page 332.
  - If you are moving your installation from a staging system to a production system and want to keep access to the database you used with the staging system.
  - If you are restoring your User Application and you want to access the encrypted data stored by your previous version of the User Application.

  Yes

  Specifies that you want to import an existing master key.

  No

  Specifies that you want the installation program to create the key.

  By default, the installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory.

- **Import Master Key**

  Applies only when you specify Yes for Security - Master Key.

  Specifies the master key that you want to use. You can copy the master key from the `master-key.txt` file.

- **Application server connection**

  Represents the settings of the URL that users need to connect to the identity applications on Tomcat. For example, `https:myserver.mycompany.com:8080`.

  NOTE: If OSP runs on a different instance of the Tomcat application server, you must also select **Connect to an external authentication server** and specify values for the OSP server.

  Protocol

  Specifies whether you want to use *http* or *https*. To use Secure Sockets Layer (SSL) for communications, specify `https`.

  Host Name

  Specifies the DNS name or IP address of the server hosting OSP. Do not use `localhost`.

  Port

  Specifies the port that you want the server to use for communication with client computers.

Connect to an external authentication server

Specifies whether a different instance of Tomcat hosts the authentication server (OSP). The authentication server contains the list of users who can log in to SSPR.

If you select this setting, also specify values for the authentication server's **Protocol**, **Host name**, and **Port**.

- **Authentication server details**

  Specifies the password that you want the identity applications to use when connecting to the authentication server. Also referred to as the client secret. The installation process creates this password.

7 Configure the settings for the identity applications in the Config Update window.

7a Browse for the **Identity Vault DNs**.

7b Click **OK**.

NOTE

- Ensure that the User Application and the Roles and Resources Service drivers are already created and deployed to the Identity Vault. For more information, see "Installation Considerations for the Identity Applications" on page 118.
- If you click **Cancel**, the installer takes you back to the Application Server Connection window.
- After installing the User Application, you can modify most of the settings in the `configureupdate.bat` files. For more information about specifying the values for the settings, see "Configuring the Settings for the Identity Applications" on page 161.

---

8 (Conditional) In a GUI installation, to immediately configure the identity applications, complete the following steps in the Configure IDM window:

8a Click **Yes** and then click **Next**.

8b In Roles Based Provisioning Module Configuration, click **Show Advanced Options.**

8c Modify the settings as needed.

NOTE

- For more information about specifying the values, see "Configuring the Settings for the Identity Applications" on page 161.
- In production environments, all administrator assignments are restricted by licensing. NetIQ collects monitoring data in the audit database to ensure that production environments comply. Also, NetIQ recommends that only one user be given the permissions of the Security Administrator.

8d Click **OK**.

9 Click **Next**.

10 In the Pre-Installation Summary window, click **Install**.

11 (Optional) Review the installation log files. For results of the basic installation, see the `user_application_install_log.log` file in the `C:\NetIQ\idm\apps\UserApplication\logs\` directory.

For information about the identity applications configuration, see the `NetIQ-Custom-Install.log` file in the `C:\NetIQ\idm\apps\UserApplication` directory.

12 (Optional) If you are using an external password management WAR, manually copy the WAR to the installation directory and to the remote application server deploy directory that runs the external password WAR functionality.

13 Continue with the post-installation tasks described in "Completing the Installation of the Identity Applications" on page 150.

Silently Installing the Identity Applications

This section describes how to perform a silent install of the identity applications. A silent installation requires no interaction during the installation and can save you time, especially when you install on more than one server.

To prepare for the installation, review the activities listed in "Checklist for Installing the Identity Applications" on page 127. Also see the Release Notes accompanying the release.

This process includes the following activities:

- "Setting Passwords in the Environment for a Silent Installation" on page 134
- "Editing the .properties File" on page 134
- "Executing a Silent Installation of the Identity Applications" on page 140

Setting Passwords in the Environment for a Silent Installation

You can create environment variables for the passwords that the silent installation process can read during the installation. This allows the silent installer to read the passwords from the environment, rather than from the `user_app-silent.properties` file. This can provide some additional security.

The following password parameters are required for the silent installation:

- NOVL_DB_USER_PASSWORD
- NOVL_CONFIG_DBADMIN_PASSWORD
- NOVL_CONFIG_LDAPADMINPASS
- NOVL_CONFIG_KEYSTOREPASSWORD

For example:

```
SET NOVL_DB_USER_PASSWORD=myPassWord
```

Editing the .properties File

You must edit the parameter values in the `user_app-silent.properties` file before performing the silent installation or configuration. The table in this section provides a list of the parameters. The parameters correspond to the basic installation parameters as well as for configuring RBPM and the identity applications. For more information about specifying the parameter values, see "Using the Guided Process to Install the Identity Applications" on page 128 and "Configuring the Settings for the Identity Applications" on page 161.

1 Log in as administrative user to the computer where you want to install the identity applications.

2 Ensure that the `user_app-silent.properties` file is stored on the local computer.

   By default, you can find the file in the `\products\UserApplication` directory within the `.iso` image file for the Identity Manager installation package.

3 Open the `user_app-silent.properties` file and modify the following parameters in the file:

Parameter Name	**Description**
USER_INSTALL_DIR=	Specify the installation path for the User Application. For example: `C:\netiq\idm\apps\UserApplication`
NOVL_APP_SERVER_TYPE_CHOICE=	Specify the application server hosting the User Application. This release of Identity Manager supports only Apache Tomcat.
NOVL_TOMCAT_BASE_FOLDER=	Specify the base folder location of the application server hosting the User Application. For example: `C:\netiq\idm\apps\tomcat`
NOVL_APPLICATION_NAME=	Specify the application context name. By default, it contains `IDMProv` as an application context name.

Parameter Name	Description
NOVL_CREATE_DB=	Specify whether you want to configure new or existing database as part of the installation process, or afterward. Alternatively, you can create a schema file at installation time, which the Database Administrator would use to create the tables later. Depending on your requirement, specify one of the following options: ◆ **Now:** The installation program creates the database tables as part of the installation process. ◆ **File:** The installation program generates a SQL script that the database administrator can run to create the databases. If you choose this option, you must also set `NOVL_CONFIG_WRITE_TO_FILE` to 1. You might select this option if you do not have permissions to create or modify a database in your environment. For more information about generating the tables with the file, see “Manually Creating the Database Schema” on page 151. ◆ **Startup:** The installation program leaves instructions to create the tables when the User Application starts for the first time.
NOVL_DATABASE_NEW=	Specify whether you want to use existing, empty databases, or create new tables in the existing database. To create a new database specify `true`. Ensure that a database exists before selecting this option. Otherwise, specify `false`.
NOVL_UPGRADE=	To upgrade your User Application using an existing database, specify `true`. If database is existing and it has User Application tables from a previous installation, specify `false`. If the existing database runs on an Oracle platform, you must prepare Oracle before updating the schema. For more information, see “Preparing an Oracle Database for the SQL File” on page 311.
NOVL_UPGRADE_PROPS_FILE=	If you are upgrading the User Application, specify the path of the properties file of the currently installed application.
NOVL_JDBC_DRIVER=	Specify the absolute path of the JDBC jar file.
NOVL_DB_JARFILE_NAME=	For example: `C:\netiq\idm\apps\postgres\postgresql-9.4.1212.jdbc42.jar`

Parameter Name	Description

NOVL_DB_DRIVER_CLASS_NAME=	Specify the database driver class name for the database that is used for installation.
	- **PostgreSQL:**
	`liquibase.database.core.PostgresDatabase`
	- **Oracle:**
	`liquibase.database.ext.OracleUnicodeDatabase`
	- **MS SQL:**
	`liquibase.database.ext.MSSQLUnicodeDatabase`
	NOTE: MS SQL is supported on Windows only.

NOVL_DB_DRIVER_NAME=	Specify the database driver name.
	- **PostgreSQL:** `org.postgresql.Driver`
	- **Oracle:**
	`oracle.jdbc.driver.OracleDriver`
	- **MS SQL:**
	`com.microsoft.sqlserver.jdbc.SQLServerDriver`
	NOTE: MS SQL is supported on Windows only.

NOVL_DB_JDBC_URL=	Specify the URL to connect to the database running the User Application. - **PostgreSQL:** `jdbc:postgresql://<database server IP address:port>/idmuserappdb` For example, `jdbc:postgresql://192.168.0.1:5432/idmuserappdb` - **Oracle:** `jdbc:oracle:thin:@<database server IP address:port>:idmuserappdb` For example, `jdbc:oracle:thin:@192.168.0.1:1521:idmuserappdb` - **MS SQL:** `jdbc:sqlserver://<database server IP address:port>;DatabaseName=idmuserappdb` For example, `jdbc:sqlserver://192.168.0.1:1433;DatabaseName=idmuserappdb` **NOTE:** MS SQL is supported on Windows only.

Parameter Name	Description
NOVL_DB_TYPE	Select the valid database type. Your options are: PostgreSQL, SQL Server, and Oracle.
NOVL_DB_ORACLE_VERSION=	If you select `Oracle` in NOVL_DB_TYPE, specify the version of the database.
NOVL_DB_HOST=	Specify the hostname or IP address of the User Application database server. For example: `192.168.0.1`
NOVL_DB_PORT=	Specify the port that is used by the User Application database server. For example: 5432
NOVL_DB_NAME=	Specify the name of your database. For example, `idmuserappdb`.
NOVL_DB_USER=	Specify the name of an account that allows the User Application to access and modify data in the databases. For example, `idmadmin`.
NOVL_DB_USER_PASSWORD= NOVL_DB_USER_PASSWORD_CONFIRM=	Specify and confirm the password for the username specified in NOVL_DB_USER.
NOVL_CONFIG_DBADMIN_NAME= NOVL_CONFIG_DBADMIN_PASSWORD= NOVL_CONFIG_DBADMIN_PASSWORD_CONFIRM =	Specify the name and password for the database administrator. You can use the same user account and password that you specified for NOVL_DB_USER and NOVL_DB_USER_PASSWORD. To use that account, do not make any changes.
NOVL_CONFIG_WRITE_TO_FILE=	By default, the value of this property is set to `0`. To write database to a file, change the value to `1`. You might select this option if you do not have permissions to create or modify a database in your environment. For more information about generating the tables with the file, see "Manually Creating the Database Schema" on page 151.
RUN_LDAPCONFIG=	Specify whether you want to configure LDAP settings now or later. The options are: ◆ **Now:** Executes the LDAP configure right away by populating the WAR with the LDAP configuration settings provided. ◆ **Later:** Just installs the User Application files without configuring LDAP settings.
NOVL_JAVA_HOME=	Specify the JAVA_HOME path for this attribute and specify the same path for `USER_MAGIC_FOLDER_1` attribute also. For example: `C:\netiq\idm\apps\jre`

Parameter Name	Description
NOVL_AUDIT_OFF= NOVL_AUDIT_ON=	Specify whether you want to set up auditing for the User Application. By default auditing is enabled. If you choose this option, you must also set NOVL_AUDIT_SERVER and NOVL_AUDIT_LOG_CACHE_DIR properties.
NOVL_AUDIT_SERVER=	If auditing is enabled, specify the hostname or IP address of the Audit server. For example: 192.168.0.1
NOVL_AUDIT_LOG_CACHE_DIR=	If auditing is enabled, specify the absolute path of audit cache. For example: C:\Program Files\Novell\audit
NOVL_XDAS_OFF= NOVL_XDAS_ON=	Do not use this option. XDAS is not supported with identity applications. You must use Common Event Format (CEF), an open log management standard, for auditing events. CEF logging is disabled by default. To enable it, see Configuring Identity Manager Components to Log Audit Events in CEF Format in the *NetIQ Identity Manager - Configuring Auditing in Identity Manager*.
NOVL_XDAS_SERVER_NAME=	Do not use this option. XDAS is not supported with identity applications.
NOVL_XDAS_LOGGING_DIR=	Do not use this option. XDAS is not supported with identity applications.
NOVL_UA_OSP_PWD=	Specify the User Application and OSP password.
NOVL_USE_EXTERNAL_AUTH_SERVER=	If OSP is installed on a different server, you can configure that server for external authentication with the User Application. If you choose this option, you must also set the following properties: ◆ NOVL_EXTERNAL_AUTH_PROTOCOL ◆ NOVL_EXTERNAL_AUTH_HOSTNAME ◆ NOVL_EXTERNAL_AUTH_PORT By default, authenticating to an external server is disabled.
NOVL_EXTERNAL_AUTH_PROTOCOL=	If you are using an external server for authentication, specify the external authentication protocol. For example: http/https
NOVL_EXTERNAL_AUTH_HOSTNAME=	If you are using an external server for authentication, specify the hostname or IP address of the authentication server. For example: 192.168.0.1

Parameter Name	Description
NOVL_EXTERNAL_AUTH_PORT=	If you are using an external server for authentication, specify the port value of the authentication server. For example: `8180` for `http`, `8443` for `https`
NOVL_CONFIG_UPDATE_FILE_PATH=	Specify the path for the configuration update properties file. For example: `C:\configupdate.properties`

Executing a Silent Installation of the Identity Applications

1. Log in as administrative user to the computer where you want to install the identity applications.
2. Specify the values for the installation. For more information, see "Setting Passwords in the Environment for a Silent Installation" on page 134.
3. To launch the installation program for your platform, enter the following command:

   ```
   IdmUserApp.exe -i silent -f \yourdirectorypath\user_app-
   silent.properties
   ```

   NOTE: If the `user_app-silent.properties` file is in a different directory from the installer script, you must specify the full path to the file. The script unpacks the necessary files to a temporary directory and then launches the silent installation.

Post-Installation Steps

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

- "Adding the User Application Schema to your Audit Server as a Log Application" on page 141
- "Passing the preferIPv4Stack Property to JVM" on page 141
- "Checking the Health of the Server" on page 142
- "Monitoring the Health Statistics" on page 142
- "Creating Compound Indexes" on page 143
- "Configuring Identity Application to Reject Client-initiated SSL Renegotiation" on page 143

If you used the convenience installer for Tomcat, the installation programs for Identity Manager configure Tomcat for you. If you installed your own Tomcat program, consider the following issues:

- You can modify the Tomcat service to perform more effectively. For more information, see *So You Want High Performance*.
- You might want to add support for logging events. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 98.

Adding the User Application Schema to your Audit Server as a Log Application

If your Audit server will use the User Application as a log application, you must copy the `dirxml.lsc` file to the server. This section applies to Novell Identity Audit only.

1. Locate the `dirxml.lsc` file.

   This file is located in the Identity Manager User Application installation directory after the install, for example `C:\NetIQ\idm\apps\UserApplication`.

2. Use a web browser to access an iManager with the Novell Identity Audit plug-in installed, and log in as an administrator.
3. Navigate to **Roles and Tasks > Auditing and Logging** and then select **Logging Server Options**.
4. Browse to the Logging Services container in your tree and select the appropriate Audit Secure Logging Server, then click **OK**.
5. In the **Log Applications** tab, select the appropriate Container Name, and then click the **New Log Application** link.
6. In the New Log Application dialog box, complete the following steps:

   6a For Log Application Name, specify any name that is meaningful for your environment.

   6b For Import LSC File, browse to the `dirxml.lsc` file.

   6c Click **OK**.

7. Click **OK** to complete your Audit server configuration.
8. Ensure that the status on the Log Application is set to **ON**. (The circle under the status should be green.)
9. Restart the Audit server to activate the new log application settings.

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`.

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,

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/
  threadinfo?stack=true
  ```

  To specify the number of threads in the JVM, specify the value for the **thread-count** parameter.

  For example,

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/
  threadinfo?thread-count=1
  ```

- **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,

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/clusterinfo
  ```

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"
```

Disabling the Prevent HTML Framing Setting for Integrating Identity Manager with SSPR

This section discusses the configuration required for Identity Manager to integrate it with an existing SSPR 4.2 environment which is not deployed by Identity Manager 4.5. SSPR provides a configurable option, **Prevent HTML Framing**, that allows users to view SSPR in an inline frame for any application that includes the iframe html source code. If you select this option, SSPR is not included in the specified iFrame for the application. To disable this option for Identity Manager, run the following steps:

1. Go to http://*<IP/DNS name>:<port>/sspr.* This link takes you to the SSPR portal.
2. Log in as SSPR administrator.
3. Click **Configuration Editor** at the top of the page and specify the OSP configuration password.
4. Click **Settings > Security** > **Always Show Advanced Settings**, and do the following actions:

   4a Browse for **Prevent HTML Framing,** de-select **Enabled** and then click **Save** to save the setting.

   4b In the confirmation window, click **OK**.

Verifying the User Properties

To enable your users to use identity applications, you must ensure that user properties with necessary rights are added to the container that consists all your system users. You can verify these properties using iManager. Perform the following steps in iManager to verify these settings:

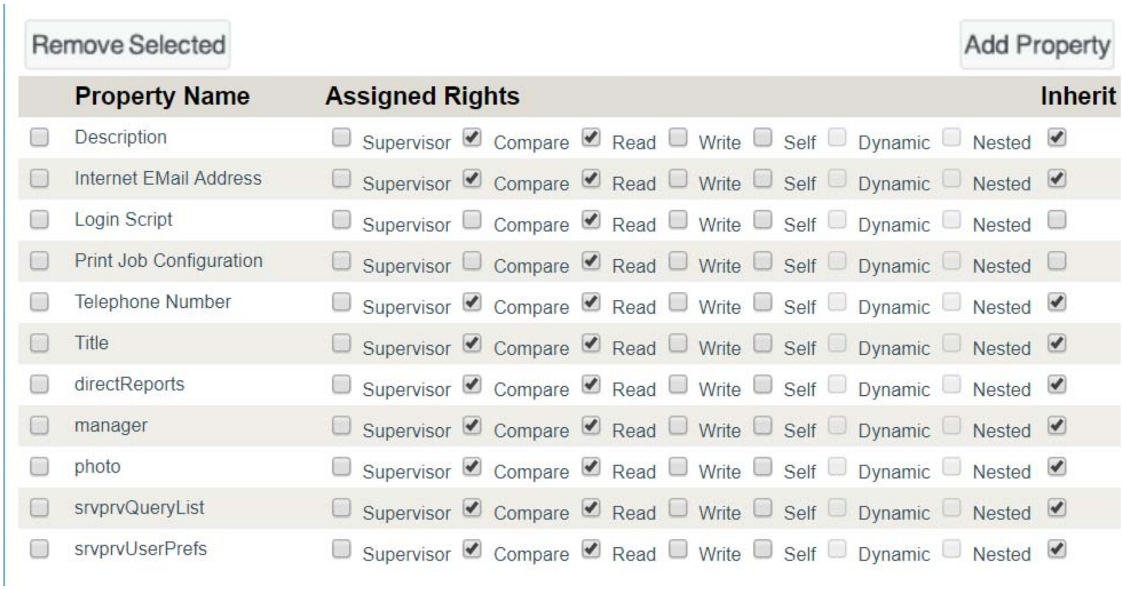
1. Log in to iManager as an administrator using your Identity Vault IP address as tree.
2. In the **Tree** panel, select the tree where your identity applications are configured.
3. Click **Assigned Rights** for the container which consists of all the system users.
4. Verify that the following properties are having the necessary rights in the list:
   - Description
   - Internet EMail Address
   - Login Script
   - Print Job Configuration
   - Telephone Number
   - Title
   - directReports
   - manager
   - photo
   - srvprvQueryList
   - srvprvUserPrefs

If any of the properties are missing, click **Add Property**.

4a Select the required property from the list and click **Done**.

4b Select the necessary rights to the property and click **Done**.

Figure 11-1 *Adding Properties to the User Container*



	Property Name	Assigned Rights							Inherit
☐	Description	☐ Supervisor	☑ Compare	☑ Read	☐ Write	☐ Self	☐ Dynamic	☐ Nested	☑
☐	Internet EMail Address	☐ Supervisor	☑ Compare	☑ Read	☐ Write	☐ Self	☐ Dynamic	☐ Nested	☑
☐	Login Script	☐ Supervisor	☐ Compare	☑ Read	☐ Write	☐ Self	☐ Dynamic	☐ Nested	☐
☐	Print Job Configuration	☐ Supervisor	☐ Compare	☑ Read	☐ Write	☐ Self	☐ Dynamic	☐ Nested	☐
☐	Telephone Number	☐ Supervisor	☑ Compare	☑ Read	☐ Write	☐ Self	☐ Dynamic	☐ Nested	☑
☐	Title	☐ Supervisor	☑ Compare	☑ Read	☐ Write	☐ Self	☐ Dynamic	☐ Nested	☑
☐	directReports	☐ Supervisor	☑ Compare	☑ Read	☐ Write	☐ Self	☐ Dynamic	☐ Nested	☑
☐	manager	☐ Supervisor	☑ Compare	☑ Read	☐ Write	☐ Self	☐ Dynamic	☐ Nested	☑
☐	photo	☐ Supervisor	☑ Compare	☑ Read	☐ Write	☐ Self	☐ Dynamic	☐ Nested	☑
☐	srvprvQueryList	☐ Supervisor	☑ Compare	☑ Read	☐ Write	☐ Self	☐ Dynamic	☐ Nested	☑
☐	srvprvUserPrefs	☐ Supervisor	☑ Compare	☑ Read	☐ Write	☐ Self	☐ Dynamic	☐ Nested	☑

Configuration and Usage Considerations for the Identity Applications

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

- Before users can access the identity applications, you must complete the following activities:
  - Ensure that all necessary Identity Manager drivers are installed.
  - Ensure that the indexes for the Identity Vault are in Online mode. For more information about configuring an index during installation, see “Miscellaneous” on page 171.
  - Enable cookies on all browsers. The applications do not work when cookies are disabled.
- Users cannot access the identity applications as a guest or anonymous user without being logged in to the identity applications. The users are prompted to log in to the user interface. For more information, see Configuring Single Sign-on Access in Identity Manager in the *NetIQ Identity Manager - Administrator’s Guide to the Identity Applications*.
- To ensure that Identity Manager enforces Universal Password functionality, configure the Identity Vault to use NMAS Login as the process for a user’s first login. Add `NDSD_TRY_NMASLOGIN_FIRST` with the string value `true` to the `HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Environment` registry key.
- (Conditional) To run reports, you must have the components for Identity Reporting installed in your environment. For more information, see *Administrator Guide to NetIQ Identity Reporting*.

- 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 the 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. For more information, see the *NetIQ Identity Manager - Configuring Auditing in Identity Manager*.

Starting the Identity Applications

This section provides instructions for starting the identity applications and logging in the first time on an application server. In a cluster environment, start the procedure on the primary node. The identity applications should be installed and ready for deployment. For more information about post-installation tasks, see "Completing the Installation of the Identity Applications" on page 150.

You use `services.msc` startup script to start the Tomcat service. You can also use this file for stopping and restarting the Tomcat service.

If your browser does not display the User Application page after you complete these steps, check the terminal console for error messages and refer to Chapter 29, "Troubleshooting," on page 321.

To start the identity applications:

1 Start the database for the identity applications. For more information, see your database documentation.

2 For the User Application to run reports, add the `Djava.awt.headless=true` flag to the startup script for Tomcat. For example:

```
JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -
Dsun.jnu.encoding=UTF-8 -server -Xms1024m -Xmx1024m -
XX:MaxPermSize=512m
```

NOTE: You do not need to perform this step if you are running on an X11 Windows system.

3 Start Tomcat where you installed the identity applications.

NOTE: In a cluster, start the primary node only.

4 At the command line, make the installation directory your working directory.

5 Execute the startup script.

6 To enable communication with the User Application driver, complete the following steps:

6a Log in to iManager.

6b Under **Roles and Tasks > Identity Manager** in the left navigation frame, click **Identity Manager Overview**.

6c In the content view, specify the driver set that contains the User Application driver, then click **Search**.

6d In the graphic showing the driver set with its associated drivers, click the red-and-white icon for the User Application driver.

6e Click **Start Driver**.

Upon start, the driver attempts a “handshake” with the User Application. If your application server is not running or if the WAR was not deployed successfully, the driver returns an error. Otherwise, the driver status changes to the yin-yang symbol, indicating that the driver is now started.

7 To start the Role and Resource Service driver, repeat the procedure in Step 6.

8 To launch and log in to the User Application, enter the following URL in your web browser:

`http://`*`hostname`*`:`*`port/ApplicationName`*

hostname

Represents the name of the application server (Tomcat). For example, `myserver.domain.com`

port

Represents the port number of the application server. For example, `8180`.

ApplicationName

Represents the name that you specified during the installation for the application when you provided application server configuration information. For example, `IDMProv`.

9 In the upper right corner of the User Application landing page, click **Login**.

10 (Conditional) To enable the User Application in a cluster group, complete the following steps:

10a Click **Administration**.

10b In the Application Configuration portal, click **Caching**.

10c In the Caching Management window, select **True** for **Cluster Enabled**.

10d Click **Save**.

10e Restart the server.

10f (Conditional) To use local settings, repeat this procedure for each server in the cluster.

Creating and Deploying the Drivers for the Identity Applications

The process for installing RBPM adds the files for creating the drivers for the Identity Applications. The driver configuration support allows you to do the following:

- Associate one User Application driver with a Role and Resource Service driver.
- Associate one User Application with a User Application driver.

Before you attempt to configure the drivers, ensure that you have all of the necessary packages in the Package Catalog in Designer. When you create a new Identity Manager project, the user interface automatically prompts you to import several packages into the new project.

- "Creating the User Application Driver" on page 148
- "Creating the Role and Resource Service Driver" on page 148
- "Deploying the Drivers for the User Application" on page 149

Creating the User Application Driver

The User Application driver serves both as a runtime component and as a storage wrapper for directory objects (comprising the User Application's runtime artifacts). It is responsible for storing application-specific environment configuration data. The driver also notifies the directory abstraction layer when important data values change in the Identity Vault. This notification causes the directory abstraction layer to update its cache.

1. Open your project in Designer.
2. In the **Modeler > Provisioning** view, select **User Application** in the palette.
3. Drag the icon for **User Application** onto the **Modeler** view.
4. In the Driver Configuration Wizard, select **User Application Base**, and then click **Next**.
5. At the prompt for installing several additional packages, click **OK**.
6. (Optional) Specify the name of the driver.

   Click **Next**.
7. In the connection parameters window, specify the ID and password for the User Application Administrator.
8. Specify the host and port for the User Application server.
9. Specify the application context for the User Application server.
10. (Optional) To allow the Provisioning Administrator to start workflows in the name of another person for whom the Provisioning Administrator is designated as proxy, select **Yes** for **Allow Initiator Override**.
11. In the **Confirm Installation Tasks** window, click **Finish**.

Creating the Role and Resource Service Driver

The User Application uses the Role and Resource Service Driver to manage back-end processing of resources. For example, it manages all resource requests, starts workflows for resource requests, and initiates the provisioning process for resource requests.

1. Open your project in Designer.
2. In the **Modeler > Provisioning** view, select **Role Service** in the palette.
3. Drag the icon for **Role Service** onto the **Modeler** view.
4. In the Driver Configuration Wizard, select **Role and Resource Service Base**, and then click **Next**.

5 (Conditional) If this is the first driver you have installed in Designer, click **OK** to install the **Common Settings Advanced Edition** package.

5a Specify the URL for the User Application server.

5b Specify the eDirectory DN for the User Application Administrator.

5c Specify the LDAP DN for the User Application Provisioning Service account. It can be the same account as your User Application Administrator or a different account.

If a Role or Resource provisioning request is initiated by this service account, then any approvals or provisioning workflows associated with this role or resource are bypassed.

6 (Optional) Specify the name of the driver.

7 Click **Next**.

8 In the User Application/Workflow Connection window, specify the User-Group base container DN and the User Application Driver that you just created.

Since the driver has not yet been deployed, the browse function will not show the User Application Driver that you just configured. You might need to type the DN for the driver.

9 Specify the URL for the User Application.

10 Specify the LDAP DN of the User Application Administrator account

The User Application Administrator account authenticates to the User Application in order to start the Approval Workflow. For more information, see “Assigning Rights to Identity Vault Administrator and User Application Administrator Account” on page 121.

11 Specify the password of the User Application Administrator account.

12 Click **Next**.

13 In the Confirm Installation Tasks window, click **Finish**.

Deploying the Drivers for the User Application

The User Application and the Role and Resource Service drivers will not be available for use until you deploy them.

NOTE: When replicating an eDirectory environment, you must ensure that the replicas contain the NCP Server object for Identity Manager. Identity Manager is constrained to local replicas of a server. Due to this, Role and Resource Service Driver might not start properly if a secondary server does not include the server object.

To deploy the drivers:

1 Open your project in Designer.

2 In either the **Modeler** or the **Outline** view, select the Driver Set.

3 Click **Live > Deploy**.

Completing the Installation of the Identity Applications

This section provides instructions for activities that you might want to perform after installing identity application and their framework:

- "Checking the Health of the Server in a Clustered Environment" on page 150
- "Accessing the Oracle Database Using Oracle Service Name" on page 150
- "Manually Creating the Database Schema" on page 151
- "Manually Import the Identity Applications and Identity Reporting Certificates into Identity Vault" on page 152
- "Recording the Master Key" on page 153
- "Configuring the Identity Vault for the Identity Applications" on page 153
- "Changing the Default Context Name for User Application" on page 153
- "Reconfiguring the WAR File for the Identity Applications" on page 156
- "Configuring Forgotten Password Management" on page 156

Checking the Health of the Server in a Clustered Environment

For more information see, "Checking the Health of the Server" on page 142

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 151.

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. Have the database administrator run the SQL script to create and configure the User Application database.
7. 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
```

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 151.
12. After the database administrator imports the SQL file, start Tomcat.

Manually Import the 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 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 -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, ensure that the SSPR application certificate is added to User Application’s `cacerts`.

  For example, you can use the following keytool command to import certificates into User Application:

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

Recording the Master Key

NetIQ recommends that you copy the encrypted master key and record it in a safe place immediately after installation. If this installation is on the first member of a cluster, use this encrypted master key when installing the identity applications on other members of the cluster.

WARNING: Always keep a copy of the encrypted master key. You need the encrypted master key to regain access to encrypted data if the master key is lost. For example, you might need the key after an equipment failure.

Configuring the Identity Vault for the Identity Applications

The identity applications must be able to interact with the objects in your Identity Vault.

To improve the performance of the identity applications, the eDirectory Administrator should create value indexes for the manager, ismanager and srvprvUUID attributes. Without value indexes on these attributes, identity application users can experience impeded performance, particularly in a clustered environment.

You can create these value indexes automatically during installation by selecting Advanced > Create eDirectory Indexes in the RBPM Configuration utility. For more information about using Index Manager to create value indexes, see the *NetIQ eDirectory Administration Guide*.

Changing the Default Context Name for User Application

Instead of using the default context name, you can create a new context based on your organizational requirements. You can change the context name by performing the following actions:

1. Stop the Tomcat service by using the `services.msc` file.
2. Navigate to the User Application directory located in `C:\NetIQ\idm\apps\UserApplication`.
3. Launch the configupdate utility in GUI mode.

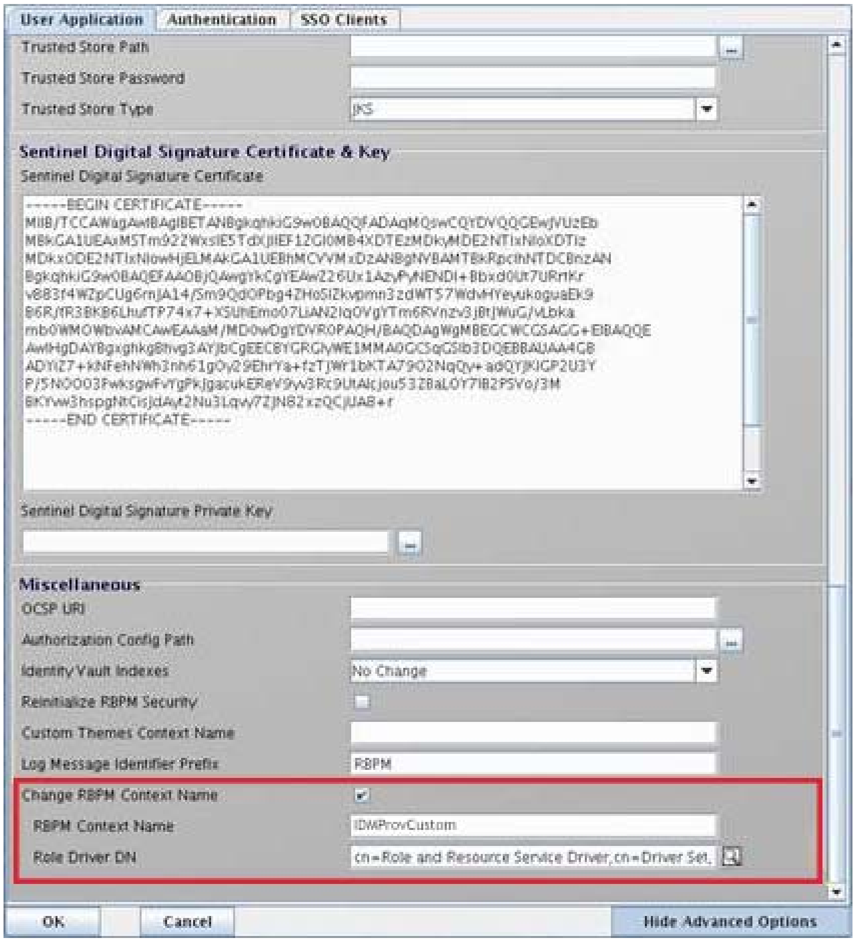
   Ensure that the `use_console` option is set to `false` in `configupdate.bat.properties` file.
4. In the **User Application** tab, click **Show Advanced Options** and perform the following steps:

   4a Select **Change RBPM Context Name**.

   4b Specify the custom context name in **RBPM Context Name**. For example, `IDMProvCustom`.

   4c Browse to and select the Roles Driver DN. For example, `cn=Role and Resource Service Driver,cn=Driver Set,o=system`.

4d Click **OK**.



Trusted Store Path

Trusted Store Password

Trusted Store Type: JKS

Sentinel Digital Signature Certificate & Key

Sentinel Digital Signature Certificate

```
-----BEGIN CERTIFICATE-----
MIIB/TCCAWagAwIBAgIBETANBgkqhkiG9w0BAQQFADAqMQswCQYDVQQGEwJVUzEb
MBkGA1UEAxMSTm92ZWxsIE5TdXJlIEF1ZGl0MB4XDTEzMDkyMDE2NTIxNloXDTIz
MDkxODE2NTIxNlowHjELMAkGA1UEBhMCVVMxDzANBgNVBAMTBkRpcihNTDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAw226Ux1AzyPyNENDI+8bxd0Ut7URnKr
v883f4WZpCUg6rnJA14/Sm9QdOPbg4ZHoSIZkvpmn3zdWT57WdvHYeyukoguaEk9
B6R/tR3BKB6LhufTP74x7+XSUhEmo07LiAN2Iq0VgYTm6RVnzv3jBtJWuG/vLbka
mb0WMOWbvAMCAwEAAaM/MD0wDgYDVR0PAQH/BAQDAgWgMBEGCWCGSAGG+EIBAQQE
AwIHgDAYBgxghkgBhvg3AYJbCgEEC8YGRGlyWE1MMA0GCSqGSIb3DQEBBAUAA4GB
ADYiZ7+kNFehNWh3nh61gOy29EhrYa+fzTJWr1bKTA79O2NqQy+adQYJKIGP2U3Y
P/5NOOO3FwksgwFvYgPkJgacukEReV9w3Rc9UtAlcjou53ZBaLOY7lB2P5Vo/3M
BKYww3hspgNtCisJdAyt2Nu3Lqvy7ZJN82xzQCjUAB+r
-----END CERTIFICATE-----
```

Sentinel Digital Signature Private Key

Miscellaneous

OCSP URI

Authorization Config Path

Identity Vault Indexes: No Change

Reinitialize RBPM Security: ☐

Custom Themes Context Name

Log Message Identifier Prefix: RBPM

Change RBPM Context Name: ☑

RBPM Context Name: IDMProvCustom

Role Driver DN: cn=Role and Resource Service Driver,cn=Driver Set,

5 Verify that the war file is renamed.

- Navigate to the `Tomcat webapps` folder and check if `IDMProvCustom.war` entry is updated.
- Navigate to `ism-configuration` properties file located in `\TOMCAT_INSTALLED_HOME\conf` and check if `portal.context` entry specifies the new context name.

6 Update your database with the new context name by using the `update-context.bat` file located in `C:\NetIQ\idm\apps\UserApplication`.

Execute the following command to run the `update-context.bat` file.

```
ua:C:\NetIQ\idm\apps\UserApplication # vi update-context.bat
```

You should see the following entries on your screen:

```
# copy and paste or execute this script before changing context name

# Substitute your new context where indicated

#
```

```
C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m  -Dwar.context.name=[New
Context Here] -Ddriver.dn=[UA Driver DN] -jar
C:\NetIQ\idm\apps\UserApplication\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase  --
driver=org.postgresql.Driver  --classpath=
C:\NetIQ\idm\apps\postgres\postgresql-9.4.1212.jdbc42.jar:
C:\NetIQ\idm\apps\tomcat\webapps\IDMProv.war --
changeLogFile=UpdateProducerId.xml   --url="jdbc:postgresql://
localhost:5432/idmuserappdb?compatible=true" --contexts="prov,updatedb"
--logLevel=debug --username=******** --password=******** update
```

For example, run the following script if you are using a PostgreSQL database:

```
C:\NetIQ\idm\apps\jre\bin\java -Xms256m -Xmx256m  -
Dwar.context.name=IDMProvCustom  -Ddriver.dn= cn=Role and Resource
Service Driver,cn=driverset1,o=system -jar
C:\NetIQ\idm\apps\UserApplication\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase  --
driver=org.postgresql.Driver  --classpath=
C:\NetIQ\idm\apps\postgres\postgresql-9.4.1212.jdbc42.jar:
C:\NetIQ\idm\apps\tomcat\webapps\IDMProv.war --
changeLogFile=UpdateProducerId.xml  --url="jdbc:postgresql://<Database
Server:5432/idmuserappdb?compatible=true" --contexts="prov,updatedb" --
logLevel=debug -–username=dbadmin --password=******** update
```

where

`-Dwar.context.name=IDMProvCustom` specifies the new context.

`-Ddriver.dn ="cn=User Application Driver,cn=driverset1,o=system"` specifies the User Application driver DN.

`--username=dbadmin` specifies the database administrator username that can create database tables, views, and other artifacts.

IMPORTANT: Do not change the database driver details in the script for other supported databases.

7 Verify that the database tables have the new context name.

Table Name	Column to Check
PORTALPRODUCERS	producerid
PORTALPRODUCERREGISTRY	producerid
PORTALREGISTRY	producerid
PORTALPORTLETSETTINGS	producerid
PORTALPORTLETHANDLES	producerid
PROFILEGROUPPREFERENCES	elementid

For example, run the following SQL command to verify the new context name in the PORTALPRODUCERS table:

```
Select * from PORTALPRODUCERS;
```

The command should return only the new context name.

8. Start the Tomcat service by using the `services.msc` file.

Reconfiguring the WAR File for the Identity Applications

To update your WAR file for the identity applications, run the RBPM Configuration utility.

1. Run the utility in the install directory by executing `configupdate.bat`.

   For more information about utility parameters, see "Configuring the Settings for the Identity Applications" on page 161.

2. Deploy the new WAR file to your application server.

   For Tomcat single server, the changes are applied to the deployed WAR.

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 156
- "Using the Legacy Provider for Forgotten Password Management" on page 158
- "Using an External System for Forgotten Password Management" on page 159
- "Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment" on page 161

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 156
- "Configuring Self Service Password Reset for Identity Manager" on page 157
- "Locking the SSPR Configuration" on page 157

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 RBPM configuration utility. For more information, see "Running the Identity Applications Configuration Utility" on page 162.
3. In the utility, navigate to **Authentication > Password Management**.
4. For **Password Management Provider**, specify **SSPR**.
5. Select **Forgotten Password**.
6. Navigate to **SSO Clients > Self Service Password Reset**.

7 For **OSP 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 **OSP client secret**, specify the password for the single sign-on client for SSPR.

9 For **OSP 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. For more information about the configuration password, see "Installing Password Management for Identity Manager" on page 107.

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 157.

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 the Legacy Provider for Forgotten Password Management

Instead of SSPR, you can use the legacy provider in Identity Manager for the Forgotten Password Management feature. If you choose the legacy provider, you do not need to install SSPR. However, you will need to reassign permissions for users to access the shared pages for password management. This section provides the steps to perform these activities:

- "Configuring the Legacy Provider for Forgotten Password Management" on page 158
- "Reassigning Permissions for the Password Management Pages" on page 159

For more information about shared pages and permissions, see Page Administration in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Configuring the Legacy Provider for Forgotten Password Management

1 Log in to the server where you installed the identity applications.

2 Run the RBPM configuration utility. For more information, see "Running the Identity Applications Configuration Utility" on page 162.

3 In the utility, navigate to **Authentication > Password Management**.

4 For **Password Management Provider**, specify **User Application (Legacy)**.

5 For **Forgotten Password**, specify **Internal**.

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

7 For **OSP redirect URL**, the setting should be empty.

8 Save your changes and close the utility.

Reassigning Permissions for the Password Management Pages

The settings for the identity applications default to SSPR during installation. You must assign or reassign the permissions for the users, groups, or containers that you want to access the shared pages for managing passwords. When you assign users `View` permission for a container page or shared page, the users can access the page and see it in a list of available pages.

1. Ensure that Identity Manager is using the legacy provider. For more information, see "Configuring the Legacy Provider for Forgotten Password Management" on page 158.
2. Log in to the User Application as the application administrator. For example, log in as `uaadmin`.
3. Navigate to **Administration > Page Admin**.
4. In the **Shared Pages** panel, navigate to **Password Management**.
5. Select the page for which you want to specify permissions. For example, Change Password or Password Challenge Response.
6. In the right panel, click **Assign Permission**.
7. In **View**, select the users, groups, or containers that you want to assign to the page.
8. (Optional) To ensure that only an application administrator can access the specified page, select **View Permission Set to Admin Only**.
9. Click **Save**.
10. Perform Step 5 through Step 9 for each page that you want to configure.
11. Select the **Home** icon to return to the Dashboard.
12. Navigate to **Applications**, then select ⚙.
13. On the **Manage Applications** page, replace the link to SSPR with the link for UserApp PwdMgt.

    For more information, see "Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment" on page 161 and the *Help for the Identity Applications*.
14. Log out and then 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 160
- "Testing the External Forgot Password Configuration" on page 160
- "Configuring SSL Communication between Application Servers" on page 161

Specifying an External Forgotten Password Management WAR File

If you did not specify this 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 "Running the Identity Applications Configuration Utility" on page 162.

   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 161.

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:

- Directly, in a browser. Go to the Forgot Password page in the external password WAR file. For example, `http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`.
- 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 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 162
- "User Application Parameters" on page 162
- "Reporting Parameters" on page 173

- "Authentication Parameters" on page 174
- "SSO Clients Parameters" on page 178
- "CEF Auditing Parameters" on page 182

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 162
- "Identity Vault DNs" on page 164
- "Identity Vault User Identity" on page 166
- "Identity Vault User Groups" on page 167
- "Identity Vault Certificates" on page 168
- "Email Server Configuration" on page 168
- "Trusted Key Store" on page 170
- "NetIQ Sentinel Digital Signature Certificate & Key" on page 170
- "Miscellaneous" on page 171
- "Container Object" on page 172

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

Specifies 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

Specifies 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

Specifies 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

Specifies 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. On Linux, the user must have permission to write to this 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 values 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 an 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. For example, `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

Applies only when you enable **Sign email***.*

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

Alias of signature key

Applies only when you enable **Sign email***.*

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

Signature key password

Applies 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 173
- "Report Retention Values" on page 174
- "Modify Locale" on page 174
- "Role Configuration" on page 174

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**

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 175
- "Authentication Configuration" on page 175
- "Authentication Method" on page 176
- "Password Management" on page 176
- "Sentinel Digital Signature Certificate and Key" on page 177

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.

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.

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.

Forgotten Password

This check box parameter applies only when you want to use SSPR.

Specifies whether you want users to recover a forgotten password without contacting a help desk.

You must also configure the challenge-response policies for the Forgotten Password feature. For more information, see the *NetIQ Self Service Password Reset Administration Guide*.

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 e 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
```

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

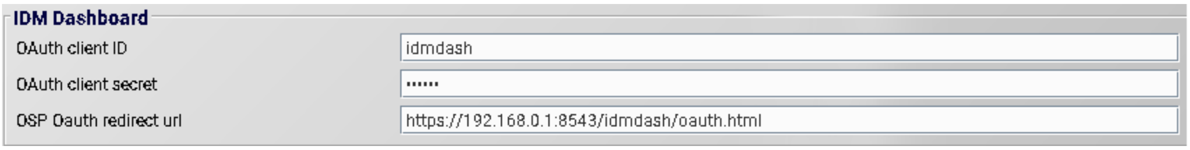
When configuring the identity applications, this tab defines the values for managing single sign-on access to the applications.

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 178
- "IDM Administrator" on page 179
- "RBPM" on page 179
- "Reporting" on page 180
- "IDM Data Collection Service" on page 181
- "DCS Driver" on page 181
- "Self Service Password Reset" on page 181

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.



IDM Dashboard

OAuth client ID: idmdash

OAuth client secret: ••••••

OSP Oauth redirect url: https://192.168.0.1:8543/idmdash/oauth.html

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

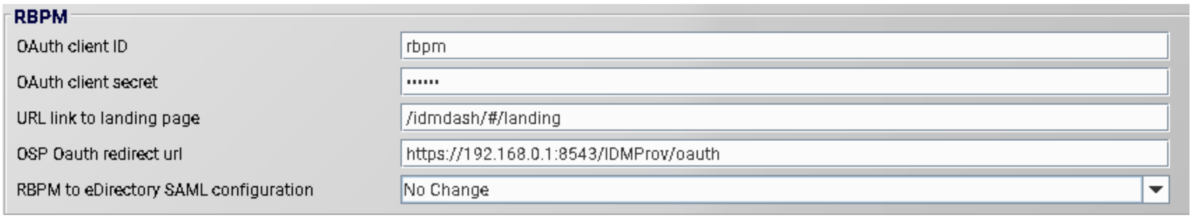
> *Required*
>
> Specifies the password for the single sign-on client for the Identity Manager Administrator.

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.



RBPM

OAuth client ID	rbpm
OAuth client secret	••••••
URL link to landing page	/idmdash/#/landing
OSP Oauth redirect url	https://192.168.0.1:8543/IDMProv/oauth
RBPM to eDirectory SAML configuration	No Change

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`.

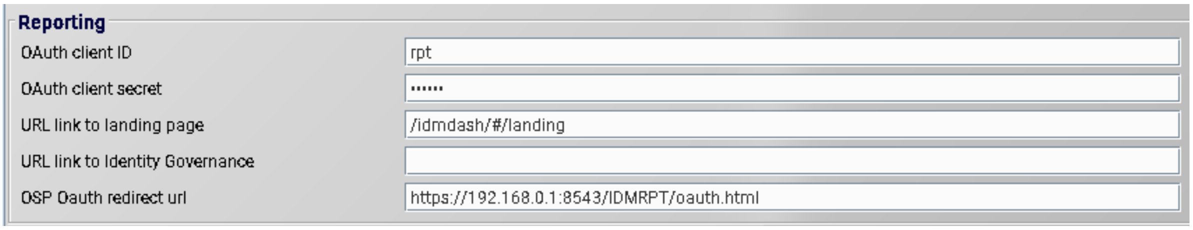
RBPM to eDirectory SAML configuration

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.



Reporting

OAuth client ID	rpt
OAuth client secret	••••••
URL link to landing page	/idmdash/#/landing
URL link to Identity Governance	
OSP Oauth redirect url	https://192.168.0.1:8543/IDMRPT/oauth.html

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.

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

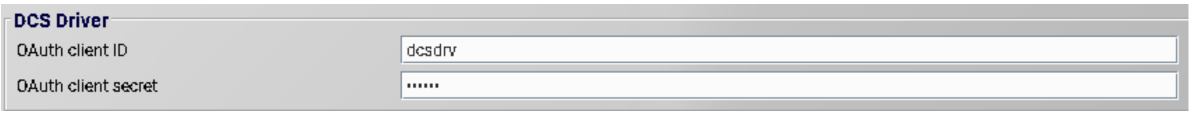
Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

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 11-2



DCS Driver

OAuth client ID	dcsdrv
OAuth client secret	••••••

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 `dcsdrv`.

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.

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/sspr/public/oauth.html`.

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 cache directory. Otherwise, you cannot access the IDMDash and IDMProv applications. Also, none of the OSP events will be logged in the cache directory. For example, you can change the permission and ownership of the directory using the `chown novlua:novlua /<directorypath>` command, where `<directorypath>` is the cache file directory path.

IV Installing Identity Reporting

This section guides you through the process of installing the required components for running reports. The installation process includes all components required for the application:

- NetIQ Identity Reporting
- Identity Manager Driver for Managed System Gateway (MSGW driver)
- Identity Manager Driver for Data Collection Services (DCS driver)

The installation files are located in the `\products\Reporting` directory within the `.iso` image file for the Identity Manager installation package. By default, the installation program installs the components in `C:\NetIQ\idm\apps\IDMReporting`.

For your convenience, the Identity Manager installation kit includes Sentinel Log Management for IGA (Sentinel) to use as a built-in auditing service. For more information, see Installing Sentinel Log Management for Identity Governance and Administration in the NetIQ Identity Manager Setup Guide for Linux.

NetIQ recommends that you review the installation process before beginning. For more information, see Chapter 12, “Planning to Install Identity Reporting,” on page 185.

WARNING: Identity Reporting is used by both Identity Manager and Identity Governance. You must always rely on Identity Manager patch channel to update Identity Reporting for Identity Manager. Otherwise, conflicts will arise during regular Identity Manager patch updates.

12 Planning to Install Identity Reporting

This section provides guidance for preparing to install the components for Identity Reporting. You can use Sentinel to audit events.

- "Checklist for Installing Identity Reporting" on page 185
- "Understanding the Installation Process for the Identity Reporting Components" on page 186
- "Prerequisites for Installing the Identity Reporting Components" on page 187
- "Identifying Audit Events for Identity Reporting" on page 187

Checklist for Installing Identity Reporting

NetIQ recommends that you complete the steps in the following checklist:

	Checklist Items
☐	1. Review the planning information. For more information, see Part I, "Planning to Install Identity Manager," on page 17.
☐	2. Review the hardware and software requirements for the computers that will host the Identity Reporting. For more information, see the following sections: - Meeting System Requirements - Prerequisites for Installing the Identity Reporting Components
☐	3. Ensure that you have installed the identity applications if you are installing Advanced Edition. For more information, see "Planning to Install the Identity Applications" on page 115. You do not need Identity Applications for Standard Edition.
☐	4. To audit events, install Sentinel on a Linux server. For more information, see the Installing Sentinel Log Management for Identity Governance and Administration in the NetIQ Identity Manager Setup Guide for Linux.
☐	5. Ensure that the server where you want to install Identity Reporting has an application server, such as Tomcat. For more information, see "Installing PostgreSQL and Tomcat" on page 92.
☐	6. (Conditional) To use the Apache Log4j service to record events in Tomcat, ensure that you have the appropriate files. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 98.
☐	7. Install Identity Reporting: - For a guided installation, see "Using the Guided Process to Install Identity Reporting" on page 189. - To install reporting silently, see "Installing Identity Reporting Silently" on page 194.

	Checklist Items
❑	8. Complete the Identity Reporting set up. For more information, see Chapter 14, “Configuring Identity Reporting,” on page 199.
❑	9. Configure the Managed System Gateway and Data Collection Services drivers. For more information, see “Configuring Drivers for Identity Reporting” on page 201.
❑	10. Deploy and start the drivers. For more information, see “Deploying and Starting Drivers for Identity Reporting” on page 207.
❑	11. Configure the environment for the drivers. For more information, see “Configuring the Runtime Environment” on page 212.
❑	12. Configure Identity Manager and Identity Vault to send data to the drivers. For more information, see “Setting Auditing Flags for the Drivers” on page 220.

Understanding the Installation Process for the Identity Reporting Components

You can install Sentinel, Identity Reporting and the Reporting drivers on the same server. However, due to the workload, NetIQ recommends installing Sentinel and Reporting on separate servers.

In case of a fresh installation, the installation program creates tables in the database and verifies connectivity. The program also installs a JAR file for the PostgreSQL JDBC driver, and automatically uses this file for database connectivity.

If you have migrated your data, for example, SIEM, from EAS to PostgreSQL database, then the installation program will connect to the existing database.

The installation program for Identity Reporting performs the following functions:

- Allows you to choose an application server platform
- Deploys the client WAR file (DCS and Reporting), which contains the user interface components for reporting, to Tomcat
- Deploys the core WAR file (DCS and Reporting), which contains the core REST services needed for reporting
- Deploys the API WAR file, which contains the documentation of REST services needed for reporting
- Deploys the API WAR file, which contains the Identity Manager Data Collection Services needed for reporting
- Configures the authentication services for Identity Reporting
- Configures the email delivery system for Identity Reporting
- Configures the core reporting services for Identity Reporting
- Creates the user accounts for Identity Reporting (**idmrptsrv** and **idmrptuser**)
- Creates the user accounts for interacting with Sentinel (**appuser** and **rptuser**)

Prerequisites for Installing the Identity Reporting Components

When installing Identity Reporting, consider the following prerequisites and considerations:

- Requires a supported and configured version of the following Identity Manager components:
  - Identity applications, including the User Application driver
  - Sentinel installed on a separate Linux computer.
  - Driver for Data Collection Service
  - Driver for the Managed System Gateway service

  For more information about required versions and patches for these components, see the latest Release Notes. For more information about installing the drivers, see Chapter 15, “Managing the Drivers for Reporting,” on page 201.
- Do not install Identity Reporting on a server in a clustered environment.
- If you want to use the database other than local database, you should create a database on a different server and specify the details during Identity Reporting installation.
- (Conditional) To run reports against an Oracle 12c database, you must install the appropriate JDBC file. For more information, see “Running Reports on an Oracle Database” on page 199.
- (Conditional) You can use your own Tomcat installation program instead of the one provided in the Identity Manager installation kit. However, to use the Apache Log4j service with your version of Tomcat, ensure that you have the appropriate files installed. For more information, see “Using the Apache Log4j Service to Log Sign-on” on page 98.
- Assign the Report Administrator role to any users that you want to access reporting functionality.
- Ensure that all servers in your Identity Manager environment are set to the same time. If you do not synchronize the time on your servers, some reports might be empty when executed. For example, this issue can affect data related to new users when the servers hosting the Identity Manager engine and the Warehouse have different time stamps. If you create and then modify a user, the reports are populated with data.
- The installation process modifies JAVA_OPTs or CATALINA_OPTS entries for JRE mapping in the `setenv.bat` file for Tomcat.

  By default, the convenience installer for Tomcat places the `setenv.bat` file in the `C:\NetIQ\idm\apps\tomcat\bin` directory. The installer also configures the JRE location in the file.

Identifying Audit Events for Identity Reporting

This section provides information on how to identify different audit events required for Identity Manager reports and custom reports. You can unzip all report sources and run the following script to identify the audit events:

```
find . -name *.jrxml -print0 |xargs -0 grep -H "'000[B3]" | perl -ne
'($file) = /^\.\/(.*?)\//;@a = /000[3B]..../g; foreach $a (@a) { print
"$file;$a\n"}' |sort -u
```

The following section provides information on how to identify and select various audit events for identity Manager reports and custom reports:

Event Name	Audit Flag
Authentication and Password Change	**Selecting Audit Flag using SSPR:** Launch **SSPR Configuration Editor** > **Audit Configuration** > Select from the following audit flags: ◆ Authenticate ◆ Change Password ◆ Unlock Password ◆ Recover Password ◆ Intruder Attempt ◆ Intruder Lock ◆ Intruder Lock User **Selecting Audit Flag using iManager:** Go to **iManager Roles and Tasks** > **eDirectory Auditing** > > **Audit Configuration** > **Novell Audit** > Select from the following audit flags: ◆ Change Password ◆ Verify Password ◆ Login ◆ Logout
All other reporting events	Go to **NetIQ Identity Manager UserApp** > **Administration** > **Logging** > **Enable audit service**

13 Installing Identity Reporting

This section describes the process for installing Identity Reporting.

Using the Guided Process to Install Identity Reporting

The following procedure describes how to install Identity Reporting using an installation wizard. To perform a silent, unattended installation, see "Installing Identity Reporting Silently" on page 194.

1 Log in to the computer where you want to install Identity Reporting.

2 Stop Tomcat.

3 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the installation files for Identity Reporting, located by default in the `\products\Reporting` directory.

4 (Conditional) If you downloaded Identity Reporting installation files from the NetIQ Downloads website, complete the following steps:

 4a Navigate to the `.tgz` file for the downloaded image.

 4b Extract the contents of the file to a folder on the local computer.

5 From the directory that contains the installation files, run the `rpt-install-win.exe` file.

6 In the installation program, specify the language that you want to use for installation, and then click **OK**.

7 Review the Introduction text and click **Next**.

8 Accept the license agreement and click **Next**.

9 Complete the guided process, using the following parameters:

- **Installation Folder**

  Specifies the path to a directory where the installation program creates the application files, including installation log files, helper scripts, and configuration scripts.

- **Reporting Setup**

  Represents the environment and its settings to which you want to add Identity Reporting. For **Identity Manager**, specify the following values:

  Identity Vault Server

  Specifies the hostname to the eDirectory server.

Secure LDAP Port

Specifies the port you want to use to establish an LDAP connection to the eDirectory server over SSL. The default port is 636.

Provisioning Home

Specifies the Identity Manager provisioning home location. This can be the full application server URL or a relative path for the URL.

- **Application Server Details**

  Represents Tomcat that you want to run Identity Reporting. The application server must already be installed.

  Secondary

  Specifies whether the current install is on a secondary node of a cluster.

  Tomcat root folder

  Specifies a path to the Tomcat instance. For example, `C:\NetIQ\idm\apps\tomcat`.

  Java JRE Base folder

  Specifies the Java JRE base folder location.

  The path contains the config update utility file and is used to launch this utility after Identity Reporting is installed.

- **Application Address**

  Represents the settings for the server that hosts Identity Reporting.

  Protocol

  Specifies whether you want to use *http* or *https*. To use SSL for communication, specify `https`.

  Host name

  Specifies the DNS name or IP address of Tomcat. Do not use `localhost`.

  Port

  Specifies the port that you want Tomcat to use for communication with the Identity Reporting application.

  Connect to an external authentication server

  Specifies whether a different instance of Tomcat hosts the authentication server (OSP). The authentication server contains the list of users who can log in to Identity Reporting.

  If you select this setting, specify values for the authentication server's **Protocol**, **Host name**, and **Port**.

- **Authentication Server Details**

  Specifies the password for the Identity Reporting Service.

  Identity Manager uses this password to connect to the OSP client on the authentication server.

- **Database Details**

  Represents the settings for the reporting database, including whether you want the installation process to create the database or generate an SQL file for creating the database later.

Database name

Specify the database name as per your requirement:

- In case of a new installation, specify the name of your Reporting database. For example, `idmrptdb` or `SIEM`.
- If you are migrating from EAS, specify the name for the EAS database, for example, `SIEM`.

Database host

Specify the database host as per your requirement:

- In case of a new installation, specify the DNS name or IP address of the server where the database has to be created.
- If you are migrating from EAS, specify the DNS name or IP address of the server that hosts your `SIEM` database.

Database type

Select the database that you want to use.

If you select **Oracle**, specify the following details:

- **JDBC driver jar**

  Specifies the path to the jar file for the Oracle JDBC driver. For example, `C:\oracle\ojdbc7.jar`.

  For more information, see "Running Reports on an Oracle Database" on page 199.
- **JDBC driver classname**

  Specifies the class of the JDBC driver.
- **JDBC driver type**

  Specifies the type of JDBC driver.

If you select **PostgresSQL**, click **Next**.

Share password

Enables you to specify a single password for all reporting users when they connect to the database.

Specify password for each user

Enables you to specify a unique password for each reporting user to the database. You need to specify a password for `idm_rpt_data_password`, `idm_rpt_cfg_password`, and `idmrptuserpassword`.

Database port

Specifies the port to connect to the database.The default port is 5432.

Configure database now or at startup

Indicates that you have the login settings for the database so the installation program can create the database immediately or during reporting startup. You must also specify the following values:

- **DBA userid**

  Specifies the name of the administrative account for the SIEM database server. For example, *postgres.*

- **DBA password**

  Specifies the password for the administrative account for the database.

- **Test Database Connection:** Indicates whether you want the installation program to test the values specified for the database.

  The installation program attempts the connection when you click **Next** or press **Enter**.

  NOTE: You can continue with installation if the database connection fails. However, after installation, you must manually create the tables and connect to the database. For more information, see "Manually Generating the Database Schema" on page 195.

Generate SQL for later

Instructs the installation program to generate a SQL file that your database administrator will use to create the database after your complete the installation process. To create the database after installation, see "Manually Generating the Database Schema" on page 195.

- **Default Language**

  Specifies the language that you want Identity Reporting to use in searches.

- **Identity Vault Credentials**

  Represents the settings that Identity Reporting uses to connect to the Identity Vault.

  Identity Vault Administrator

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

  Identity Vault Administrator Password

  Specifies the password for the Identity Vault administrator.

  Keystore Path

  Specifies the full path to your keystore (`cacerts`) file of the JRE that Tomcat uses to run.

  Keystore Password

  Specifies the password for the keystore file.

  Report Admin Role Container DN

  Specify the DN for the container that stores the Report Administrator role.

  Report Admin User DN

  Specifies an existing user account in the Identity Vault that has the rights to perform administrative tasks for Identity Reporting.

- **User Application driver**

  Represents the name of your application driver, driver set, and driver set container.

  User Application Driver

  Specifies the name of the User Application driver.

  Driver set name

  Specifies the name of the driver set.

Driver set container

Specifies the name of the driver set container.

- **Email Delivery**

  Represents the settings for the SMTP server that sends report notifications. To modify these settings after installation, use the RBPM Configuration utility.

  Default email address

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

  SMTP server

  Specifies the IP address or DNS name of the SMTP email host that Identity Reporting uses for notifications. Do not use `localhost`.

  SMTP server port

  Specifies the port number for the SMTP server. The default port is 465.

  Use SSL for SMTP

  Specifies whether you want to use SSL protocol for communication with the SMTP server.

  Require server authentication

  Specifies whether you want to use authentication for communication with the SMTP server. You must also specify the following values:

  - ***SMTP user name***

    Specifies the name of an login account for the SMTP server.

  - ***SMTP password***

    Specifies the password of a login account for the SMTP server.

- **Report Details**

  Represents the settings for report definitions and completed reports.

  Keep finished reports for

  Specifies the amount of time that Identity Reporting will retain completed reports before deleting them.

  For example, to specify six months, enter 6 and then select **Month**.

  Location of report definitions

  Specifies a path where you want to store the report definitions.

  For example, `C:\NetIQ\idm\apps\IdentityReporting`.

10 In the Pre-Installation Summary window, click **Install**.

Installing Identity Reporting Silently

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, the system uses information from a `.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process. To perform a guided installation, see "Using the Guided Process to Install Identity Reporting" on page 189.

1 (Conditional) To avoid specifying the administrator passwords for the installation in the `.properties` file for a silent installation, use the `export` or `set` command. For example: `set NOVL_ADMIN_PWD=`*`myPassWord`*

The silent installation process reads the passwords from the environment, rather than from the `.properties` file.

Specify the following passwords:

NOVL_DB_RPT_USER_PASSWORD

Specifies the password for the administrator for the SIEM database.

NOVL_IDM_SRV_PWD

Specifies the password for the owner of the database schemas and objects for reporting.

NOVL_IDM_USER_PWD

Specifies the password for the idmrptuser that has read-only access to reporting data.

NOVL_ADMIN_PWD

(Conditional) To enable subcontainer searches at login time, specifies the password of an LDAP administrator.

NOVL_SMTP_PASSWORD

(Conditional) To use authentication for email communications, specifies the password for the default SMTP email user.

2 To specify the installation parameters, complete the following steps:

2a Ensure that the `.properties` file is located in the same directory as the execution file for installation.

For your convenience, NetIQ provides two `.properties` files, located by default in the `products\Reporting` directory of the `.iso` image:

- `rpt_installonly.properties` to use the default installation settings
- `rpt_configonly.properties` to customize the installation settings

2b In a text editor, open the `.properties` file.

2c Specify the parameter values. For a description of the parameters, see Step 9 on page 189.

NOTE: The `.properties` file for installing Standard Edition includes only the parameters required for that version.

2d Save and close the file.

3 To launch the installation process, enter the following command:

```
rpt-install.exe -i silent -f path_to_properties_file
```

NOTE: If the `.properties` file resides in a different directory from the installation script, you must specify the full path to the file. The script unpacks the necessary files to a temporary directory and then launches the silent installation.

Manually Generating the Database Schema

You can recreate the database tables after installation without having to reinstall. This section helps you create the database schema.

1. Stop Tomcat by using the `services.msc` file.
2. (Conditional) Create a new database.

   If your database is running on a separate server, you must connect to that database server. For a remotely installed PostgreSQL database, verify that the database server is running. To connect to a remote PostgreSQL database, see "Connecting to a Remote PostgreSQL Database" on page 196. If you are connecting to an Oracle database, ensure that you have created an Oracle database instance in that database server. For more information, see Oracle documentation.
3. Add the required roles to the database using the following SQLs from `C:\NetIQ\idm\apps\IdentityReporting\sql`.
   - **PostgreSQL:** `create_dcs_roles_and_schemas.sql` and `create_rpt_roles_and_schemas.sql`
   - **Oracle:** `create_dcs_roles_and_schemas-orcale.sql` and `create_rpt_roles_and_schemas-orcale.sql`
4. To create IDM_RPT_DATA, IDM_RPT_CFG and IDMRPTUSER roles, perform the following actions:
   - **PostgreSQL:** Run the following commands in the given order:

     ```
     Select CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>');
     ```

     ```
     Select CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>',
     '<Set pwd for IDMRPTUSER>');
     ```
   - **Oracle:** Run the following commands in the given order:

     ```
     begin
     CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>');
     end;

     begin
     CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>', '<Set pwd
     for IDMRPTUSER>');
     end;
     ```
5. Add get_formatted_user_dn function to the IDM_RPT_DATA schema.

   5a Log in to the database as a database admin user.

   5b Add get_formatted dn function from `C:\NetIQ\idm\apps\IdentityReporting\sql`.

   Locate `get_formatted_user_dn.sql` for PostgreSQL and `get_formatted_user_dn-oracle.sql` for Oracle.

6 Clear the database checksums for the following `.sql` files located 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`

6a Append the following line at the beginning of each SQL:

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

The modified content should look similar to the following:

```
--
*******************************************************************
**
-- Update Database Script
--
*******************************************************************
**
-- Change Log: IdmDcsDataDropViews.xml
-- Ran at: 2/23/18 5:17 PM
-- Against: IDM_RPT_CFG@jdbc:oracle:thin:@192.99.170.20:1521/orcl
-- Liquibase version: 3.5.1
--
*******************************************************************
**
update databasechangelog set md5sum = null;
```

6b Run each SQL with the corresponding user.

7 Commit the changes to the database.

8 Start Tomcat by using the `services.msc` file.

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 remoteTCP/IP connection, add the following entry to the `C:\NetIQ\idm\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\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.

14 Configuring Identity Reporting

After installing Identity Reporting, you can still modify many of the installation properties by running the `configupdate.bat` 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.

Running Reports on an Oracle Database

Identity Reporting provides the ability to run reports against remote Oracle databases. However, you must add an Oracle JDBC file to the library for your application server.

1. Download the `ojdbc7.jar` file from the Oracle website.
2. Copy the file to the appropriate location for Tomcat server (`common/lib` directory in the *`tomcat_lib`*.).

For more information about supported Oracle databases, see the NetIQ Identity Manager Technical Information website (https://www.netiq.com/products/identity-manager/advanced/technical-information/).

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` is automatically deployed when Identity Reporting is installed.

While working in a staging or production environment, manually delete the `rptdoc war` files and folders from your environment on Tomcat.

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 remoteTCP/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.

15 Managing the Drivers for Reporting

Identity Reporting requires the following drivers:

- Identity Manager Managed System Gateway Driver
- Identity Manager Data Collection Service Driver

You can use the package management tools provided with Designer to install and configure the drivers. This process includes the following activities:

- "Configuring Drivers for Identity Reporting" on page 201
- "Deploying and Starting Drivers for Identity Reporting" on page 207
- "Configuring the Runtime Environment" on page 212
- "Setting Auditing Flags for the Drivers" on page 220

Configuring Drivers for Identity Reporting

This section helps you install and configure the Managed System Gateway and Data Collection Service drivers for Identity Reporting.

NOTE: This section assumes that you have already installed and configured the User Application and Role and Resource Service drivers for Identity Applications. For more information, see "Creating and Deploying the Drivers for the Identity Applications" on page 147.

- "Installing the Driver Packages for Identity Reporting" on page 201
- "Configuring the Managed System Gateway Driver" on page 202
- "Configuring the Driver for Data Collection Service" on page 203
- "Configuring Identity Reporting to Collect Data from the Identity Applications" on page 206

Installing the Driver Packages for Identity Reporting

Before you attempt to configure the drivers, you must have all of the necessary packages for the drivers in the Package Catalog. When you create a new Identity Manager project in Designer, the user interface automatically prompts you to import several packages into the new project. You do not need to import the packages during installation but you must install them at some point for Identity Reporting to function appropriately.

1 Open your project in Designer.

2 Select **Package Catalog > Import Package**.

3 In the Select Package dialog box, click **Select All**, and then click **OK**.

Designer adds several new package folders under the **Package Catalog**. These package folders correspond to the objects in the palette on the right side of the Modeler view in Designer.

4 Click **Save**.

Configuring the Managed System Gateway Driver

1 Open your project in Designer.

2 In the palette of the **Modeler** view, select **Service > Managed System Gateway**.

3 Drag the icon for **Managed System Gateway** onto the **Modeler** view.

4 In the Driver Configuration Wizard, select **Managed System Gateway Base**, and then click **Next**.

5 In the Select Mandatory Features window, select the mandatory features, and then click **Next**.

6 (Conditional) If the application prompts you for an additional package called **Advanced Java Class**, select the package and then click **OK**.

7 (Optional) Specify the name that you want to use for the driver.

8 Click **Next**.

9 For Connection Parameters, specify the values that Identity Reporting uses to request data from the driver.

When you specify more than one IP address, you continue to use the same port number to listen on all the interfaces. For example, if you specify `192.168.0.1,127.0.0.1` for the address and `9000` for the port, then the driver uses the following settings:

```
192.168.0.1:9000
127.0.0.1:9000
```

10 (Optional) To enable end-point tracing, select **true** and then specify a location for the trace file.

11 Click **Next**.

12 (Optional) To connect the driver to a remote loader, complete the following steps:

12a In the Remote Loader window, select **yes**.

12b Specify the settings for the remote loader that you want to use.

13 Click **Next**.

14 Review the information in the Confirm Installation Tasks window, and then click **Finish**.

15 (Optional) To configure additional settings for the driver, complete the following steps in the Modeler view:

15a Right-click the line connecting the Managed System Gateway Driver to the driver set, and then click **Properties**.

15b In the Properties dialog box, select **Driver Configuration > Startup Option**.

15c Select **Manual** for the startup option, and then click **Apply**.

15d Select the **Driver Parameters** tab.

15e (Optional) In the **Driver Options** tab, modify the settings for the driver, connections, and end-point tracing.

You might need to select **show** under **Connection Parameters** and **Driver Parameters** to display the settings.

15f (Optional) To have the driver send periodic status messages on the Publisher channel, click the **Publisher Options** tab, and then specify a value in minutes for **Publisher heartbeat interval**.

If no traffic occurs on the Publisher channel within the specified interval, the driver sends a new heartbeat.

15g Click **Apply**.

16 (Optional) To specify global configuration values for the server, complete the following steps:

16a In the navigation pane, select **GCVs**.

16b Specify global configuration values, such as the following:

Query Managed Systems across driversets

Defines the scope of operation for the Managed System Gateway Driver. If set to **true**, the driver returns information about managed systems across driversets. Otherwise, the scope is restricted to the local driverset.

Add end-point request data to queries

Specifies whether end-point request data be added to the queries sent by the driver. This will be added as an `operation-data` node.

End-point request data node name

Specifies a node-name that will be added to the `operation-data` of the queries. The node attributes will contain the details about the request.

16c Click **Apply**.

17 (Optional) To review the packages that have been installed, click **Packages** in the navigation pane.

You do not need to change the **Operation** settings unless you want to uninstall a particular package.

18 Click **OK**.

19 Enable the Subscriber channel for Identity Reporting to function correctly.

Configuring the Driver for Data Collection Service

1 Open your project in Designer.

2 In the palette of the **Modeler** view, select **Service > Data Collection Service**.

3 Drag the icon for **Data Collection Service** onto the **Modeler** view.

4 In the Driver Configuration Wizard, select **Data Collection Service Base**, and then click **Next**.

5 In the Select Mandatory Features window, select the mandatory features, and then click **Next**.

6 Select the optional features that you want to apply, and then click **Next**.

7 (Conditional) If the application prompts you for an additional package called **LDAP Library**, complete the following steps:

7a Select the package, and then click **OK**.

7b (Optional) To configure a global connection profile for all drivers, on the Install LDAP Library page, select **Yes**.

8 Click **Next**.

9 (Optional) Specify the name that you want to use for the driver.

10 Click **Next**.

11 For Connection Parameters, specify the values that Identity Reporting uses to request data from the driver.

For example, specify the user and password of the Reporting Administrator for authentication.

When you specify more than one IP address, you continue to use the same port number to listen on all the interfaces. For example, if you specify `192.168.0.1,127.0.0.1` for the address and `9000` for the port, then the driver uses the following settings:

```
192.168.0.1:9000
127.0.0.1:9000
```

12 Click **Next**.

13 For **Identity Vault Registration**, specify the settings for the Identity Vault.

You must specify an IP address. Do not specify an address of localhost for the Identity Vault Registration.

14 (Optional) To register the Managed System Gateway driver, complete the following steps:

14a For **Managed System Gateway Registration**, click **yes**.

14b Specify the DN for the driver, as well as the user and password for the LDAP administrator.

NOTE: Because the driver has not yet been deployed, the browse function does not show the Managed System Gateway driver you just configured, so you might need to type the DN for the driver.

15 Click **Next**.

16 (Optional) To connect the driver to a remote loader, complete the following steps:

16a In the Remote Loader window, select **yes**.

16b Specify the settings for the remote loader that you want to use.

17 Click **Next**.

18 For **Scoping Configuration**, specify the role for the Data Service Collection driver.

19 Review the information in the Confirm Installation Tasks window, and then click **Finish**.

20 (Optional) To configure additional settings for the driver, complete the following steps in the Modeler view:

20a Right-click the line connecting the Data Collection Service driver to the driver set, and then click **Properties**.

20b In the Properties dialog box, select **Driver Configuration > Startup Option**.

20c Select **Manual** for the startup option, and then click **Apply**.

20d Select the **Driver Parameters** tab.

In environments where the driver receives large numbers of events, NetIQ recommends setting the number of batches per file to no more than 5. If you set this parameter to a value greater than 5, the driver cannot process events efficiently.

20e (Optional) In the **Driver Options** tab, modify the settings for the driver, connections, and registration.

In a test environment, you might want to use low numbers to be sure your events are processed correctly. However, in a production environment, you probably want to use higher numbers so that the system does not process events unnecessarily.

IP Address

Specifies the IP address of the server that hosts Identity Reporting.

Port

Specifies the port number that Identity Reporting uses for REST connections.

Protocol

Specifies the protocol for accessing Identity Reporting. If you select HTTPS, you must also indicate whether you want to trust the server's certificate.

Name

Specifies the name that you want to use to refer to your Identity Vault within Identity Reporting.

Description

Specifies a short description of the Identity Vault.

Address

Specifies the IP address of the Identity Vault.

For example, `192.168.0.1`

NOTE: You must specify an IP address. Do not specify an address of "localhost" for the Identity Vault Registration.

Register Managed System Gateway

Specifies whether you want to register the Managed System Gateway Driver.

Managed System Gateway Driver DN (LDAP)

Specifies the DN of the Managed System Gateway Driver in slash format.

Managed System Gateway Driver Configuration Mode

Specifies whether the driver is configured locally or is remote.

User DN (LDAP)

Specifies the LDAP DN of the user that the driver should use to authenticate to the Managed System Gateway Driver. This DN must exist in the Identity Vault.

Password

Specifies the password for the user.

Time interval between submitting events

The maximum amount of time, in minutes, that an event can remain in the persistence layer before being submitted to the DCS (and to the database for Identity Reporting).

20f (Conditional) To collect data from the identity applications, specify the values for **SSO Service Support**. For more information, see "Configuring Identity Reporting to Collect Data from the Identity Applications" on page 206.

20g Click **Apply**.

21 To configure DNs, complete the following steps:

  21a In the navigation menu, select **Engine Control Values**.

  21b For the **Qualified form for DN-syntax attribute values** setting, select **True**.

  21c Click **Apply**.

22 (Optional) To specify global configuration values for the server, complete the following steps:

  22a In the navigation pane, select **GCVs**.

  22b For **Show override options**, select **Show**.

  22c Modify the settings to override the global configuration values.

  22d Click **Apply**.

23 Click **OK**.

Configuring Identity Reporting to Collect Data from the Identity Applications

For Identity Reporting to collect data from the identity applications, you must configure the DCS driver to support the single sign-on process.

1 Open your project in Designer.

2 In the **Outline** view, right-click the Data Collection Service driver, then click **Properties**.

3 Click **Driver Configuration > Driver Parameters**.

4 Click **Show connection parameters > show**.

5 Click **SSO Service Support > Yes**.

6 Specify the parameters for single sign-on functionality:

SSO Service Address

Required

Specifies the relative URL of the authentication server that issues tokens to OSP. For example, `10.10.10.48`.

This value must match the value that you specified in the RBPM configuration utility for **OSP server host identifier**. For more information, see “Authentication Server” on page 175.

SSO Service Port

Required

Specifies the port for the authentication server. The default value is 8180.

This value must match the value that you specified in the RBPM configuration utility for **OSP server TCP port**. For more information, see “Authentication Server” on page 175.

SSO Service Client ID

Required

Specifies the name that you want to use to identify the single sign-on client for the DCS driver to the authentication server. The default value is `dcsdrv`.

This value must match the value that you specified in the RBPM configuration utility for **OSP client ID**. For more information, see “Reporting” on page 180.

SSO Service Client Secret

Required

Specifies the password for the single sign-on client for the DCS driver.

This value must match the value that you specified in the RBPM configuration utility for **OSP client secret**. For more information, see "Reporting" on page 180.

Protocol

Specifies whether the service client uses the `http` (non-secure) or `https` (secure) protocol when communicating with the authentication server.

7. Click **Apply**, then click **OK**.
8. (Conditional) If you changed these settings after deploying the driver, you must deploy and restart the driver. For more information, see "Deploying and Starting Drivers for Identity Reporting" on page 207.
9. Repeat this procedure for each DCS driver in your environment.

Deploying and Starting Drivers for Identity Reporting

Identity Reporting requires the following drivers:

- Identity Manager Managed System Gateway Driver
- Identity Manager Driver for Data Collection Service

This process includes the following activities:

- "Deploying the Drivers" on page 207
- "Verifying that the Managed Systems are Working" on page 208
- "Starting the Drivers for Identity Reporting" on page 210

For more information about installing and configuring these drivers, see "Configuring Drivers for Identity Reporting" on page 201.

Deploying the Drivers

You must deploy the two drivers for Identity Reporting.

1. Open your project in Designer.
2. In the **Modeler** or **Outline** view, right-click the driver set that you want to deploy.
3. Select **Live** > **Deploy**.
4. Specify the Identity Vault credentials for the selected driver.

Verifying that the Managed Systems are Working

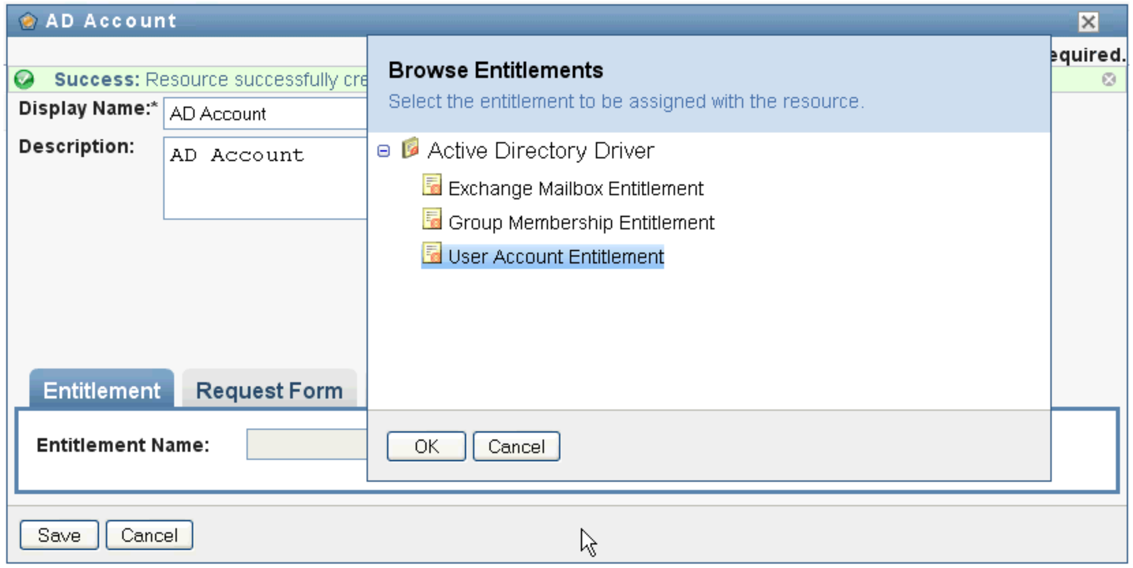
Before you start the Managed System Gateway Driver and the Data Collection Service Driver, you should confirm that the underlying managed systems are properly configured. This process helps you isolate problems with your environment that do not relate to the configuration of the reporting drivers.

To troubleshoot your Active Directory environment, for example, you might want to test an Active Directory entitlement by assigning a resource in the User Application.

NOTE: For more information about the Active Directory driver, see the *NetIQ Identity Manager Driver for Active Directory Implementation Guide*.

The following steps demonstrate one way to confirm that Active Directory is properly configured:

1. Ensure that the User Application and Identity Reporting are both running on the same server.
2. In iManager, verify that the User Application Driver and the Role and Resource Service Driver are running, then ensure that the driver for the managed system is running.
3. To verify that the User Application can retrieve information from Active Directory, log in to the User Application as a User Application Administrator.
4. In the Resource Catalog, create a new resource for Active Directory accounts:
5. Bind the resource to an entitlement within the Active Directory Driver, such as **User Account Entitlement**.



AD Account

Success: Resource successfully cre

equired.

Display Name:* AD Account

Description: AD Account

Browse Entitlements

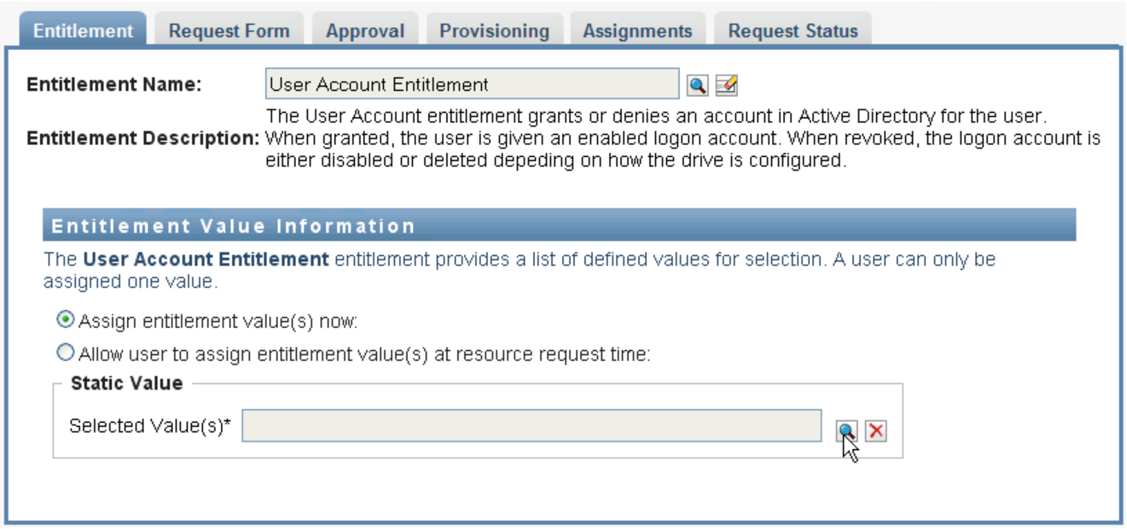
Select the entitlement to be assigned with the resource.

- Active Directory Driver
  - Exchange Mailbox Entitlement
  - Group Membership Entitlement
  - User Account Entitlement

Entitlement Name:

The User Application can retrieve the entitlement from the driver.

6. Because this particular resource pertains to accounts, configure the resource to assign an account value.



Entitlement Name: User Account Entitlement

Entitlement Description: The User Account entitlement grants or denies an account in Active Directory for the user. When granted, the user is given an enabled logon account. When revoked, the logon account is either disabled or deleted depeding on how the drive is configured.

Entitlement Value Information

The **User Account Entitlement** entitlement provides a list of defined values for selection. A user can only be assigned one value.

● Assign entitlement value(s) now:

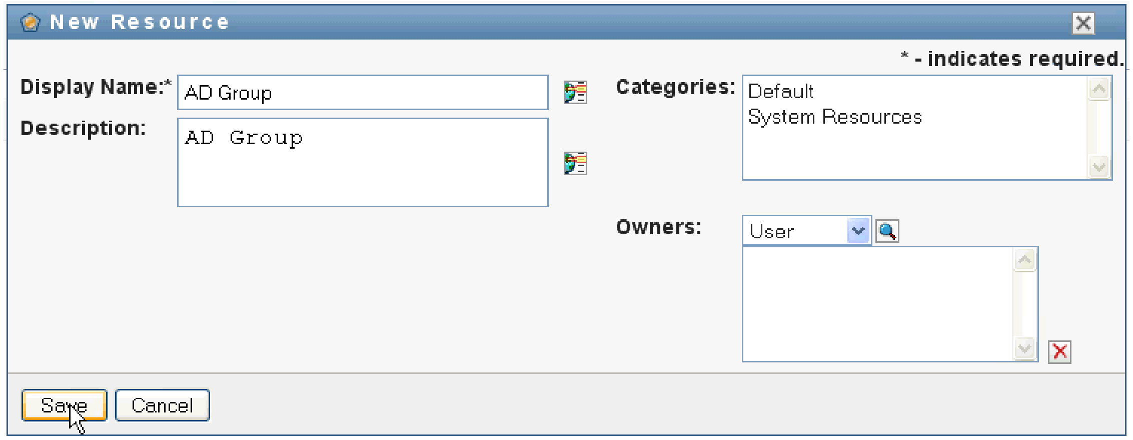
○ Allow user to assign entitlement value(s) at resource request time:

Static Value

Selected Value(s)*

7 Select the account value, and then click **Add**.

8 Create another resource that assigns groups.



* - indicates required.

Display Name:* AD Group

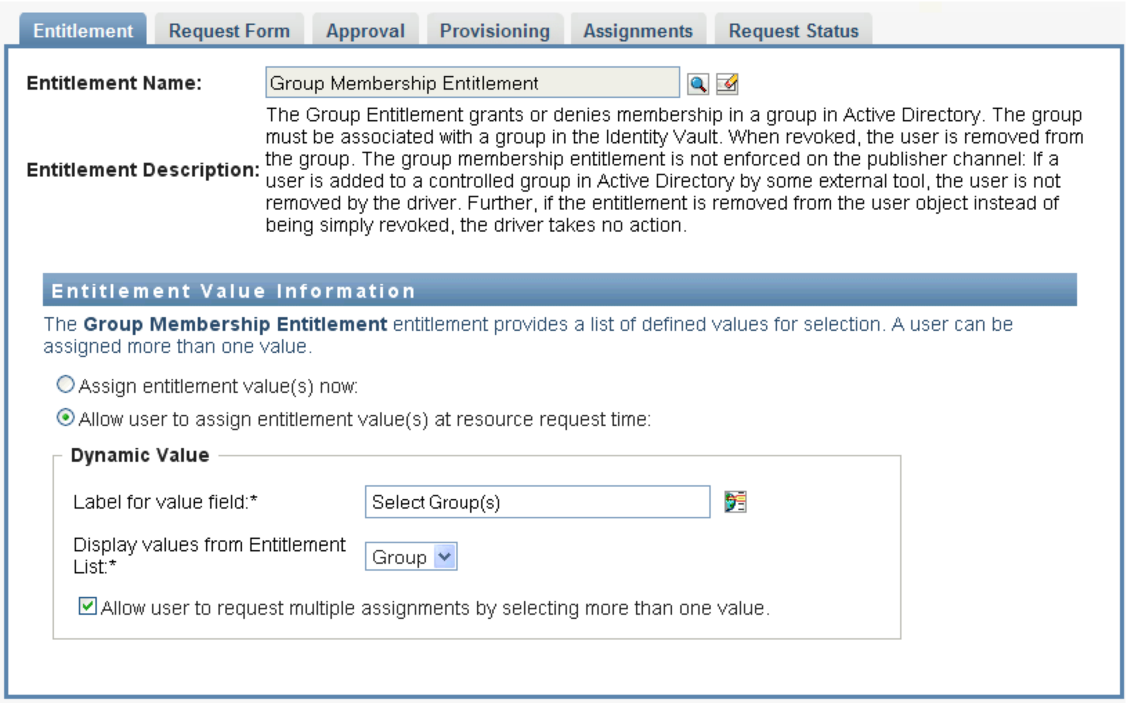
Description: AD Group

Categories: Default
System Resources

Owners: User

9 Bind the resource to an entitlement that is suitable for groups. For this particular resource, map to the **Group Membership Entitlement**.

10 Configure this resource so that the user assigns the entitlement value at request time, and allow the user to select multiple values for a single assignment request.



Entitlement Name: Group Membership Entitlement

Entitlement Description: The Group Entitlement grants or denies membership in a group in Active Directory. The group must be associated with a group in the Identity Vault. When revoked, the user is removed from the group. The group membership entitlement is not enforced on the publisher channel: If a user is added to a controlled group in Active Directory by some external tool, the user is not removed by the driver. Further, if the entitlement is removed from the user object instead of being simply revoked, the driver takes no action.

Entitlement Value Information

The **Group Membership Entitlement** entitlement provides a list of defined values for selection. A user can be assigned more than one value.

○ Assign entitlement value(s) now:

● Allow user to assign entitlement value(s) at resource request time:

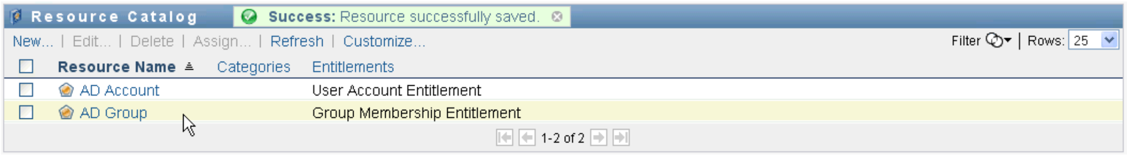
Dynamic Value

Label for value field:* Select Group(s)

Display values from Entitlement List:* Group

☑ Allow user to request multiple assignments by selecting more than one value.

11 Verify that the entitlements were created successfully.


Resource Catalog
New... | Edit... | Delete | Assign... | Refresh | Customize...
Filter | Rows: 25
1-2 of 2

Success: Resource successfully saved.

Resource Name	Categories	Entitlements
AD Account		User Account Entitlement
AD Group		Group Membership Entitlement

At this point, you can see that the underlying architecture for the managed system (in this case, Active Directory) is functioning properly. This can help you to troubleshoot any problems that might arise later on.

Starting the Drivers for Identity Reporting

This section provides instructions for starting the Managed System Gateway Driver and the Data Collection Service Driver.

1 Open iManager.

2 Right-click the Managed System Gateway Driver, and then click **Start driver**.

3 Right-click the Data Collection Service Driver, and then click **Start driver**.

4 After the drivers have started, verify that the console displays additional information in the server console. For example:

```
21:22:56,399 INFO  [LogEvent] [DCS_Driver_Registration_Add] DCS Driver DN
TREE\novell\TestDrivers\Data Collection Service Driver; DCS-Report Driver
d44571a5708446bad65832481bb401d
```

5 Log in to Identity Reporting as a Reporting Administrator.

6 In the navigation pane on the left, click **Overview**.

7 Verify that the **Configuration** section reports that an Identity Vault has been configured.

8 In the navigation pane, click **Identity Vaults**.

9 Verify that the Identity Vault page provides details about the Data Collection Service Driver and the Managed System Gateway Driver. The Managed System Gateway Driver status should indicate that the driver has been initialized.

At this point, you can look at the contents of the Identity Information Warehouse to learn more about the rich data that is stored about the Identity Vault, as well as the managed systems in your enterprise.

10 To see the data in the Identity Information Warehouse, use a database administration tool such as PGAdmin for PostgreSQL to look at the contents of the SIEM database. When you look at the SIEM database, you should see the following schemas:

idm_rpt_cfg

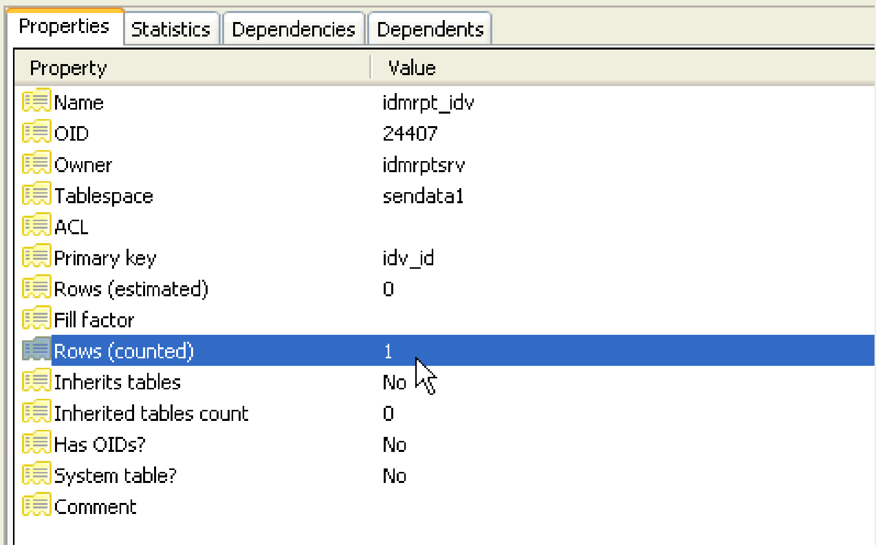
Contains reporting configuration data, such as report definitions and schedules. The installation program for Identity Reporting adds this schema to the database.

idm_rpt_data

Contains information collected by the Managed System Gateway Driver and the Data Collection Service Driver. The installation program for Identity Reporting adds this schema to the database.

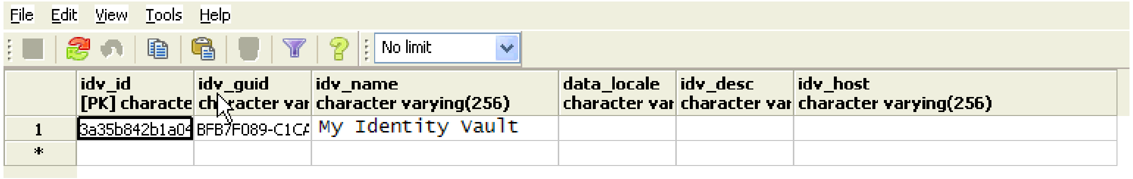
11 To view data collected by the drivers, expand **idm_rpt_data > Tables > idmrpt_idv**.

12 Verify that a single row was added to this table for the new Data Collection Service Driver:



Property	Value
Name	idmrpt_idv
OID	24407
Owner	idmrptsrv
Tablespace	sendata1
ACL	
Primary key	idv_id
Rows (estimated)	0
Fill factor	
Rows (counted)	1
Inherits tables	No
Inherited tables count	0
Has OIDs?	No
System table?	No
Comment	

13 Verify that the data for this table shows the name of the Identity Vault:



	idv_id [PK] characte	idv_guid character var	idv_name character varying(256)	data_locale character var	idv_desc character var	idv_host character varying(256)
1	3a35b842b1a04	BFB7F089-C1CA	My Identity Vault			
*						

If you see the new row in this table, the driver registration process was successful.

Configuring the Runtime Environment

This section provides some additional configuration steps you should take 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 212
- "Migrating the Data Collection Service Driver" on page 213
- "Adding Support for Custom Attributes and Objects" on page 215
- "Adding Support for Multiple Driver Sets" on page 218
- "Configuring the Drivers to Run in Remote Mode with SSL" on page 219

If you have problems with one or more drivers that are difficult to understand, see Troubleshooting in the Administrator Guide to NetIQ Identity Reporting.

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 your project does not already include a Data Collection Service driver, import the driver into your project. For more information, see "Creating and Deploying the Drivers for the Identity Applications" on page 147.

4 (Conditional) If you have not already upgraded your DCS driver to the supported patch version, complete the following steps:

4a Download the latest DCS driver patch file.

4b Extract the patch file to a location on your server.

4c 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
change this
```

4d Restart eDirectory.

4e 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. For more information about software requirements, see the "Prerequisites for Installing the Identity Reporting Components" on page 187.

4f Redeploy and restart the DCS driver in Designer.

5 In the **Outline** view, right-click the DCS driver, then select **Properties**.

6 Click **Driver Configuration**.

7 Click the **Driver Parameters** tab.

8 Click **Show connection parameters**, then select **show**.

9 Click **SSO Service Support**, then select **Yes**.

10 Specify the IP address and port for the Reporting Module.

11 Specify a password for the SSO Service Client. The default password is `driver`.

12 Click **Apply**, then click **OK**.

13 In the **Modeler** view, right-click the DCS driver, then select **Driver > Deploy**.

14 Click **Deploy**.

15 If prompted to restart the DCS driver, click **Yes**.

16 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 the iManager.

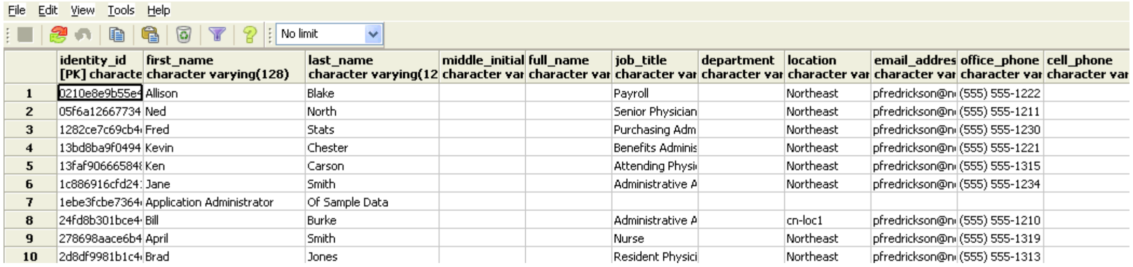
2 In the **Overview** panel for the Data Collection Service Driver, select **Migrate From Identity Vault**.

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.

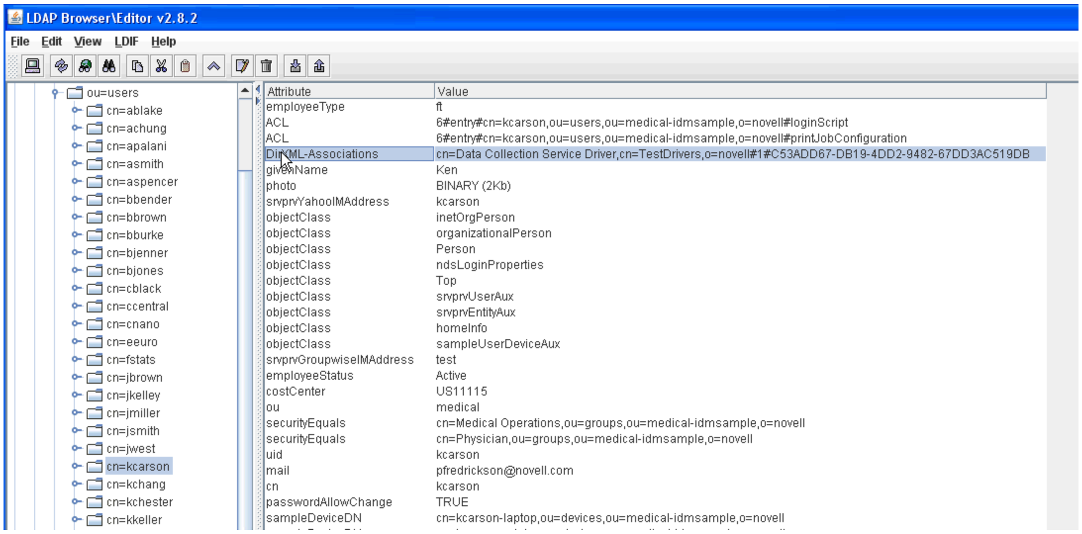
5 In the **idmrpt_identity** and **idmrpt_acct** tables, which provide information about the identities and accounts in the Identity Vault, ensure they contain the following type of information:



	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	Allison	Blake			Payroll		Northeast	pfredrickson@n	(555) 555-1222	
2	05f6a12667734	Ned	North			Senior Physician		Northeast	pfredrickson@n	(555) 555-1211	
3	1282ce7c69cb4	Fred	Stats			Purchasing Adm		Northeast	pfredrickson@n	(555) 555-1230	
4	13bd8ba9f0494	Kevin	Chester			Benefits Adminis		Northeast	pfredrickson@n	(555) 555-1221	
5	13faf90666584	Ken	Carson			Attending Physi		Northeast	pfredrickson@n	(555) 555-1315	
6	1c886916cfd24	Jane	Smith			Administrative A		Northeast	pfredrickson@n	(555) 555-1234	
7	1ebe3fcbe7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative A		cn-loc1	pfredrickson@n	(555) 555-1210	
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@n	(555) 555-1319	
10	2d8df9981b1c4	Brad	Jones			Resident Physici		Northeast	pfredrickson@n	(555) 555-1313	

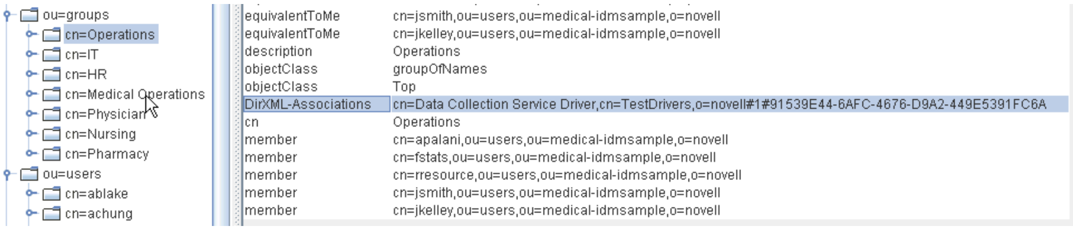
6 In the LDAP browser, verify that the migration process adds the following references for DirXML-Associations:

- For each user, verify the following type of information:



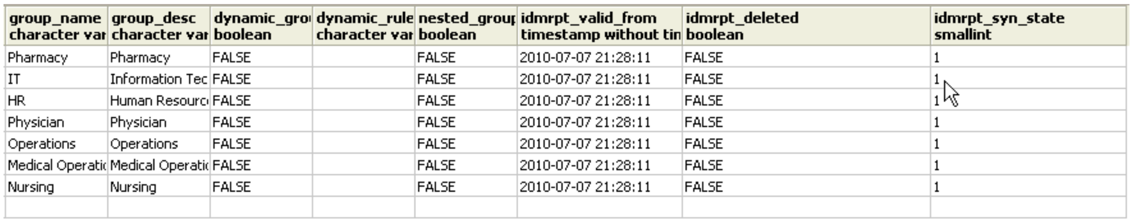
Attribute	Value
employeeType	ft
ACL	6#entry#cn=kcarson,ou=users,ou=medical-idmsample,o=novell#loginScript
ACL	6#entry#cn=kcarson,ou=users,ou=medical-idmsample,o=novell#printJobConfiguration
DirXML-Associations	cn=Data Collection Service Driver,cn=TestDrivers,o=novell#1#C53ADD67-DB19-4DD2-9482-67DD3AC519DB
givenName	Ken
photo	BINARY (2Kb)
srvprvYahooIMAddress	kcarson
objectClass	inetOrgPerson
objectClass	organizationalPerson
objectClass	Person
objectClass	ndsLoginProperties
objectClass	Top
objectClass	srvprvUserAux
objectClass	srvprvEntityAux
objectClass	homeInfo
objectClass	sampleUserDeviceAux
srvprvGroupwiseIMAddress	test
employeeStatus	Active
costCenter	US11115
ou	medical
securityEquals	cn=Medical Operations,ou=groups,ou=medical-idmsample,o=novell
securityEquals	cn=Physician,ou=groups,ou=medical-idmsample,o=novell
uid	kcarson
mail	pfredrickson@novell.com
cn	kcarson
passwordAllowChange	TRUE
sampleDeviceDN	cn=kcarson-laptop,ou=devices,ou=medical-idmsample,o=novell

- For each group, verify the following type of information:



equivalentToMe	cn=jsmith,ou=users,ou=medical-idmsample,o=novell
equivalentToMe	cn=jkelley,ou=users,ou=medical-idmsample,o=novell
description	Operations
objectClass	groupOfNames
objectClass	Top
DirXML-Associations	cn=Data Collection Service Driver,cn=TestDrivers,o=novell#1#91539E44-6AFC-4676-D9A2-449E5391FC6A
cn	Operations
member	cn=apalani,ou=users,ou=medical-idmsample,o=novell
member	cn=fstats,ou=users,ou=medical-idmsample,o=novell
member	cn=rresource,ou=users,ou=medical-idmsample,o=novell
member	cn=jsmith,ou=users,ou=medical-idmsample,o=novell
member	cn=jkelley,ou=users,ou=medical-idmsample,o=novell

7 Ensure that the data in the **idmrpt_group** table appears similar to the following information:



group_name character var	group_desc character var	dynamic_gro boolean	dynamic_rule character var	nested_group boolean	idmrpt_valid_from timestamp without tin	idmrpt_deleted boolean	idmrpt_syn_state smallint
Pharmacy	Pharmacy	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
IT	Information Tec	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
HR	Human Resourc	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Physician	Physician	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Operations	Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Medical Operati	Medical Operati	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Nursing	Nursing	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1

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 216
- "Including a Name and Description in the Database" on page 216
- "Adding Extended Attributes to Known Object Types" on page 217

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:

```
<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="notify"/>
<filter-attr attr-name="Owner" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<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:

```
<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:

```
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 new 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.

  If you also use the Data Collection Service Driver as primary on this secondary server, the driver cannot see object changes that it needs to report. To configure the Data Collection Service Driver on this server, see "Configuring the Driver for Data Collection Service" on page 203.
- **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 on page 219 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 on page 219 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 on page 219.

5e Save and restart the driver.

Setting Auditing Flags for the Drivers

This section outlines the recommended auditing settings for the Managed System Gateway Driver and the Data Collection Service Driver.

- "Setting Audit Flags in Identity Manager" on page 220
- "Setting Audit Flags in eDirectory" on page 221

Setting Audit Flags in Identity Manager

NetIQ recommends that you set auditing flags in Identity Manager for the drivers. These flags are for Novell Auditing (not XDAS).

To set the flags in iManager, go to **Driver Set Properties > Log Level > Log specific events**.

Category	Recommended Flags
Metadirectory Engine Events	◆ Metadirectory Engine Warnings
Status Events	◆ Success **NOTE:** The **Correlated Resource Assignment Events per User** report requires the Success flag. If you want to be able to run this report or customized versions of it, then you need to enable the Success flag. ◆ Error ◆ Fatal
Operation Events	◆ Modify ◆ Add Association ◆ Check Password ◆ Add Value ◆ Add ◆ Rename ◆ Remove Association ◆ Check Object Password ◆ Clear Attribute ◆ Remove Value ◆ Get Named Password ◆ Remove ◆ Move ◆ Change Password ◆ Add Value (on modify) ◆ Reset Attributes
Transformation Events	◆ Password Reset ◆ User Agent Request ◆ Password Sync
Credential Provisioning Events	◆ Set SSO Credentials ◆ Clear SSO Credentials ◆ Set SSO Passphrase

Setting Audit Flags in eDirectory

NetIQ recommends that you set auditing flags in eDirectory for the drivers. These flags are for Novell Auditing (not XDAS).

To set the flags in iManager, go to **eDirectory Auditing > Audit Configuration > Novell Auditing**.

Category	Recommended Flags
Global	◆ Do Not Send Replicated Events
Meta	◆ (*Select all flags)*
Objects	◆ Add Property ◆ Allow Login ◆ Change Password ◆ Change Security Equals ◆ Create ◆ Delete ◆ Delete Property ◆ Login ◆ Logout ◆ Modify RDN ◆ Move (Source) ◆ Move (Destination) ◆ Remove ◆ Rename ◆ Restore ◆ Search ◆ Verify Password
Attributes	◆ *(Select all flags)*
Agent	◆ DS Reloaded ◆ Local Agent Opened ◆ Local Agent Closed ◆ NLM Loaded
Miscellaneous	◆ Generate CA Keys ◆ Recertified Public Key

Category	Recommended Flags
LDAP	◆ LDAP Bind ◆ LDAP Bind Response ◆ LDAP Modify ◆ LDAP Modify Response ◆ LDAP Password Modify ◆ LDAP Unbind ◆ LDAP Delete ◆ LDAP Delete Response ◆ LDAP Modify DN ◆ LDAP Modify DN Response ◆ LDAP Search ◆ LDAP Search Response ◆ LDAP Add ◆ LDAP Add Response

V 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`.

You cannot use Designer 2.1*x* workspaces for Designer 3.0 or later because older workspace versions are not compatible with more recent versions of Designer. Designer stores projects and configuration information in **workspaces**. For example, on **Windows 10 and Windows 7**, Designer 4.x workspaces are installed in `%UserProfile%\designer_workspace` directory by default.

NetIQ recommends that you review the installation process before beginning. For more information, see Chapter 16, "Planning to Install Designer," on page 227.

16 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 227

Checklist for Installing Designer

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

	Checklist Items
□	1. Review the planning information. For more information, see Part I, "Planning to Install Identity Manager," on page 17.
□	2. Review the considerations for installing Designer to ensure that the computer meets the prerequisites. For more information, see "Meeting System Requirements" on page 22.
□	3. To install Designer, see one of the following sections: - "Running the Windows Executable File" on page 229 - "Using the Silent Installation Process" on page 229
□	4. Install the rest of the Identity Manager components.
□	5. (Optional) To start a project for your Identity Manager solution, see the *NetIQ Designer for Identity Manager Administration Guide*.

17 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. Use the installation program, located by default in `\products\Designer\` directory:

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 229
- "Using the Silent Installation Process" on page 229
- "Modifying an Installation Path that Includes a Space Character" on page 230

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_4.7_Windows_Designer.zip` from the NetIQ Downloads Website.
3. Extract the `Identity_Manager_4.7_Windows_Designer.zip` file.
4. Run the `install.exe` file.
5. 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, by default in the *`Path_to_unzipped_Designer_file`*`\products\Designer` 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 one of the following command:

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

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
```

VI 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.

The installation files are located in the `\products\Analyzer` directory within the `.iso` image file for the Identity Manager installation package. 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 233.

18 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 233

Checklist for Installing Analyzer

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

	Checklist Items
❑	1. Review the planning information. For more information, see Part I, "Planning to Install Identity Manager," on page 17.
❑	2. Review the considerations for installing Analyzer to ensure that the computer meets the prerequisites. For more information, see "Meeting System Requirements" on page 22.
❑	3. To install Analyzer, see the following sections: ◆ To use the installation wizard, see "Using the Wizard to Install Analyzer" on page 235. ◆ For a silent installation, see "Installing Analyzer Silently" on page 236
❑	4. (Optional) To automatically receive and display audit events from Analyzer, install the XDAS client. For more information, see "Installing an Audit Client for Analyzer" on page 236.
❑	5. To activate Analyzer, see Activating Analyzer in the *NetIQ Identity Manager Overview and Planning Guide*.

19 Installing Analyzer

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

- "Using the Wizard to Install Analyzer" on page 235
- "Installing Analyzer Silently" on page 236
- "Installing an Audit Client for Analyzer" on page 236

Using the Wizard to Install Analyzer

The following procedure describes how to install Analyzer using an installation wizard. To perform a silent, unattended installation, see "Installing Analyzer Silently" on page 236.

To prepare for the installation, review the prerequisites and system requirements listed in "Checklist for Installing Analyzer" on page 233.

1 Log in to the computer where you want to install Analyzer.

2 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the Analyzer installation files, located by default in the `\products\Analyzer` directory.

3 (Conditional) If you downloaded the Analyzer installation files, complete the following steps:

  3a Navigate to the `win.zip` file for the downloaded image.

  3b Extract the contents of the file to a folder on the local computer.

4 From the `\products\Analyzer` directory, execute the `install.exe` installation program:

5 Follow the instructions in the wizard until you finish installing Analyzer.

6 When the installation process completes, review the post-installation summary to verify the installation status and the location of the log file for Analyzer.

7 Click **Done**.

8 (Optional) To configure role-based services for Analyzer on the Windows computer, open the link to the `gettingstarted.html` website, located by default in the `C:\Program Files (x86)\NetIQ\Tomcat\webapp\nps\help\en\install` directory.

You use iManager to configure the role-based services.

9 To activate Analyzer, see Activating Analyzer in the *NetIQ Identity Manager Overview and Planning Guide*.

Installing Analyzer Silently

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, InstallAnywhere uses information from a default `analzerInstaller.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process.

By default, the installation program installs Analyzer in the `Program Files (x86)\NetIQ\Analyzer` directory.

1 Log in as to the computer where you want to install Analyzer.

2 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the Analyzer installation files, located by default in the `\products\Analyzer` directory.

3 Conditional) If you downloaded the Analyzer installation files from the NetIQ Downloads website, complete the following steps:

  3a Navigate to the `win.zip` file for the downloaded image.

  3b Extract the contents of the file to a folder on the local computer.

4 (Optional) To specify a non-default installation path, complete the following steps:

  4a Open the `analzerInstaller.properties` file, located by default in the `\products\Analyzer` directory.

  4b Add the following text to the properties file:

```
USER_INSTALL_DIR=installation_path
```

5 To run the silent installation, issue the following command:

```
install.exe -i silent -f analyzerInstaller.properties
```

6 To activate Analyzer, see Activating Analyzer in the*NetIQ Identity Manager Overview and Planning Guide*.

Installing an Audit Client for Analyzer

Analyzer includes an XDAS library that automatically generates audit events from the Data Browser editor when you send data updates back to the application. For more information about using the Data Browser editor to update data in the source application, see “Modifying Data” in the NetIQ Analyzer for Identity Manager Administration Guide.

To view these audit events, install an XDAS client that can receive the audit events from Analyzer. More information about XDAS is available at the OpenXDAS Project (http://openxdas.sourceforge.net).

Analyzer includes a Windows XDAS client as part of its download package. However, the installation program for Analyzer does not install the XDAS client.

1 Install Analyzer.

2 Navigate to the OpenXDAS installation files, located by default in the `\products\Analyzer\openxdas\`*`Operating_system`* directory of the `.iso` image file.

3 Launch the installation program (`.msi` file) for the XDAS client:

4. Follow the prompts to install the XDAS client.
5. After the installation process completes, launch the XDAS client to automatically receive and display audit events from Analyzer.

20 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 239
- "Creating and Configuring a Driver Set" on page 239
- "Creating a Driver" on page 242
- "Defining Policies" on page 242
- "Managing Driver Activities" on page 243
- "Activating Identity Manager" on page 243

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 240
- "Assigning the Default Password Policy to Driver Sets" on page 240
- "Creating the Password Policy Object in the Identity Vault" on page 240
- "Creating a Custom Password Policy" on page 241
- "Creating the Default Notification Collection Object in the Identity Vault" on page 241

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 240 and "Creating a Custom Password Policy" on page 241.

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:

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
nsimPwdRuleEnforcement: FALSE
nspmSpecialAsLastCharacter: TRUE
nspmSpecialAsFirstCharacter: TRUE
nspmSpecialCharactersAllowed: TRUE
nspmNumericAsLastCharacter: TRUE
nspmNumericAsFirstCharacter: TRUE
nspmNumericCharactersAllowed: TRUE
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: <driverset LDAP dn>
```

NOTE: Copying the content as is might insert some hidden special characters in the file. If you receive a `ldif_record() = 17` error message when you add these attributes to the Identity Vault, insert an extra space between the two DNs.

2 To add the DirMXL-PasswordPolicy object in the Identity Vault, import the attributes from the file by running `ldapmodify.exe` from the `install/utilities` directory of the Identity Manager installation kit.

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*.

NOTE: You must also assign the DirXML-PasswordPolicy object to the driver sets. For more information, see "Creating the Password Policy Object in the Identity Vault" on page 240.

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.

3 Right-click the Identity Vault, then click Identity Vault **Properties**.

4 Click **Packages**, then click the **Add Packages** icon.

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

6 Click **Apply** to install the packages with the **Install** operation.

7 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*.

VII Upgrading Identity Manager

This section provides information for upgrading Identity Manager components. To migrate existing data to a new server, see Part IX, “Migrating Identity Manager Data to a New Installation,” on page 301. For more information about the difference between upgrade and migration, see “Understanding Upgrade and Migration” on page 249.

21 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 4.7. Otherwise, you can encounter severe conflicts during regular Identity Manager patch updates

- "Checklist for Upgrading Identity Manager" on page 247
- "Understanding Upgrade and Migration" on page 249
- "Upgrade Order" on page 250
- "Supported Upgrade Paths" on page 251
- "Backing Up the Current Configuration" on page 254

Checklist for Upgrading Identity Manager

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

	Checklist Items
□	1. Review the differences between an upgrade and a migration. For more information, see "Understanding Upgrade and Migration" on page 249.
□	2. Upgrade to Identity Manager 4.5.6. You cannot upgrade or migrate to version 4.7 from versions before 4.5.6. For more information, see the NetIQ Identity Manager 4.5 Setup Guide.
□	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*.
□	4. Ensure that your computers meet the hardware and software prerequisites for a newer version of Identity Manager. For more information, see "Meeting System Requirements" on page 22.
□	5. Back up the current project, driver configuration, and databases. For more information, see "Backing Up the Current Configuration" on page 254.
□	6. Upgrade Designer to the latest version. For more information, see "Upgrading Designer" on page 259.

	Checklist Items
□	7. Install or upgrade iManager to the latest version for Identity Manager. For more information, see one of the following sections: ◆ **Installation**: “Installing iManager” on page 73 ◆ **Upgrade**: “Upgrading iManager” on page 260
□	8. On the server running Identity Manager, upgrade eDirectory to the latest version and patch. If you are upgrading eDirectory 9.0 or later in an environment where a 64-bit Remote Loader is already upgraded, the eDirectory installation fails and the Remote Loader stops working. To ensure that the Remote Loader works properly, perform the following steps before upgrading eDirectory: 1. Stop the Remote Loader and its instances. 2. Uninstall `novell-DXMLopensslx` RPM. 3. Install eDirectory 9.1 or later version. Upgrading eDirectory stops ndsd, which in turn stops all drivers. For more information, see the *NetIQ eDirectory Installation Guide*.
□	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 263.
□	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 280.
□	11. Upgrade the Identity Manager engine. For more information, see “Upgrading the Identity Manager Engine” on page 265. **NOTE:** 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 308.
□	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 263.
□	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 282. 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.
□	14. (Conditional) If OSP is not installed, install OSP. For more information, see Chapter 9, “Installing the Single Sign-on Component,” on page 97.
□	15. (Conditional) If SSPR is not installed, install SSPR. For more information, see Chapter 10, “Installing the Password Management Component,” on page 105. **NOTE:** Install SSPR if you are currently using the legacy provider for password management. For more information, see “Understanding the Legacy Password Management Provider” on page 25.

	Checklist Items
❑	16. Upgrade the User Application, Identity Manager Dashboard, OSP, SSPR, and Identity Reporting using upgrade program. For more information, see “Upgrading Identity Applications and Identity Reporting” on page 267. Alternatively, you can upgrade these components manually. For more information, see Part IX, “Migrating Identity Manager Data to a New Installation,” on page 301.
❑	17. Upgrade Identity Reporting and associated drivers. For more information, see “Upgrading Identity Reporting” on page 278.
❑	18. 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 280.
❑	19. (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 284.
❑	20. (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 285.
❑	21. Activate your upgraded Identity Manager solution. For more information, see “Activating Identity Manager” on page 243.

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 4.7 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.

During the product evaluation period or after activating Advanced Edition, you might want to **switch** to Standard Edition if you do not want Advanced Edition functionality in your environment. Identity Manager allows you to switch from Advanced Edition to Standard Edition by following a simple procedure.

Upgrade

In general, you can upgrade Identity Manager 4.6 Standard and Advanced Editions.

- **Identity Manager 4.6 Standard Edition:** If you currently have Identity Manager 4.6 Standard Edition, you can directly upgrade it to Identity Manager 4.6 Standard Edition. For more information, see Quick Start Guide for Installing and *Upgrading NetIQ Identity Manager 4.7 Standard Edition*.

To upgrade Identity Manager 4.6 Standard Edition to Identity Manager 4.7 Advanced Edition, choose one of the following approaches to complete the upgrade:

- Upgrade Identity Manager 4.6 Standard Edition to Identity Manager 4.7 Standard Edition and then upgrade to Identity Manager 4.7 Advanced Edition. For more information, see *Upgrading NetIQ Identity Manager 4.7 Standard Edition*.
- Upgrade Identity Manager 4.6 Standard Edition to Identity Manager 4.6 Advanced Edition and then upgrade to Identity Manager 4.7 Advanced Edition. For more information, see *Upgrading NetIQ Identity Manager 4.6 Standard Edition*.

- **Identity Manager 4.6 Advanced Edition:** If you currently have Identity Manager 4.6 Advanced Edition, you can directly upgrade it to Identity Manager 4.7 Advanced Edition. For more information, see "Checklist for Upgrading Identity Manager" on page 247.

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 4.7 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 4.7 or later.

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.

IMPORTANT: If you have already applied Advanced Edition activation, you need not move to Standard Edition as all Standard Edition functionality is available in Advanced Edition. You must 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. For more information, see Chapter 23, "Switching from Advanced Edition to Standard Edition," on page 287.

Upgrade Order

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

1. Designer
2. iManager
3. Sentinel Log Management for IGA
4. Identity Vault
5. Identity Manager Engine/Remote Loader

6. iManager Plug-Ins
7. Tomcat and PostgreSQL Components
8. Single Sign-on (One SSO Provider)
9. Self Service Password Reset
10. Identity Applications (for Advanced Edition)
11. Identity Reporting
12. Analyzer

For information about the latest supported upgrade paths, see the Release Notes for your version from the Identity Manager 4.6 Documentation web site.

Supported Upgrade Paths

Identity Manager 4.7 includes support for upgrade from 4.6.x and 4.5.x versions. Before starting the upgrade, NetIQ recommends that you review the information from the appropriate release notes for your current version.

- "Upgrading from Identity Manager 4.6.x Versions" on page 251
- "Upgrading from Identity Manager 4.5.x Versions" on page 252

Upgrading from Identity Manager 4.6.x Versions

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

Component	Base Version	Upgraded Version
Identity Manager Engine	4.6.x	1. Upgrade the operating system to a supported version. 2. Upgrade Identity Vault to 9.1. 3. Upgrade Identity Manager Engine to 4.7.
Remote Loader/Fanout Agent	4.6.x	Install 4.7 Remote Loader/Fanout Agent
Designer	4.6.x	1. Install Designer 4.7. 2. Convert your workspace from NCP to LDAP. Designer 4.7 is LDAP-based. Before using this version, see *NetIQ Identity Manager LDAP Designer Release Notes*.

Component	Base Version	Upgraded Version
Identity Applications	4.6.x	Before you upgrade Identity Applications, ensure that the Identity Vault and Identity Manager engine are upgraded to 9.1 and 4.7 respectively. 1. Upgrade the operating system to a supported version. 2. Upgrade the database to a supported version. For supported database versions, see the NetIQ Identity Manager Technical Information website. 3. (Conditional) If SSPR is installed on a separate server, upgrade the component to 4.7 version. 4. Update the User Application driver and Roles and Resources driver packages. 5. Upgrade Identity Applications to 4.7. 6. Stop Tomcat.
Identity Reporting	4.6.x	1. Upgrade the operating system to a supported version. 2. Upgrade the database to a supported version. For supported database versions, see the NetIQ Identity Manager Technical Information website. 3. Upgrade SLM for IGA. 4. Update the Data Collection Services and Managed Services Gateway driver packages. 5. Install Identity Reporting 4.7. 6. Create a data synchronization policy from the Identity Manager Data Collection Services page.

Before starting the upgrade, NetIQ recommends that you review the information from the release notes for your version:

- NetIQ Identity Manager 4.6 Service Pack 2 Release Notes
- NetIQ Identity Manager 4.6 Service Pack 1 Release Notes
- NetIQ Identity Manager 4.6 Release Notes

Upgrading from Identity Manager 4.5.x Versions

The following table lists component-wise upgrade paths for Identity Manager 4.5.x versions:

Component	**Base Version**	**Intermediate Step**	**Upgraded Version**
Identity Manager Engine	Identity Manager 4.5.x (where x is 0 to 5) with eDirectory 8.8.8.x (where x is 3 to 9)	Apply the 4.5.6 patch	1. Upgrade the operating system to a supported version. 2. Upgrade Identity Vault to 9.1. 3. Upgrade Identity Manager Engine to 4.7.
Remote Loader/ Fanout Agent	4.5.x, where x is 0 to 5	Apply the 4.5.6 patch	Install 4.7 Remote Loader/Fanout Agent.
Designer	4.5.x, where x is 0 to 5	Apply the 4.5.6 patch	1. Install Designer 4.7. 2. Convert your workspace from NCP to LDAP. Designer 4.7 is LDAP-based. Before using this version, see *NetIQ Identity Manager LDAP Designer Release Notes*.
Identity Applications	4.5.x, where x is 0 to 5	◆ If you are using JBoss or Websphere, migrate to Tomcat application server. ◆ Apply the 4.5.6 patch.	Before upgrading Identity Applications, ensure that Identity Vault and Identity Manager engine are upgraded to 9.1 and 4.7 versions respectively. 1. Upgrade the operating system to a supported version. 2. Update the User Application driver and Roles and Resources driver packages. 3. Upgrade the database to a supported version. For supported database versions, see the NetIQ Identity Manager Technical Information website. 4. (Conditional) If SSPR is installed on a separate server, upgrade the component to 4.7 version. 5. Upgrade Identity Applications to 4.7. 6. Stop Tomcat.

Component	Base Version	Intermediate Step	Upgraded Version
Identity Reporting	4.5.x, where x is 0 to 5	- If you are using JBoss or Websphere, migrate to Tomcat application server. - Apply the 4.5.6 patch.	1. Upgrade the operating system to a supported version. 2. Upgrade the database to a supported version. For supported database versions, see the NetIQ Identity Manager Technical Information website. 3. Migrate Event Auditing Service data to a supported version of PostgreSQL or Oracle database. 4. Install SLM for IGA. 5. Update the Data Collection Services and Managed Services Gateway driver packages. 6. Install Identity Reporting 4.7. 7. Create a data synchronization policy from the Identity Manager Data Collection Services page.

Before starting the upgrade, NetIQ recommends that you review the information from the release notes for your version:

- NetIQ Identity Manager 4.5 Service Pack 6 Release Notes
- NetIQ Identity Manager 4.5 Service Pack 5 Release Notes
- NetIQ Identity Manager 4.5 Service Pack 4 Release Notes
- NetIQ Identity Manager 4.5 Service Pack 3 Release Notes
- NetIQ Identity Manager 4.5 Service Pack 2 Release Notes
- NetIQ Identity Manager 4.5 Service Pack 1 Release Notes
- NetIQ Identity Manager 4.5 Release Notes

Backing 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 255
- "Exporting the Configuration of the Drivers" on page 256

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 255
- "Creating a New Project from the Identity Vault" on page 255

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 256
- "Using iManager to Create an Export of the Driver" on page 256

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.

22 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

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 Identity Manager media (`\products\Designer\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**.

15 Review the summary of what happens during the conversion, then click **Convert**.

16 Review the summary after the conversion finishes, then click **Open**.

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 iManager

In general, the upgrade process for iManager uses the existing configuration values in the `configiman.properties` file, such as port values and authorized users. Before upgrading, NetIQ recommends that you back up the `server.xml` and `context.xml` configuration files if you have previously modified them.

If you are on eDirectory 9.1, upgrade your iManager version to 3.1. iManager 3.1 installation files are located in the `<iso_extracted_directory>\products\iManager277\installs\win` directory.

The upgrade process includes the following activities:

- "Upgrading iManager on Windows" on page 260
- "Updating Role-Based Services" on page 262
- "Re-installing or Migrating Plug-ins for Plug-in Studio" on page 263
- "Updating iManager Plug-ins after an Upgrade or Re-installation" on page 263

Upgrading iManager on Windows

If the setup program for iManager Server detects a previously installed version of iManager, it might prompt you to upgrade the installed version. If you choose to upgrade, the program replaces the existing JRE and Tomcat versions with the latest versions. This will also upgrade the iManager to the latest version.

Before upgrading iManager, ensure that the computer meets the prerequisites and system requirements. For more information, see the following sources:

- The Release Notes accompanying the update.
- For iManager, see "Considerations for Installing iManager Server" on page 76.
- For iManager Workstation, see "Considerations for Installing iManager Workstation" on page 76.

NOTE: The upgrade process uses the HTTP port and SSL port values that were configured in the previous version of iManager.

To install iManager Server on Windows:

1. Log in as a user with administrator privileges on the computer where you want to upgrade iManager.
2. (Conditional) If you modified the `server.xml` and `context.xml` configuration files, save a backup copy of the files in a different location before performing the upgrade.

   The upgrade process replaces the configuration files.
3. At the NetIQ Downloads website, select the iManager version that you want, then download the `win.zip` file to a directory on your server. For example, `iMan_277_win.zip`.
4. Extract the `win.zip` file to the iManager folder.
5. Run `iManagerInstall.exe`, located by default in the *`extracted_directory`*`\iManager\installs\win` folder.
6. In the iManager welcome window, select a language, and then click **OK**.
7. In the **Introduction** window, and then click **Next**.
8. Accept the License Agreement, and then click **Next**.
9. (Optional) To use IPv6 addresses with iManager, click **Yes** in the **Enable IPv6** window.

   You can enable IPv6 addresses after you upgrade iManager. For more information, see "Configuring iManager for IPv6 Addresses after Installation" on page 85.
10. Click **Next**.
11. At the Upgrade prompt, select **Upgrade**.
12. (Conditional) Review the **Detection Summary** window.

    The **Detection Summary** window lists the latest version of Servlet container and JVM software that iManager will use once it is upgraded.
13. Click **Next**.
14. Read the **Pre-installation summary** page, and then click **Install**.

    The upgrade process can take several minutes. The process might add new files for iManager components or change the iManager configuration. For more information, see the Release Notes for the upgrade.
15. (Conditional) If the **Install Complete** window displays the following error message, complete the following steps:

    ```
    The installation of iManager version is complete, but some errors
    occurred during the install.
    Please see the installation log Log file path for details. Press "Done"
    to quit the installer.
    ```

    15a Note the path to the log file that the error message displays.

    15b In the **Install Complete** window, click **Done**.

    15c Open the log file.

    15d (Conditional) If you find the following error in the log file, you can ignore the error message. The installation was successful, and iManager functions properly.

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class
com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The
process cannot access the file because it is being used by another
process)
```

15e (Conditional) If the log file does not contain the error listed in Step 21d, NetIQ recommends that you retry the installation.

16 Click **Done**.

17 When the initialization of iManager finishes, click the first link in the Getting Started page, and then log in. For more information, see "Accessing iManager" in the *NetIQ iManager Administration Guide*.

18 (Conditional) If you made backup copies of the `server.xml` and `context.xml` configuration files before starting the upgrade process, replace the new configuration files with the backup copies.

Updating Role-Based Services

The first time that you use iManager to log in to an eDirectory tree that already contains a Role-Based Services (RBS) collection, you might not see all of the roles information. This behavior is normal because you must update some of the plug-ins to function with the latest version of iManager. 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. The RBS Configuration table lists which RBS modules need to be updated.

Be aware that you might have multiple roles with the same name. Starting with iManager 2.5, some plug-in developers changed task IDs or module names but retained the same display names. This issue causes the roles to appear to be duplicated when, in fact, one instance is from one version and the other is from a newer version.

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**. For more information, see "Understanding Installation for iManager Plug-ins" on page 74.
- 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 (Optional) 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.

3b Select the module you that want to update.

3c Click **Update** at the top of the table.

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. For more information, see "Understanding Installation for iManager Plug-ins" on page 74.

1 Open iManager.

2 Navigate to **Configure > Plug-in Installation > Available Novell Plug-in Modules**.

3 Update the plug-ins.

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 (Conditional) To run a silent installation on a Windows server, ensure that the `silent.properties` file includes the path to the directory that contains the installed Remote Loader files. For example:

```
X64_CONNECTED_SYSTEM_LOCATION=c:\novell\remoteloader\64bit
```

The installation program does not detect the default path for the previous installation.

6 Run the installation program for the Remote Loader.

The installation process updates the files and binaries to the current version. For more information, see Part II, “Installing Identity Manager Engine,” on page 29.

7 After the installation finishes, verify that your configuration files contain your environment’s information.

8 (Conditional) If there is a problem with the configuration file, copy the backup file that you created in Step 1. Otherwise, continue with Step 9 on page 264.

9 Start the Remote Loader service or daemon for each driver.

In the Remote Loader Console, select the Remote Loader instance, then click **Start**.

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 266.

Upgrading the Java Remote Loader

1 Create a backup of the Java Remote Loader configuration files.

2 Verify that the drivers are stopped. For more information, see “Stopping the Drivers” on page 280.

3 Stop the Remote Loader service or daemon for each driver.

```
dirxml_jremote -config path_to_configfile -u
```

4 Download and extract the `Identity_Manager_4.7_Windows.iso` from the NetIQ Downloads website.

5 Navigate to the `products\idm\java_remoteloader` directory.

6 Copy and replace the `dirxml_jremote_dev.tar.gz` file in your existing Java Remote Loader installed directory.

7 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`

8 Extract the files that you have copied in step 6 and step 7.

Use 7-Zip or supported software to unzip the `.tar.gz` files.

9 (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.

10 Start the Remote Loader service or daemon for each driver.

```
dirxml_jremote -config path_to_config_file
```

Upgrading the Identity Manager Engine

When you upgrade Identity Manager engine or separately update a SAML method, iMonitor displays both present and not present status flags for SAML methods. You can ignore the not present status flag because eDirectory correctly uses the updated method. When the engine is upgraded, the upgrade process restarts eDirectory that internally takes care of using the updated SAML method. If you separately update a SAML method, manually restart the eDirectory server to use the updated SAML method.

After you upgrade the Remote Loader and the Roles Based Services, you can upgrade the Identity Manager Engine. The upgrade process updates the driver shim files that are stored in the file system on the host computer.

If your driver is using MapDB, ensure that your upgraded driver works correctly with the upgraded Engine. For more information, see "Working with MapDB 3.0.5" on page 266.

Upgrading the Identity Manager Engine

1. Ensure that there are no events in the cache file before you begin upgrading Identity Manager Engine.
2. Verify that the drivers are stopped. For more information, see Stopping, Starting, or Restarting a Driver in Designer in the *NetIQ Identity Manager Driver Administration Guide*.
3. Launch the installation program for Identity Manager engine from `IDM`*`version`*`_Win:\products\idm\Windows\setup\idm_install.exe`.
4. Select the language that you want to use for the installation.
5. Read and accept the license agreement.
6. To update the Identity Manager engine and driver shim files, select the following options:
    - **Identity Manager Server**
    - **iManager Plug-ins for Identity Manager**
    - **Drivers**
7. Specify a user and the user password with administrative rights to eDirectory in LDAP format.
8. Review the summary, then click **Install**.
9. Read the installation summary, then click **Done**.

The 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 a driver using MapDB after upgrading the driver. For more information, see "Working with MapDB 3.0.5" on page 266.

Working with MapDB 3.0.5

Identity Manager 4.7 adds support for MapDB 3.0.5. In 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 4.7 Engine Support for Driver Versions" on page 266
- "Manually Removing the MapDB Cache Files" on page 266

Understanding Identity Manager 4.7 Engine Support for Driver Versions

Review the following considerations before upgrading an Identity Manager driver that uses MapDB:

- Drivers shipped with Identity Manager 4.7 are compatible with Identity Manager 4.7 Engine or Remote Loader. You must follow the driver upgrade steps from the specific driver implementation guide.
- Drivers shipped before Identity Manager 4.7 are not compatible with Identity Manager 4.7 Engine or Remote Loader.
- Drivers shipped with Identity Manager 4.7 are not backward compatible with Identity Manager 4.6.x Engine or Remote Loader.
- Drivers shipped with Identity Manager 4.7 are not backward compatible with Identity Manager 4.5.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 (`C:\Novell\NDS\DIBFiles`). You must manually remove these files for your driver after upgrading the driver. This action ensures that your driver works correctly with Identity Manager 4.7 engine.

The following table lists the MapDB cache files that must be removed:

Identity Manager Driver	MapDB State Cache File To Remove

Data Collection Services	`DCSDriver_<driver instance guid>-*`
	`<driver instance guid>-*`

JDBC	`jdbc_<driver instance guid>_*`

Identity Manager Driver	MapDB State Cache File To Remove
LDAP	ldap_<driver instance guid>*
Managed System Gateway	MSGW-<driver-instance-guid>.*
Office 365 and Azure Active Directory	<Azure driver name>_obj.db.*
Salesforce	<Salesforce driver name>.*
	<Salesforce driver name>

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
- 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 Identity Applications and Identity Reporting

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
- Identity Reporting

NetIQ provides an upgrade program to upgrade these components. This program is located in the `products\CommonApplication\` directory in the Identity Manager installation package. Navigate to the directory that contains the `ApplicationUpgrade.exe` file.

After the upgrade, the components are upgraded to the following versions:

- Tomcat – 8.5.27
- ActiveMQ – 5.15.2
- Java – 1.80_162
- One SSO Provider – 6.2.1
- Self-Service Password Reset – 4.2.0.4
- Identity Applications – 4.7.0
- Identity Reporting – 6.0.0

This section provides information about the following topics:

- "Understanding the Upgrade Program" on page 268
- "Prerequisites and Considerations for Upgrade" on page 268
- "Upgrading the PostgreSQL Database" on page 269
- "System Requirements" on page 271
- "Upgrading the Driver Packages for Identity Applications" on page 271
- "Using the Guided Process to Upgrade" on page 272
- "Post-Upgrade Tasks" on page 275

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.

Prerequisites and Considerations for Upgrade

Before performing an upgrade, review the following considerations:

- **Identity Manager is upgraded to version 4.5.6:** You cannot upgrade to version 4.7 from versions lesser than 4.5.6. For more information about how to upgrade to Identity Manager 4.5, see Upgrading Identity Manager in the *NetIQ Identity Manager Setup Guide*.
- **System Requirements:** The upgrade process requires at least 3 GB free disk space for storing the current configuration and the temporary files that are created during upgrade. Ensure that your server has sufficient space to store the back-up and additional free space available for upgrade.

  On a Windows server, the upgrade program stores the temporary files in a directory specified in the %TEMP% environment variable. If this directory does not have the required space, set TEMP and TMP environment variables to a directory on your file system that has sufficient free space. This will redirect the upgrade program to store the files in that directory.

  To set these environment variables to a different directory, complete the following steps before starting the upgrade:

  1. Open the command prompt and enter the following command:

     ```
     SET TMP=D:\custom_tmp
     SET TEMP=D:\custom_tmp
     ```

     where `D:\custom_tmp` is the path to the directory that has sufficient free disk space.

     NOTE: For cluster environment, backup the Identity Applications certificates (`cacerts`).

  2. Start the upgrade program from the command line.
- **Tomcat as an application server:** This version of Identity Manager supports only Tomcat as an application server.

NOTE: Ensure you have installed Tomcat application server using the convenience installer during your previous installation. The upgrade process allows you to upgrade only Tomcat that has been installed using the convenience installer.

- **Database platform is upgraded:** This program does not upgrade the database platform for the identity applications. Manually upgrade your current version of the database to a supported version. For upgrading the PostgreSQL database, see "Upgrading the PostgreSQL Database" on page 269.
- **Identity applications and Identity Reporting drivers are upgraded:** Ensure you have upgraded the following drivers for identity applications and Identity Reporting.
  - User Application Driver
  - Roles and Resource Driver
  - Manage System Gateway Driver
  - Data Collection Service Driver

  For more information, see Upgrading Installed Packages in the *NetIQ Designer for Identity Manager Administration Guide*
- **Administrator user has the highest access privileges:** Provide the highest access privileges to the administrator user.
- **User Account Control settings are changed to Never Notify:** Go to **Control Panel > User Accounts** and **Change User Account Control Settings** to **Never Notify**.
- **Self Service Password Reset:** If you are upgrading from SSPR 4.0, ensure you have updated `CATALINA_OPTS` property and `-Dsspr.application.Path` is set to the folder where your SSPR configuration is stored.

  For example: `set CATALINA_OPTS="-Dsspr.applicationPath=C:\sspr_data`

  Backup your SSPR LocalDB before upgrading. To export or download LocalDB, perform the following steps:
  1. Log in to SSPR portal as an administrator.
  2. Navigate to **Your ID > Configuration Manager** from the drop-down menu.
  3. Click **LocalDB**.
  4. Click **Download LocalDB**.

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_9_3`.
3. Install PostgreSQL version supported on your operating system.

You must choose a location other than the current installation location of PostgreSQL.

3a Mount the `Identity_Manager_4.7_Windows.iso` image file and navigate to the `products\CommonApplication\postgre_tomcat_install` directory containing the PostgreSQL installation files.

3b Install the PostgreSQL application by running 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.

---

4 Stop the newly installed PostgreSQL service. Go to **Services**, search for PostgreSQL 9.6 service, and stop the service.

NOTE: Appropriate users can perform stop operations after providing valid authentication.

---

5 Change the permissions for the newly installed PostgreSQL directory by performing the following actions:

Create a `postgres` user:

1. Go to **Control Panel > User Accounts > User Accounts > Manage Accounts**.
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**.

6 Access the PostgreSQL directory as `postgres` user.

1. Login 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. Open a command prompt and set PGPASSWORD by using the following command:

   ```
   set PGPASSWORD=<your pg password>
   ```

3. Change to the newly installed PostgreSQL directory.

   For example: `C:\Users\postgres>cd C:\NetIQ\idm\apps1\postgresql962\bin`.

7 Upgrade PostgreSQL from new PostgreSQL `bin` directory. Run the following command and click **Enter**.

```
pg_upgrade.exe --old-datadir "C:\NetIQ\idm\apps1\postgres\data" --new-datadir "C:\NetIQ\idm\apps1\postgresql962\data" --old-bindir "C:\NetIQ\idm\apps1\postgres\bin" --new-bindir "C:\NetIQ\idm\apps1\postgresql962\bin"
```

8 Start the upgraded PostgreSQL database service.

Go to **Services**, search for PostgreSQL 9.6 service, and start the service.

NOTE: Appropriate users can perform start operations after providing valid authentication.

9 Disable the old PostgreSQL service to ensure that the service does not automatically start.

10 (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\apps1\postgresql961\bin`

NOTE: You must run this step only if you want to delete the old data files.

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 Driver Packages for Identity Applications

This section explains how to update the packages for the User Application Driver and Roles and Resource Service drivers to the latest version. You must perform this task before upgrading Identity Applications.

1 In Designer, open your current project.

2 Right-click **Package Catalog > Import Package**.

3 Select the appropriate package. For example, **User Application Driver Base package**.

4 Click **OK**.

5 In the Developer View, right-click the driver and then click **Properties**.

6 Navigate to the **Packages** tab in the **Properties** page.

7 Click the **Add package (+)** symbol in the top right corner.

8 Select the package, and then click **OK**.

9 Deploy and restart the driver.

10 Repeat the same procedure to upgrade the package for the Roles and Resource Service driver.

NOTE

- Ensure that the User Application driver and Roles and Resource Service driver are connected to the upgraded Identity Manager.
- If you install any notification templates while upgrading User Application Driver package, deploy the **Default Notification Collection** objects to your Identity Manager server.

Using the Guided Process to Upgrade

The following procedure describes how to upgrade Identity Applications, OSP, SSPR, Tomcat, ActiveMQ, and Identity Reporting using wizard.

1. Log in to the server where you want to run upgrade process.
2. Mount the `.iso` image file, navigate to the directory containing the upgrade executable, located by default in the `products\CommonApplication\` directory.
3. Stop Tomcat service and ensure that all the User Application related files are closed.
4. Launch the upgrade program. Right-click `ApplicationUpgrade.exe` and select **Run as administrator**.
5. On the **Introduction** page, you can view Identity Manager components that you can upgrade, then click **Next**.
6. Read and accept the license agreement, then click **Next**.
7. Review the **Deployed Applications** page, then click **Next**.

   This page lists the currently installed components and lists their versions. If other applications are deployed on the server, the upgrade process displays a warning that those applications might not work properly after the upgrade.

   You must restore them manually from the back-up created by the upgrade process.
8. To proceed with the upgrade, click **Next**.
9. Complete the guided process, using the following parameters. This program auto populates the values for existing components. Ensure that the correct values are specified for the parameters.
   - **One SSO Provider Installation folder**

     Represents the path to a directory where the upgrade program creates the application files for OSP. If the path is not correct, browse to the path where OSP is installed.
   - **SSPR Installation folder**

     Represents the path to a directory where the upgrade program creates the application files for SSPR. If the path is not correct, browse to the path where SSPR is installed.
   - **User Application Installation folder**

     Represents the path to a directory where the upgrade program creates the application files for the User Application. If the path is not correct, browse to the path where User Application is installed.
   - **Database Connection**

     Represents the settings for connecting to the User Application database, Identity Applications also connects to this database. The upgrade program includes these details in the User Application configuration file.

     Database Platform

     Represents the platform of the User Application database.

     Database Host

     Specifies the name or IP address of the server that hosts the User Application.

     Database Port

     Specifies the port that the database server uses for communication with the User Application.

Database Driver JAR File

Specifies jar file for the database platform.

The database vendor provides the driver JAR file, which represents the jar for the database server. For example, for PostgreSQL, you might specify `postgresql-9.4-1212.jdbc42.jar`, by default in `C:\NetIQ\idm\apps\postgres`. Similarly, specify the appropriate jar files for your database platform.

- **(Conditional) Reporting Database Connection**

  Represents the settings for connecting to the Identity Reporting database.

  Database Host

  Specifies the name or IP address of the server that hosts the User Application.

  Database Port

  Specifies the port that the database server uses for communication with the User Application.

  Database Name

  Specifies the name of the database. By default, the database name is `idmrptdb`.

- **(Conditional) Reporting Database Credentials**

  Reporting Database User

  Specifies the name of an account that allows the User Application to access and modify data in the databases. By default, the database username is `postgres`.

  Reporting Database Password

  Specifies the password for the specified username.

  Upgrade Reporting Database

  Upgrade Database Now: The upgrade program updates the schema for the reporting database tables as part of the upgrade process.

  Upgrade Database at Application Startup: The upgrade program leaves instructions to update the schema for the database tables when the User Application starts for the first time after the upgrade.

  Write SQL to File: Generates a SQL script that the database administrator can run to update the databases. If you choose this option, you must also specify a name for **Schema File**. The setting is in the **SQL Output** File configuration.You might select this option if you do not have permissions to create or modify a database in your environment. For more information about generating the tables with the file, see “Manually Creating the Database Schema” on page 151.

  Database Driver JAR File

  Specifies jar file for the database platform.

  The database vendor provides the driver JAR file, which represents the jar for the database server. For example, for PostgreSQL, you might specify `postgresql-9.4-1212.jdbc42.jar`, by default in `C:\NetIQ\idm\apps\postgres`. Similarly, specify the appropriate jar files for your database platform.

- **Upgrade Database**

  Upgrade Database Now

  The upgrade program updates the schema for the database tables as part of the upgrade process.

Upgrade Database at Application Startup

The upgrade program leaves instructions to update the schema for the database tables when the User Application starts for the first time after the upgrade.

Write SQL to File

Generates a SQL script that the database administrator can run to update the databases. If you choose this option, you must also specify a name for **Schema File**. The setting is in the **SQL Output** File configuration.You might select this option if you do not have permissions to create or modify a database in your environment. For more information about generating the tables with the file, see "Manually Creating the Database Schema" on page 151.

- **Database Administrator**

  Represents the name and password for the database administrator.

  Database Username

  Specifies the account for a database administrator that can create database tables, views, and other artifacts.

  Password

  Specifies the password for the database administrator.

- **Reporting Database Connection**

  Represents the host name and password for the database administrator.

  Database Username

  Specifies the account for a database administrator that can create database tables, views, and other artifacts.

  Password

  Specifies the password for the database administrator.

10. Review the **Pre-Upgrade Summary** page, then click **Install**.

    The upgrade process stops the Tomcat service and starts the upgrade, which might take some time to complete.

11. When the upgrade process completes, review the upgrade log files from `/tmp/rbpm_upgrade/`and you need to update few configurations manually, see "Post-Upgrade Tasks" on page 275.

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

After upgrading Identity Applications, ensure you perform the following:

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 275
- "Tomcat" on page 275
- "Identity Applications" on page 276
- "One SSO Provider" on page 277
- "Self-Service Password Reset" on page 277
- "Kerberos" on page 277

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 Cerificate_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 Verify JRE home location is `tomcat\bin\setenv.bat`.

3 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

```
<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

```
<Connector port="8543" 
protocol="org.apache.coyote.http11.Http11NioProtocol"
       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

Restore the customized identity applications configurations from the backup taken during the upgrade process.

If you are upgrading Identity Manager from 4.5.6 version, you must manually create the compound indexes for each attribute that you want to use to sort users in Identity Manager Dashboard, see "Creating Compound Indexes" on page 143.

1 Launch the configupdate utility (`configupdate.bat`) file.

  In the `configupdate.bat.properties` file, ensure that the `use_console` value is set to `false`.

2. Connect to Identity Vault server and accept the eDirectory certificate.
3. In the **SSO Clients** tab, navigate to **RBPM** and click **Show Advanced Options**.
4. Set the **RBPM to eDirectory SAML configuration** to Auto.

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 "Self Service Password Reset" on page 181 in the "SSO Clients Parameters" on page 178.

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 sever 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 Tasks" on page 111.

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 **4.7.0**.

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 the driver package for the Data Collection Services.
2. Upgrade the driver package for the Managed System Gateway Service.
3. Migrate to Sentinel Log Management for IGA.
4. Upgrade Identity Reporting.

Upgrading the Driver Packages for Identity Reporting

This section explains how to update the packages for the Managed System Gateway and Data Collection Service drivers to the latest version. You must perform this task before upgrading Identity Reporting.

1. In Designer, open your current project.
2. Right-click **Package Catalog > Import Package**.
3. Select the appropriate package. For example, **Manage System Gateway Base package 2.0.0.20120509205929**.
4. Click **OK**.
5. In the Developer View, right-click the driver and then click **Properties**.
6. Navigate to the **Packages** tab in the **Properties** page.
7. Click the **Add package (+)** symbol in the top right corner.
8. Select the package, and then click **OK**.
9. Complete the configuration process for the driver. For more information, see the following sections:
   - "Configuring the Managed System Gateway Driver" on page 202
   - "Configuring the Driver for Data Collection Service" on page 203
10. Repeat Step 2 through Step 9 to upgrade the package for the Data Collection Service Driver.
11. Ensure that the Managed System Gateway Driver and Data Collection Service Driver are connected to the upgraded Identity Manager.

Upgrading Identity Reporting

Before upgrading Identity Reporting, you must upgrade the identity applications and SLM for IGA. To upgrade Identity Reporting from version 4.0.2 or later, install the new version on top of the older version. For more information, see "Installing Identity Reporting" on page 189.

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 `analyzer_4.6_patch1_20121128.zip`, 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 280
- "Starting the Drivers" on page 281

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 280
- "Using iManager to Stop the Drivers" on page 280

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 281
- "Using iManager to Start the Drivers" on page 281

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 “Managing Packages” in the *NetIQ Designer for Identity Manager Administration Guide*.

NOTE: If you upgrade the 3.*x* version of the User Application driver to the User Application version 4.0.2 package, Designer installs both 3.*x* and 4.0 versions of the same driver policies. Having both 3.*x* and 4.0 policies within the package catalog might cause Designer to not function properly. Delete the version 3.*x* policies and retain the version 4.0 policies.

You can upgrade your drivers to packages in the following ways:

- “Creating a New Driver” on page 282
- “Replacing Existing Content with Content from Packages” on page 283
- “Keeping the Current Content and Adding New Content with Packages” on page 283

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 266.

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 256.
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.

   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 285.

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 256.

   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 307. If you are using iManager, complete the following procedure:

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 **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 284
- "Using iManager to Remove the Old Server from the Driver Set" on page 285
- "Decommissioning the Old Server" on page 285

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 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 **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 285
- “Using iManager to Restore Custom Policies and Rules to the Driver” on page 286

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.

23 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 `<install folder>/tomcat/conf` directory to a backup directory.
8. Install Identity Reporting from the Identity Manager 4.6 media.
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

- 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://192.99.17.22:8180/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://192.99.179.202:8180/sspr/public/oauth`

For more information about Configuration Utility, see "Running the Identity Applications Configuration Utility" on page 162.

10 Save the changes and exit the Configuration Utility.

11 Start Tomcat.

VIII Deploying Identity Manager on Microsoft Azure

This section explains the planning and implementation of Identity Manager on the Microsoft Azure cloud.

24 Planning and Implementation of Identity Manager on Microsoft Azure

Identity Manager adds support for deploying the following Identity Manager components on Microsoft Azure.

- Identity Vault
- 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

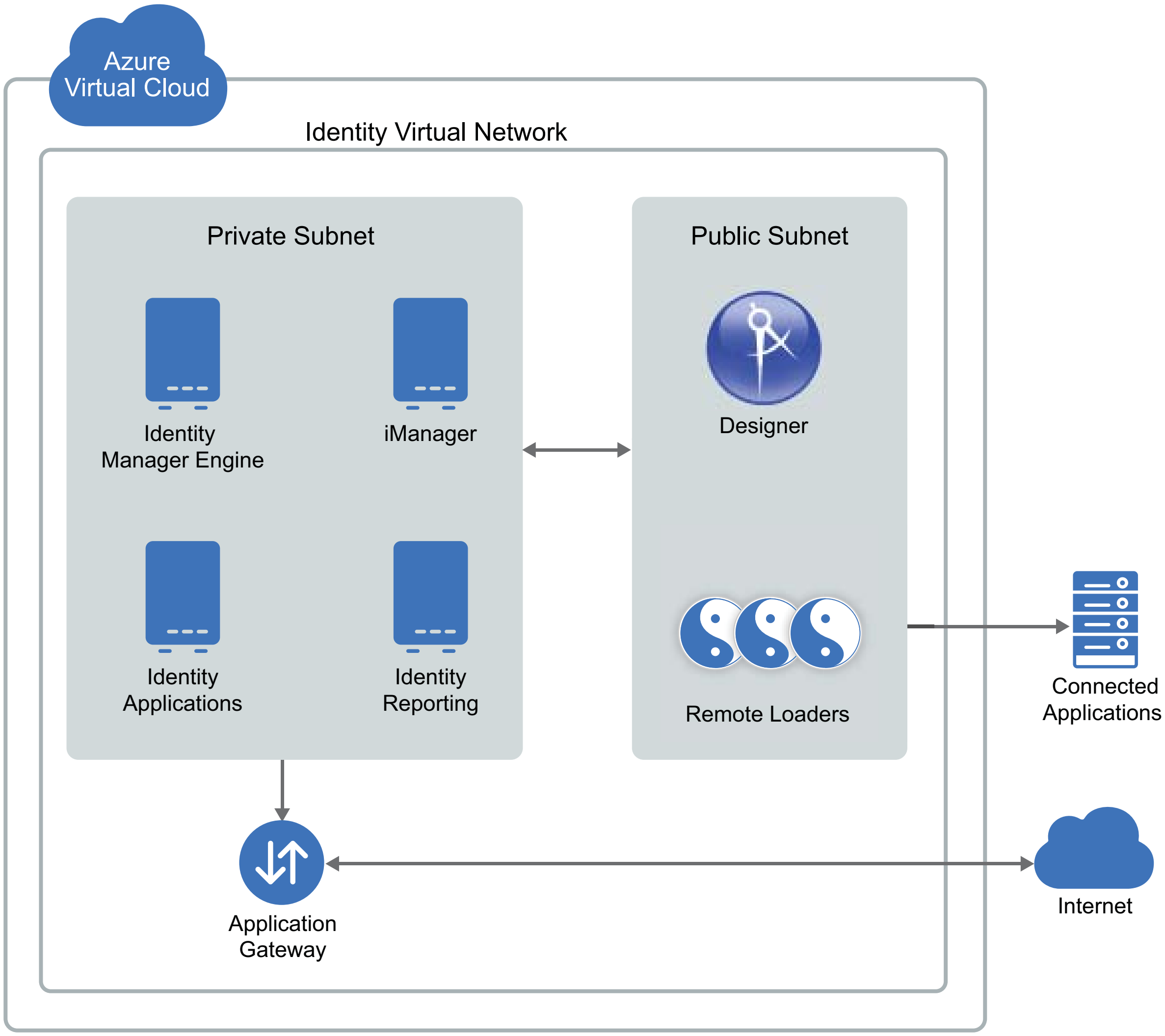
In addition to the system requirements of Identity Manager components, ensure that you meet the following prerequisites:

- An administrative account on Microsoft Azure.
- `Identity_Manager_4.7_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 24-1, “Identity Manager Deployment on Microsoft Azure,” on page 292 illustrates a sample deployment that is used in the subsequent sections.

Figure 24-1 Identity Manager Deployment on Microsoft Azure



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 293
- "Creating a Virtual Network and Subnet" on page 293
- "Creating an Application Gateway" on page 293
- "Creating a Virtual Machine Instance" on page 294
- "Setting Up Designer" on page 295
- "Configuring the Application Gateway" on page 295

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 or determine an existing resource group:

1. Log in to the Azure portal as an `administrator`.
2. Click **New**.
3. Search for resource group and select the resource group.
4. Click **Create**.

Creating a Virtual Network and Subnet

1. In the Azure portal, click **New**.
2. Search for `virtual network` and select **Virtual Network**.
3. Click **Create**.
4. Configure the required network settings, such as Name, Subscription, Location, Address Space, Resource Group, Subnet name, and Subnet address range.

   The following is an example configuration:

   Name: IDM-subnet1

   Address space: 10.10.10.0/24

   Resource group: Use the existing resource group which is already created. See, "Creating a Resource Group" on page 293.

   Subnet name: default

   Subnet address range: 10.10.10.0/24
5. Click **Create**.

Creating an Application Gateway

1. In the left menu, click **Create a resource**.
2. Select **Networking > Application Gateway**.
3. In **Basics**, specify the basic details to create an application gateway:

   3a Specify the required gateway settings, such as Name, Standard Tier and SKU size, Instance count, Resource Group, Subscription, Location.

   The following is an example configuration:

   Name: Identity Applications Gateway

   Standard Tier and SKU size: Medium

   Instance count: default

   Resource group: Use the existing resource group which is already created. See, "Creating a Resource Group" on page 293.

   Subnet name: default

   3b Click **OK**.

4 In **Settings**, specify the application gateway network related details:

4a Select the virtual network and corresponding subnet which is created earlier. See, "Creating a Virtual Network and Subnet" on page 293.

4b In **Frontend IP configuration**, select **Public > Create new Public IP address**.

4c Specify the DNS name to access the VMs from an external network through the application gateway.

4d In **Listener configuration**, select the following options:

Field	Description
Protocol	HTTPS
Port	8443

5 In **Summary**, review your settings and click **Create**.

Creating a Virtual Machine Instance

Create a separate virtual machine to host Identity Manager components.

1 In the left menu, click **Create a resource** and select **Compute**.

2 Click **Windows Server > Windows server 2016 Datacenter**.

3 In **Deployment Model**, select **Resource Manager** and click **Create**.

4 Configure the following settings:

Field	Description
Name	Specify the VM name.
VM disk type	Select the disk type. For example SSD.
Username and **Password**	Specify the preferred username and password.
Subscription	Select your subscription.
Resource Group	Select the existing resource group. See "Creating a Resource Group" on page 293.
Location	Specify location where this VM should host the application.

5 Click **OK**.

6 In **High Availability and Storage**, retain the default settings.

7 In **Network**, select the virtual network and corresponding subnet that is already created. See, "Creating a Virtual Network and Subnet" on page 293.

8 (Conditional) If you want to access the virtual machine outside of the virtual network, select a public IP address for your virtual machine.

9 Specify the firewall rules for your Network security group to control incoming and outgoing requests of your virtual machine.

These firewall rules are required if you want to access the virtual machine from an external network.

10 Retain the default values for the rest of the options and click **OK**.

11 In **Summary**, review your settings and click **Create the VM**.

To host the following Identity Manager Components on the respective VMs, see:

- Installing Identity Manager Engine
- Installing Identity Applications
- Installing Identity Reporting

Setting Up Designer

1 On a public subnet, launch a Virtual Machine instance. See, "Creating a Virtual Machine Instance" on page 294.

For the Windows security group, use `rdesktop` port only. For example 3389

2 Install Designer. See, Installing Designer.

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, and Identity Reporting.

1a In **Backend pools**, click **Add**.

1b Specify the following details:

Field	Description
Name	Specify the name of a backend pool to identify the Identity Manager component.
Type	Specify the type in one of the following ways: ◆ **IP address or FQDN:** Specify the IP address or FQDN of the required Identity Manager component. ◆ **Virtual Machine:** Select the Virtual Machine that is hosting the required Identity Manager component.

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, 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:

Field	Description
Name	Specify the name of an HTTP setting to identify the Identity Manager component.
Protocol	Select HTTPS.
Port	Specify the port of the Identity Manager Component. For example: ◆ **iManager:** 8443 ◆ **Identity Applications:** 8543 ◆ **Identity Reporting:** 8643
Backend Authentication Certificates	1. Select Create new. 2. Specify the name of the certificate. 3. Browse and upload the exported public certificate for the corresponding Identity Manager component. 4. Click Add Certificate.

2c Click **OK**.

Repeat this step to configure additional HTTP settings.

3 Configure a separate listener for each Identity Manager component such as iManager, Identity Applications, and Identity Reporting.

3a In **Listeners**, click **Basic**.

3b Specify the following details:

Field	Description
Name	Specify the name of the listener to identify the Identity Manager component.
Frontend IP configuration	1. Select the Virtual Network and subnet that is created earlier. See, "Creating a Virtual Network and Subnet" on page 293. 2. Specify the Name and Port number of the application. For example: **iManager:** 8443 **Identity Applications:** 8543 **Identity Reporting:** 8643
Protocol	Select HTTPS.
Certificate	1. Browse and upload the PFX certificate. 2. Specify the Name and Password of the certificate.

3c Click OK.

Repeat this step to configure additional listeners.

4 Create a basic rule for Identity Manager components such as iManager, Identity Applications, 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:

Field	Description
Name	Specify the name of a rule that helps in identifying the Identity Manager component.
Listener	Select the respective listener that is created in Step 3.
Backend Pool	Select the respective backend pool that is created in Step 1.
HTTP setting	Select the respective HTTP setting that is created in Step 2.

4c Click OK.

Repeat this step to configure additional rules.

25 Example Scenarios of Hybrid Identity Manager

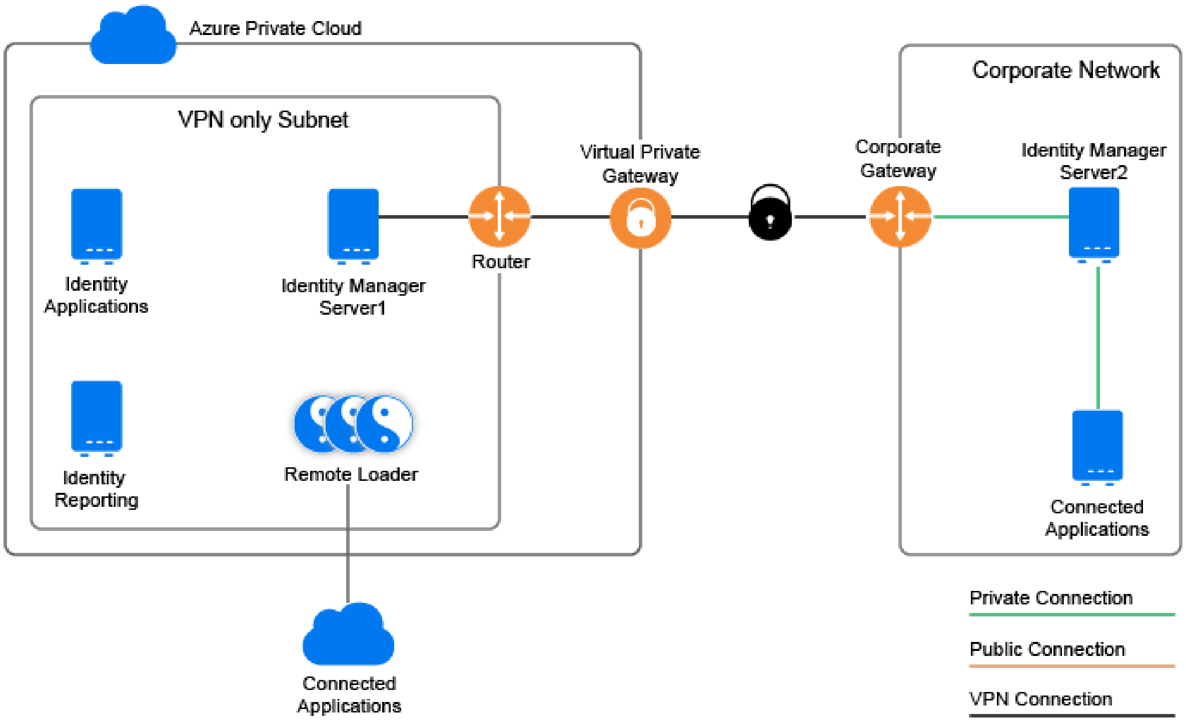
You can configure Identity Manager components where the identities are synchronized seamlessly between your enterprise premise and MS Azure cloud. Implementing this type of a hybrid scenario requires you to configure a VPN connection between the Azure subnet and the enterprise network. This section explains the following hybrid scenarios:

- "Using Multi-Server Driver Set Connection" on page 299
- "Using eDirectory Driver Connection" on page 300

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.

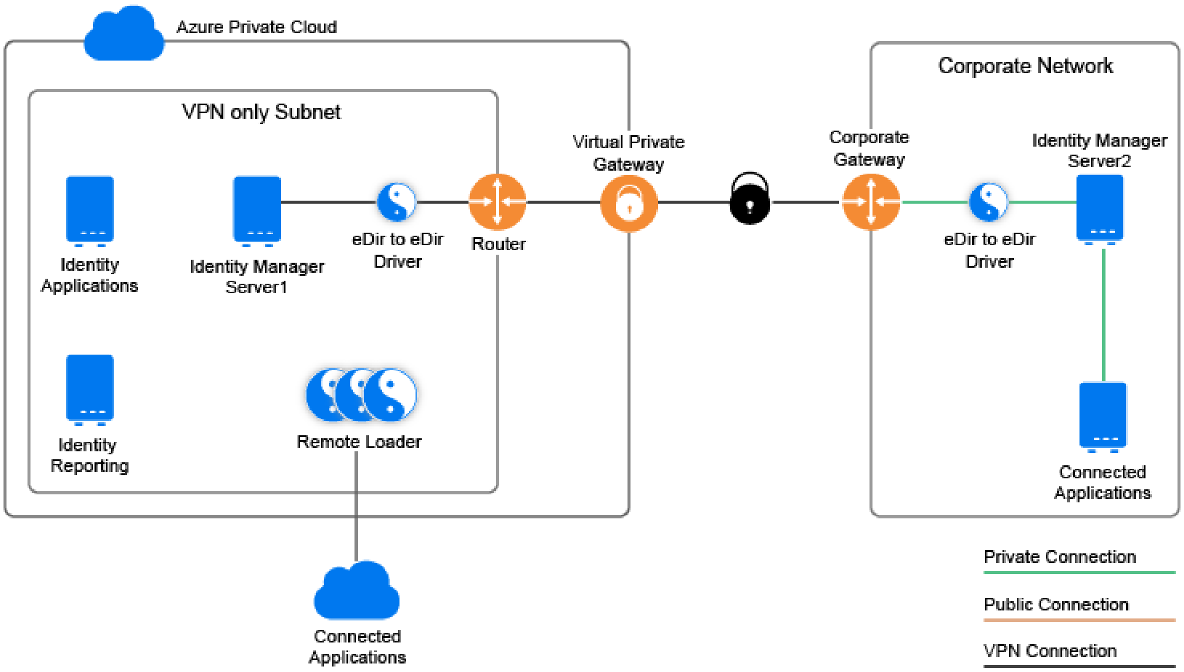
Figure 25-1 *Hybrid Scenario Using Multi-Sever Driver Set Connection*



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 25-2 *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.

IX 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 VII, “Upgrading Identity Manager,” on page 245. For more information about the difference between upgrade and migration, see “Understanding Upgrade and Migration” on page 249.

26 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.

	Checklist Items
□	1. Ensure that you have the latest installation kit to migrate your Identity Manager data.
□	2. Ensure that your computers meet the hardware and software prerequisites for a newer version of Identity Manager. For more information, see Preparing to Migrate Identity Manager, Considerations for Installing Identity Manager Components, and the Release Notes for the version to which you want to upgrade.
□	3. Upgrade eDirectory to the latest supported version for the Identity Vault. For more information, see “Prerequisites and Considerations for Installing the Identity Vault” on page 32.
□	4. Add the eDirectory replicas that are on the current Identity Manager server to the new server. For more information, see Section 27, “Migrating Identity Manager to a New Server,” on page 305.
□	5. Install Identity Manager on the new server. For more information, see “Planning to Install Identity Manager” on page 17.
□	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 263.
□	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 305.
□	8. Add the new server to the driver set. For more information, see “Adding the New Server to the Driver Set” on page 284.
□	9. Change the server-specific information for each driver. For more information, see “Copying the Server-specific Information in Designer” on page 307.
□	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 307
□	11. Update your drivers to the package format. For more information, see “Upgrading the Identity Manager Drivers” on page 282.

	Checklist Items
❑	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 285.
❑	13. Remove the old server from the driver set. For more information, see “Removing the Old Server from the Driver Set” on page 284.
❑	14. Activate your upgraded Identity Manager solution. For more information, see “Activating Identity Manager” on page 243.

27 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

NetIQ recommends that you complete the steps in the following checklist.

	Checklist Items
□	1. Back up the directories and databases of your Identity Manager solution.
□	2. Ensure that you have installed the latest versions of the Identity Manager components, except for the identity applications. For more information, see "Recommended Installation Scenarios and Server Setup" on page 21 and the latest release notes for the components. **NOTE:** To continue using your current User Application database, specify **Existing Database** in the installation program. For more information, see Chapter 11, "Installing Identity Applications," on page 115.
□	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 306.
□	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 308.
□	7. Create a new Designer project in the latest version of Designer, then import the User Application driver to prepare for migration.

	Checklist Items
❑	8. Migrate the User Application driver. For more information, see "Migrating the User Application Driver" on page 309.
❑	9. Create a new Role and Resource Service driver. You cannot migrate an existing Role and Resource Service driver. For more information, see "Creating the Role and Resource Service Driver" on page 148.
❑	10. Deploy the two drivers to the Identity Vault. For more information, see "Deploying the Drivers for the User Application" on page 149.
❑	11. Upgrade the Identity Applications. For more information, see "Upgrading Identity Applications and Identity Reporting" on page 267.
❑	12. 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 312.
❑	13. (Conditional) Reinstate your custom settings for the SharedPagePortlet. For more information, see "Updating the Maximum Timeout Setting for the SharedPagePortlet" on page 312.
❑	14. 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 312.

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.

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 307
- "Changing the Server-specific Information in iManager" on page 308
- "Changing the Server-specific Information for the User Application" on page 308

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 161.

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.

For more information, see Part II, “Installing Identity Manager Engine,” on page 29.

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.

3b Navigate to `*designer_root*/packages/eclipse/plugins/NOVLUABASE_*version_of_latest_package*.jar`.

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.
- Understand the differences in the providers for managing passwords. SSPR is the default provider. To use Identity Manager’s legacy provider or an external provider, you must update the configuration of the identity applications after the upgrade. For more information, see “Using Self-Service Password Management in Identity Manager” on page 24.

For more information about upgrading the Identity Applications, see “Upgrading Identity Applications and Identity Reporting” on page 267.

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:

   ```
   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:

   ```
   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

   ```
     -- 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 151.

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.

Using the Legacy Provider or an External Provider for Managing Passwords

By default, Identity Manager uses SSPR for password management. However, to use your existing password policies, you might want to use Identity Manager's internal legacy provider. Alternatively, you can use an external provider. For more information about configuring Identity Manager for these providers, see one of the following sections:

- "Using the Legacy Provider for Forgotten Password Management" on page 158
- "Using an External System for Forgotten Password Management" on page 159

Updating the Maximum Timeout Setting for the SharedPagePortlet

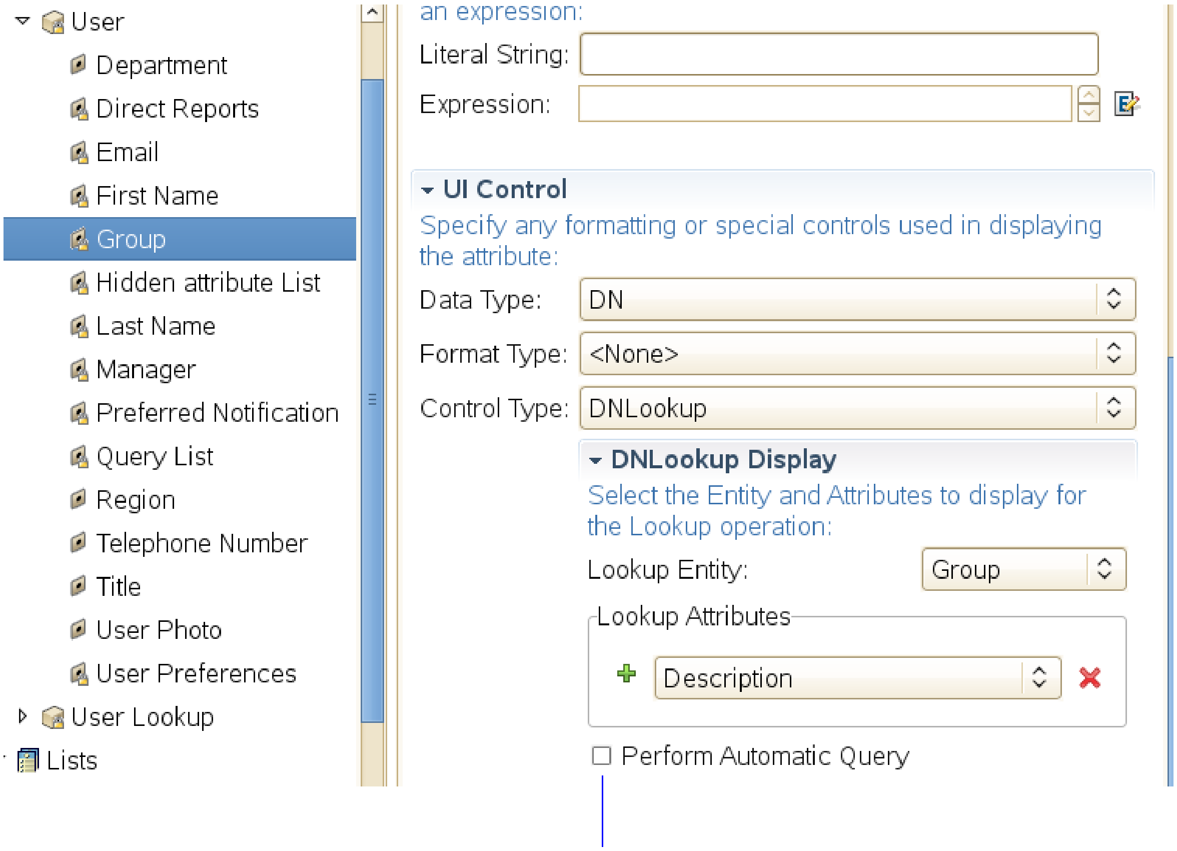
If you have customized any of the default settings or preferences for the SharedPagePortlet, then it has been saved to your database and this setting will get overwritten. As a result, navigating to the Identity Self-Service tab might not always highlight the correct Shared Page. To be sure that you 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:



an expression:

Literal String:

Expression:

UI Control

Specify any formatting or special controls used in displaying the attribute:

Data Type: DN

Format Type: <None>

Control Type: DNLookup

DNLookup Display

Select the Entity and Attributes to display for the Lookup operation:

Lookup Entity: Group

Lookup Attributes

Description

☐ Perform Automatic Query

uncheck this if you don't want the autoquery to occur

28 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.
3. Select **Partitions and Replica > Merge Partition**.
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 316.

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 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 316.

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 318.
2. Delete Identity Reporting. For more information, see “Uninstalling Identity Reporting” on page 318.
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 318.

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**.

29 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 the User Application 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.

Issue	Suggested Actions

The upgrade process does not set the default User Application Administrative account as `cn=uaadmin.ou=sa.o=data`. The following error is logged to the catalina.out file.
`AuthorizationManagerService [RBPM] Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.com.novell.srvprv.spi.security.IDMAuthorizationException: Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.at com.novell.idm.security.authorization.ldap.LdapRightsUtil.getPropertyRights(LdapRightsUtil.java:152)`
`Unable to fetch roles from edirectory in the predefined time set.`
	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.

Issue	Suggested Actions
You want to modify one or more of the following the User Application 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`
Starting Tomcat causes the following exception: `port 8180 already in use`	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.
When Tomcat starts, the application reports it cannot find trusted certificates.	Ensure that you start Tomcat by using the JDK specified during the installation of the User Application.
Cannot log in to the portal admin page.	Ensure that the User Application Administrator account exists. This account is not the same as your iManager administrator account.
Cannot create new users even with administrator account.	The User Application Administrator must be a trustee of the top container and should have Supervisor rights. You can try setting the User Application Administrator’s rights equivalent to the LDAP Administrator’s rights (using iManager).
Starting application server throws keystore errors.	Your application server is not using the JDK specified during the installation of the User Application. Use the `keytool` command to import the certificate file: `keytool -import -trustcacerts -alias` *`aliasName`* `-file` *`certFile`* `-keystore ..\lib\security\cacerts -storepass changeit` - Replace *aliasName* with a unique name of your choice for this certificate. - Replace *certFile* with the full path and name of your certificate file. - The default keystore password is `changeit` (if you have a different password, specify it).

Issue	Suggested Actions
Email notification not sent.	Run the `configupdate` utility to check whether you supplied values for the following User Application configuration parameters: **Email From** and **Email Host**. Run the following command from the installation directory (by default, `C:\NetIQ\idm\apps\UserApplication\`): `configupdate.bat`

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.

Issue	Suggested Actions
Uninstallation process reports as incomplete but the log file shows no failures.	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.

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.

Issue	Suggested Actions
When Identity Applications and Identity Reporting are installed on the same server and you perform configuration changes using the configuration update utility located at `<reporting install folder>\bin` directory, the Identity Manager Dashboard fails to launch. The following error is reported in `catalina.out` log file for Tomcat: `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.`	For any configuration changes, use the configuration update utility located at `C:\NetIQ\idm\apps\UserApplication` directory.
User is unable to login in large scale environment (>2 million objects)	Add an index for `mail (Internet Mail Address)` attribute with the rule set as `Value` in both eDirectory master and replica servers.
When you sign out from Identity Applications page, SSPR shows an error `5053 ERROR_APP_UNAVALIABLE`.	Ignore this error. It does not cause any functionality loss.

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.

Issue	Suggested Actions
SSPR Reports Out of Order Page Request Error This issue occurs when you click the **Back** button while in an SSPR page. SSPR displays an incorrect sequence message in the SSPR error log similar to the following: `ERROR, password.pwm.servlet.TopServlet, 5035 ERROR_INCORRECT_REQUEST_SEQUENCE (expectedPageID=3, submittedPageID=4, url=<some sspr url>`	Disable the Back button detection from **SSPR Configuration Manager > Settings > Security > Web Security**. **NOTE:** Changing this setting has no effect on end users.

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.

Issue	Suggested Actions
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.	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.

X Deploying Identity Manager for High Availability

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.

For more information about...	See...
Determining the server configuration for Identity Manager components	see High Availability Configuration in *NetIQ Identity Manager Overview and Planning Guide*.
Running the Identity Vault in a cluster	Sample Identity Manager Cluster Deployment Solution Deploying eDirectory on High Availability Clusters in the *NetIQ eDirectory Installation Guide*.
Running the identity applications in a cluster	Sample Identity Applications Cluster Deployment Solution

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 30, “Preparing for Installing Identity Manager in a Cluster Environment,” on page 329
- Chapter 31, “Sample Identity Manager Cluster Deployment Solution,” on page 333
- Chapter 32, “Sample Identity Applications Cluster Deployment Solution,” on page 335

30 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 log ins 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 331
- "Setting System Properties for Workflow Engine IDs" on page 331
- "Using the Same Master Key for Each User Application in the Cluster" on page 332

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.

For more information about prerequisites for installing in a cluster environment, see "Prerequisites and Considerations for Installing the Identity Applications" on page 117.

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 creating the master key, see **Security - Master Key** in Step 6 on page 128. 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.

31 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 2012 R2 platform.

Prerequisites

eDirectory 8.8.8 SP9 or 9.0.2 or later services are running in a cluster environment on Windows 2012 R2. For detailed information about setting up an eDirectory cluster, see Clustering eDirectory Services on Windows in the *NetIQ eDirectory Installation Guide*.

NOTE: eDirectory 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.

32 Sample Identity Applications Cluster Deployment Solution

The section provides instructions on how to configure the identity applications into a cluster environment on the Tomcat application server with an example deployment.

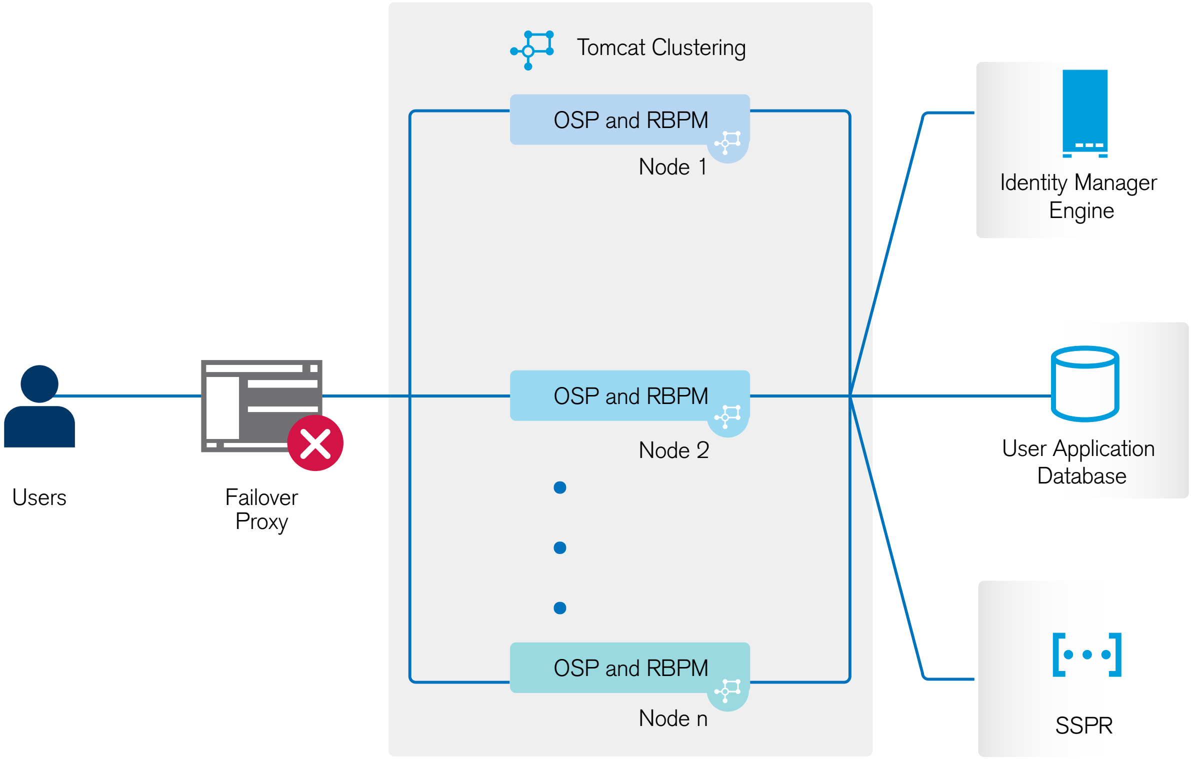
Clustering allows you to run the identity applications on several parallel servers (cluster nodes) and allows you to achieve high availability. To build a cluster, you need to group several Tomcat instances (nodes) together. The load is distributed across different servers, and even if any of the servers 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 32-1 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 337.
- 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 4.7 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.

Figure 32-1 Sample cluster deployment solution



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

- Two servers running Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 for nodes.
- Identity Manager components installed with a minimum version of 4.7. For upgrading to Identity Manager 4.7, see Chapter 22, "Upgrading Identity Manager Components," on page 259.
- 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.

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 Chapter 5, “Installing the Engine, Drivers, and iManager Plug-ins,” on page 59. For a production-level deployment, it is recommended to install Identity Manager engine on a separate server.
2. Install PostgreSQL. For step-by-step instructions, see “Installing PostgreSQL and Tomcat” on page 92. For a production-level deployment, it is recommended to install PostgreSQL on a separate server.
3. Create and deploy the following drivers for the Identity Applications:
    - User Application driver
    - Roles and Resource Service driver

    For step-by-step instructions, see “Creating and Deploying the Drivers for the Identity Applications” on page 147.
4. On Node1, install the following Identity Manager components:
    a. Tomcat

    Install Tomcat by using the convenience installer and select only Tomcat during the installation process. For step-by-step instructions, see “Installing PostgreSQL and Tomcat” on page 92.

    b. OSP

    For more information about installing OSP, see “Installing Password Management for Identity Manager” on page 107.

    During the installation process, provide the IP address and port number of the Identity Manager engine (eDirectory) server in the Authentication details page.

    c. 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 4.7 supported databases.

    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: If you are using other Identity Manager 4.7 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. For more information, see “Configuring the Database for the Identity Applications” on page 123.

    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.

NOTE: For detailed instructions and more information to install the User Application, see "Installing the Identity Applications" on page 127.

---

5. On Node2, perform the following actions:

   a. Install Tomcat by using the convenience installer (select only Tomcat during the installation process).

      For step-by-step instructions, see "Installing PostgreSQL and Tomcat" on page 92.

   b. Install OSP.

      For more information on installing OSP, see "Installing Password Management for Identity Manager" on page 107.

      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 4.7 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 4.7 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. For more information, see"Configuring the Database for the Identity Applications" on page 123.

      ---

      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 `/TOMCAT_INSTALLED_HOME/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 User Application, see "Installing the Identity Applications" on page 127.

---

6. In load balancer server, start an instance of load balancer with Identity Applications port number. For example,

```
./balance 8543 node.47app1.novell.com:8543 !
```

7. 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. Update the SSPR information on Node1 by launching 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.

c. 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`.

d. After completing the SSPR installation, launch SSPR (`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:

```
http:<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.

NOTE: Verify that the values for these parameters are updated in Node2.

8. 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 161.

   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.

9. 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>"
   ```

   For example: `C:\NetIQ\Common\JRE\bin\keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"`

   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.

10. (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
    ```

11. 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 9.

12. Copy the new `osp.jks` file located at from Node1 to other User Application nodes in the cluster.

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.

    b. To reflect this change in all other nodes of the cluster, copy the `ism-configuration properties` file located in `/TOMCAT_INSTALLED_HOME/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 **Administration** tab.

       The User Application displays the Application Configuration portal.
    d. Click **Caching**.

       The User Application displays the Caching Management page.
    e. Select **True** for the **Cluster Enabled** property.
    f. Click **Save**.
    g. 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 344.
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:

    ```
    <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. For more information see "Configuring the User Application Driver for Clustering" on page 345.

20. To change the URL of Roles and Resource Service Driver, repeat steps in the procedure "Configuring the User Application Driver for Clustering" on page 345 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.

22. Import the User application certificate to the iManager certificate path: `/opt/netiq/common/jre/lib/security/cacerts` using the following keytool command:

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

    This step allows you to view the running PRDs or move a PRD from one node to the other node in a cluster through iManager.

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
```

Configuring OSP and SSPR for Clustering

Identity Manager supports SSPR configuration in a Tomcat cluster environment.

Configuring SSPR to Support Clustering

Perform the following steps to configure SSPR that already exists on a separate computer:

1. Review the prerequisites and system requirements in "Checklist for Installing Password Management Components" on page 105.

2. Follow the instructions from "Using the Wizard to Install Self Service Password Request" on page 107 and ensure the following steps are considered during the installation process.

    a. 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.

    b. 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, update the SSL settings. For more information, and Updating the SSL Settings for Self Service Password Reset in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

3. To update the SSPR information in the first node of the cluster, launch the Configuration utility from `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.

Configuring Tasks on Cluster nodes

Perform the following configuration tasks on the cluster nodes:

1 To update the Forgotten Password link with the SSPR IP address, log in to the User Application on the first node and click **Administration** > **Forgot Password**.

For more information on SSPR configuration, see "Configuring Forgotten Password Management" on page 156.

2 To change the Change my password link, see "Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment" on page 161.

3 Verify that the Forgot Password link and Change my password links are updated with the SSPR IP address on the other nodes in the cluster.

NOTE: If the Change Password and Forgot Password links are already updated with the SSPR IP address, no changes are required.

4 In the first node, 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\idm\apps\jre\bin\keytool -genkey -keyalg RSA -keysize 2048 -
keystore osp.jks -storepass <password> -keypass <password> -alias osp -
validity 1800 -dname "cn=<loadbalancer IP/DNS>"
```

For example : `C:NetIQ\idm\apps\jre\bin\keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"`

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.

5 (Conditional) To verify if the `osp.jks` file is updated with the changes, run the following command:

```
C:NetIQ\idm\apps\jre\bin\keytool -list -v -keystore osp.jks -storepass
changeit
```

6 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 3.

7 Copy the new `osp.jks` file located at `C:\NetIQ\idm\apps\osp\` from the first node to all other User Application nodes in the cluster.

8 Launch the Configuration utility in the first node 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.

8a Save the changes in the Configuration utility.

8b To reflect this change in all other nodes of the cluster, copy the `ism-configuration properties` file located in `\TOMCAT_INSTALLED_HOME\conf` from the first node to all other User Application nodes.

NOTE: You copied the `ism.properties` file from the first node to the other nodes in the cluster. If you specified custom installation paths during 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 load balancer. Do this for all the servers where OSP is installed. 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.

9 Perform the following actions in the `setenv.bat` file in the `\TOMCAT_INSTALLED_HOME\bin\` directory:

9a 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.bat` file in all nodes.

9b Add "-Dcom.novell.afw.wf.Engine-id=Engine" in the `setenv.bat` file in the first node.

The engine name should be unique. Provide the name that was given during the installation of the first node. The default name is "Engine" in case no name was specified.

Similarly, add a unique engine name for other nodes in the cluster. For example, for second node, the engine name can be Engine2.

10 Enable clustering in the User Application. For more information see, Step 10 on page 147.

11 Enable the permission index for clustering. For more information see, "Enabling the Permission Index for Clustering" on page 344.

12 Enable Tomcat cluster. For more information see, Step 9 in "Preparing Your Environment for the Identity Applications" on page 125.

13 Restart Tomcat on all nodes.

14 Configure the User Application driver for clustering. For more information see "Configuring the User Application Driver for Clustering" on page 345.

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:

```
<property>
<key>com.netiq.idm.cis.clustered</key>
<value>true</value>
</property>
```

5. Click **OK.**
6. Click **Apply** > **OK**.

Configuring 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.

1 Log in to the instance of iManager that manages your Identity Vault.

2 In the navigation frame, select **Identity Manager**.

3 Select **Identity Manager Overview**.

4 Use the search page to display the Identity Manager Overview for the driver set that contains your User Application driver.

5 Click the round status indicator in the upper right corner of the driver icon:

6 Select **Edit Properties**.

7 For **Driver Parameters**, change **Host** to the host name or IP address of the Load balancer.

8 Click **OK**.

A Configuring a Multi-Server Environment

After installing the Identity Vault, you can configure the directory and use the DHost utility create, start, and stop server instances. You can also configure the Identity Vault to work with IPv6 addresses, if your server already supports IPv6 addressing.

Modifying the eDirectory Tree and Replica Server

After installing the Identity Vault, you can use the DHost utility to configure the Identity Vault. You must have Administrator rights to use the DHost utility. When you use this utility with arguments, it validates all arguments and prompts for the password of the user having Administrator rights. If you use the utility without arguments, ndsconfig displays a description of the utility and available options.

You can also use this utility to remove the eDirectory Replica Server and change the current configuration of eDirectory Server. For more information, see "Configuring the Identity Vault after Installation" on page 51.

When you use the DHost utility, the following conditions apply:

- The maximum number of characters allowed for the `treename`, `admin_FDN`, and `server_FDN` variables are as follows:
  - `treename`: 32 characters
  - `admin_FDN`: 255 characters
  - `server_FDN`: 255 characters
- When you add a server to an existing tree and the context that you specify does not exist in the Server object, the DHost utility creates the context while adding the server.
- You can add LDAP and security services to the existing tree after installing the Identity Vault.
- To enable encrypted replication in the server, include the `-E` option in the commands for adding a server to an existing tree. For more information about encrypted replication, see "Encrypted Replication" in the *NetIQ eDirectory Administration Guide*.

For more information about using the DHost utility to modify eDirectory, see the *NetIQ eDirectory Administration Guide*.

Adding a New Tree to the Identity Vault

When you create a new tree in the Identity Vault, you can specify an IPv6 address for the new tree, if your Identity Vault server already supports IPv6 addresses.

Adding a Server to an Existing Tree

You can add a server to an existing tree by running the eDirectory installation program.

Removing the Identity Vault and its Database from the Server

1. Navigate to the `dsreports` directory.
2. Delete the HTML files that you previously created using iMonitor.

Removing an eDirectory Server Object and Directory Services from a Tree

Use DHost utility to remove the server object and directory services from a tree. For more information, see the *NetIQ eDirectory Administration Guide*.