
NetIQ® Identity Manager Security Guide

February 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/>.

Copyright (C) 2018 NetIQ Corporation. All rights reserved.

Contents

About this Book and the Library	5
About NetIQ Corporation	7
1 Security Best Practices	9
Using SSL	9
Securing Directory Access	9
Granting Task-Based Access to Drivers and Driver Sets	10
Understanding Identity Manager Communication	11
Managing Passwords	13
Creating Strong Password Policies	14
Securing ActiveMQ Communication	15
Configuring a Whitelist of Target URLs	15
Configuring a Whitelist of Target URLs in Identity Applications	15
Configuring a Whitelist of Target URLs in OSP	15
Preventing Clickjacking Attacks in Identity Manager	16
Rejecting Client-initiated SSL Renegotiation on Windows	18
Securing Connected Systems	18
Password Generation	18
Designer for Identity Manager	19
Industry Best Practices for Security	20
Tracking Changes to Sensitive Information	20
Using iManager to Log Events	20
Using Designer to Log Events	21
Establishing a Security Equivalent User	24

About this Book and the Library

The *Security Guide* provides information about security best practices you might want to implement in your Identity Manager environment.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

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
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

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

1 Security Best Practices

The following sections provide information you should consider as you secure your Identity Manager system:

- ♦ “Using SSL” on page 9
- ♦ “Securing Directory Access” on page 9
- ♦ “Understanding Identity Manager Communication” on page 11
- ♦ “Managing Passwords” on page 13
- ♦ “Creating Strong Password Policies” on page 14
- ♦ “Securing ActiveMQ Communication” on page 15
- ♦ “Configuring a Whitelist of Target URLs” on page 15
- ♦ “Preventing Clickjacking Attacks in Identity Manager” on page 16
- ♦ “Rejecting Client-initiated SSL Renegotiation on Windows” on page 18
- ♦ “Securing Connected Systems” on page 18
- ♦ “Designer for Identity Manager” on page 19
- ♦ “Industry Best Practices for Security” on page 20
- ♦ “Tracking Changes to Sensitive Information” on page 20
- ♦ “Establishing a Security Equivalent User” on page 24

Using SSL

Enable SSL for all transports, where it is available. Enable SSL for communication between the Identity Manager engine and Remote Loader and between the Identity Manager engine or Remote Loader and the connected systems. For information, see “[Creating a Secure Connection to the Identity Manager Engine](#)” in the *NetIQ Identity Manager Driver Administration Guide*.

If you don't enable SSL, you are sending sensitive information such as passwords in clear text.

Securing Directory Access

Make sure that you secure access to Identity Vaults and to Identity Manager objects.

Physical Security: Protect access to the physical location of the servers where an Identity Vault is installed.

File System Access: The security of the file system for Identity Manager is critical to ensuring the security of the system as a whole. Verify that the directories containing eDirectory, the Identity Manager engine, and the Remote Loader are accessible only to the appropriate administrators.

There is an issue with the file system when the Remote Loader is installed on a Windows 2000 server. For more information, see [TID 3243550, Securing a Remote Loader Install on a Microsoft Windows 2000 Server \(http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3243550&sliceId=SAL_Public&dialogID=47824778&stateId=0%20%2047832401\)](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3243550&sliceId=SAL_Public&dialogID=47824778&stateId=0%20%2047832401).

The Identity Manager files and directories have permissions that specify who and what can read, write, modify, and access them. This is important because Identity Manager may need access to write to files in your file system to enable certain functions.

The contains the minimum required permissions for different directories:

Table 1-1 Minimum File and Directory Permissions

Path	Directory	Minimum Permission Required
/var/opt/novell/	eDirectory	755
/var/opt/novell/	dirxml	750
/var/opt/novell/	iManager	750
/var/opt/novell/	idm	750

To see the permissions set for a file, open the command line and type: `ls -l`.

For security requirements, NetIQ recommends that you make a note of these permissions.

Access Rights: Identity Manager requires Administrative rights to create Identity Manager objects and configure drivers. Monitor and control who has rights to create or modify the following:

- ♦ An Identity Manager driver set
- ♦ An Identity Manager driver
- ♦ Driver configuration objects (filters, style sheets, policies), especially policies that are used for password retrieval or synchronization
- ♦ Password policy objects (and the iManager task for editing them), because they control which passwords are synchronized to each other, and which Password Self-Service options are used

Granting Task-Based Access to Drivers and Driver Sets

In addition to the eDirectory standard object-based access controls, Identity Manager lets you assign trustee rights to perform only certain tasks on an Identity Manager driver, rather than just granting full Supervisor rights to the driver object. For example, you can assign trustee rights so that one user can only configure the driver object (create and modify object properties), while another user can only start and stop the driver.

Identity Manager provides the following driver object attributes that enable role-based access:

Attribute	Description
DirXML-AccessRun	Start and stop Identity Manager drivers and jobs
DirXML-AccessMigrate	Manage migration operations into the Identity Vault
DirXML-AccessSubmitCommand	Manage the driver's pass-through commands
DirXML-AccessCheckObjectPassword	Manage the driver's check object password commands
DirXML-AccessConfigure	Manage the driver's configuration and job configuration
DirXML-AccessManage	View and modify the driver's cache file contents

Setting trustee rights to these attributes grants access to the associated Identity Manager verbs and sub-verbs. Read access lets users view state (get verb state), and Write access lets users modify or change state (set verb state.) For example, granting Read access to a driver object's DirXML-AccessRun attribute lets the user get the driver state (started or stopped.) Granting Write access lets the user set the driver state (change from started to stopped, or vice versa.)

The goal of providing this attribute-based access to driver tasks is to let you create well-defined administrative roles, perhaps using the eDirectory Administrative Role object, that let users perform certain management tasks without exposing all management functionality. Creating these roles can go beyond providing access to the DirXML-Access attributes described above and can include access rights to other attributes, as well as access to other Identity Manager objects. The following examples demonstrate the flexibility available for creating administrative roles:

Start/Stop Driver Admin: This administrative role lets the assigned user start and stop all drivers in a given driver set. It requires the following access rights:

- ◆ Browse rights to the Driver Set object
- ◆ Read and Write access, with inheritance, to the DirXML-AccessRun attribute of the Driver Set object

Driver Admin: This administrative role lets the assigned user manage a single Driver object. It requires the following access rights:

- ◆ Browse and Create rights to the Driver object
- ◆ Read and Write access to [All Attribute Rights] in the Driver object

NOTE: Make sure the rights are inherited so the driver Admin can also manage the driver's policy objects.

Information about using iManager to grant eDirectory access rights is available in the [iManager Administration Guide \(https://www.netiq.com/documentation/imanager-31/\)](https://www.netiq.com/documentation/imanager-31/).

Understanding Identity Manager Communication

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

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

Port Number	Component Computer	Port Use
389	Identity Vault	Used for LDAP communication in clear text with Identity Manager components
465	Identity Reporting	Used for communication with the SMTP mail server
524	Identity Vault	Used for NetWare Core Protocol (NCP) communication
636	Identity Vault	Used for LDAP with TLS/SSL communication with Identity Manager components
5432	Identity Applications	Used for communication with the identity applications database

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

Managing Passwords

When you choose to exchange information between connected systems, you should take precautions to make sure that the exchange is secure. This is especially true for passwords.

- ♦ The Password Hint attribute (nsimHint) is publicly readable, to allow unauthenticated users who have forgotten a password to access their own hints. Password Hints can help reduce help desk calls.

For security, Password Hints are checked to make sure that they do not contain the user's actual password. However, a user could still create a Password Hint that gives too much information about the password.

To increase security when using Password Hints:

- ♦ Allow access to the nsimHint attribute only on the LDAP server used for Password Self-Service.
- ♦ Require that users answer Challenge Questions before receiving the Password Hint.
- ♦ Remind users to create Password Hints that only they would understand. The Password Change Message in the password policy is one way to do this. See “Adding a Password Change Message” in the [Password Management 3.3 Administration Guide](#).

If you choose not to use Password Hint at all, make sure you don't use it in any of the password policies. To prevent Password Hints from being set, you can go a step further and remove the Hint Setup gadget completely, as described in “Disabling Password Hint by Removing the Hint Gadget” in the [Password Management 3.3 Administration Guide](#).

- ♦ Challenge Questions are publicly readable, to allow unauthenticated users who have forgotten a password to authenticate another way. Requiring Challenge Questions increases the security of Forgotten Password Self-Service, because a user must prove his or her identity by giving the correct responses before receiving a forgotten password or a Password Hint, or resetting a password.

The intruder lockout setting is enforced for Challenge Questions, so the number of incorrect attempts an intruder could make is limited.

However, a user could create Challenge Questions that hold clues to the password. Remind users to create Challenge Questions and Responses that only they would understand. The Password Change Message in the password policy is one way to do this. See “Adding a Password Change Message” in the [Password Management 3.3 Administration Guide](#).

- ♦ For security, the Forgotten Password actions of **E-mail password to user** and **Allow user to reset password** are available only if you require the user to answer Challenge Questions.
- ♦ A security enhancement was added to NMAS 2.3.4 regarding Universal Passwords changed by an administrator. It works basically the same way as the feature previously provided for NDS Password.

If an administrator changes a user's password, such as when creating a new user or in response to a help desk call, the password is automatically expired if you have enabled the setting to expire passwords in the password policy. The setting in the password policy is in Advanced Password Rules, named **Number of days before password expires (0-365)**. For this particular feature, the number of days is not important, but the setting must be enabled.

- ♦ You are recommended to use password-ref GCV for passwords.

Creating Strong Password Policies

Password policy objects are publicly readable to allow applications to check whether passwords are compliant. This means that an unauthenticated user could query an Identity Vault and find out what password policies are in place. If the password policies require users to create strong passwords, this should not pose a risk, as noted in “Create Strong Password Policies” in the [NetIQ Password Management Administration Guide](#).

Identity Manager Password Synchronization lets you simplify user passwords and reduce help desk costs. Bidirectional password synchronization lets you share passwords among eDirectory and connected systems in multiple ways, as described in the scenarios in the [NetIQ Identity Manager Password Management Guide](#).

Using Universal Password and password policies allows you to enforce strong password syntax requirements for users. Use the Advanced Password Rules in password policies to define your organization’s best practices for passwords. The Advanced Password Rules features let you manage password syntax by using either NetIQ syntax or the Microsoft Complexity Policy. For more information, see “Managing Passwords by Using Password Policies” in the [NetIQ Password Management Administration Guide](#).

For example, using NetIQ password syntax options, you can require user passwords to comply with rules such as the following:

- ◆ Requiring unique passwords.

You can prevent users from reusing passwords, and control the number of passwords the system should store in the history list for comparison

- ◆ Requiring a minimum number of characters in the password.

Requiring longer passwords is one of the best ways to make passwords stronger.

- ◆ Requiring a minimum number of numerals in the password.

Requiring at least one numeric character in a password helps protect against “dictionary attacks,” in which intruders try to log in using words in the dictionary.

- ◆ Excluding passwords of your choice.

You can exclude words that you consider to be security risks, such as the company name or location, or the words “test” or “admin.” Although the exclusion list is not meant to import an entire dictionary, the list of words you exclude can be quite long. Just keep in mind that a long list of exclusions makes login slower for your users. A better protection from dictionary attacks is to require numerals or special characters.

Keep in mind that you can create multiple password policies if you have different password requirements in different parts of the tree. You can assign a password policy to the whole tree, a partition root container, container, or even an individual user. (To simplify administration, we recommend that you assign password policies as high up in the tree as possible.)

In addition, you can use intruder lockout. As always, this eDirectory feature lets you specify how many failed login attempts are allowed before an account is locked. This is a setting on the parent container instead of in the password policy. See “Managing User Accounts” in the [NetIQ eDirectory Administration Guide](#) (<https://www.netiq.com/documentation/edirectory-91/>).

Securing ActiveMQ Communication

Identity Manager uses ActiveMQ for supporting messaging service in the following components:

- ◆ JDBC Fan-Out driver, between the Fan-Out driver shim and ActiveMQ and between ActiveMQ and the Fan-Out agent

For more information, see [Securing Fan-Out Driver Communication](#) in the *NetIQ Identity Manager Driver for JDBC Fan-Out Implementation Guide*.

- ◆ User Application

NetIQ recommends using Secure Socket Layer (SSL) protocol for ActiveMQ communication. By default, SSL protocol is not configured in the components interacting with ActiveMQ. You must manually configure it.

Configuring a Whitelist of Target URLs

URL redirection, which many applications and services require, inherently brings in security risks. While redirecting, the request can be tampered to redirect users to an external, malicious site. To prevent such issues, you can configure a list of permissible URLs in OSP configuration. This restricts redirection only to the configured URLs. For example, when an authentication request is not targeted to the OSP's whitelisted URLs, OSP rejects the request.

- ◆ [“Configuring a Whitelist of Target URLs in Identity Applications” on page 15](#)
- ◆ [“Configuring a Whitelist of Target URLs in OSP” on page 15](#)

Configuring a Whitelist of Target URLs in Identity Applications

You can control which URLs the identity applications can redirect to post logout. This behavior is controlled by `com.novell.pwdmgmt.login.PREF_LOGOUT_WHITELIST` entry in the `ism-configuration.properties` file. To allow identity applications to redirect to a URL after logout, add that URL or a regular expression matching that URL to this entry in one of the following formats:

```
https://google.com
```

or

```
https://www\\.((google)|(wikipedia))\\.com
```

Configuring a Whitelist of Target URLs in OSP

The whitelist feature is turned on by default. You can manually configure the whitelist entries or disable the whitelist by modifying certain settings in the `ism-configuration.properties` file.

To disable the whitelist, add the following property to the `ism-configuration.properties` file:

```
com.netiq.idm.osp.target-white-list.enabled = false
```

To configure the whitelist manually, add the following property to the `ism-configuration.properties` file:

```
com.netiq.idm.osp.target-white-list.mode = manual
```

You can add one or both of the following properties:

```
com.netiq.idm.osp.target-white-list.uris = <space-separated-list-of-urls>

com.netiq.idm.osp.target-white-list.uri-patterns = <space-separated-list-of-url-
regex>
```

For example:

```
com.netiq.idm.osp.target-white-list.uris = https://www.google.com/ http://bing.com

com.netiq.idm.osp.target-white-list.uri-patterns = \\Qhttps\\E://.*\\Q.provo.novell.com\\E
\\Qhttps\\E://.*\\Q.microfocus.com\\E
```

To add to the automatically configured whitelist, include `com.netiq.idm.osp.target-white-list.uris` or `com.netiq.idm.osp.target-white-list.uri-patterns` or both properties and specify `com.netiq.idm.osp.target-white-list.mode = mixed`.

Preventing Clickjacking Attacks in Identity Manager

If Identity Manager is deployed in a distributed setup and User Application and OSP are installed on separate servers, your Identity Manager environment can be susceptible to clickjacking attacks. For more information, see [HTTP Strict Transport Security \(https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\)](https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security) and [Clickjacking \(https://en.wikipedia.org/wiki/Clickjacking\)](https://en.wikipedia.org/wiki/Clickjacking).

HSTS forces all responses to pass through HTTPS connections instead of plain text HTTP. This ensures that the entire channel is encrypted before any data is sent on the channel and eliminates any chances for the attackers to read or modify the data in transit. To prevent clickjacking attacks, perform the following actions:

Update OSP Server Configuration

- 1 Stop Tomcat. For example, `systemctl stop netiq-tomcat`
- 2 Navigate to `<tomcat-install-directory>/conf/web.xml` or `<tomcat-install-directory>/conf/ directory`.
- 3 Add the following filter to the `web.xml` file:

```
<filter>
  <filter-name>httpHeaderSecurity</filter-name>
  <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</
filter-class>
  <async-supported>>true</async-supported>
  <init-param>
    <param-name>antiClickJackingOption</param-name>
    <param-value>ALLOW-FROM</param-value>
  </init-param>
  <init-param>
    <param-name>antiClickJackingUri</param-name>
    <param-value>User Application URI</param-value>
  </init-param>
</init-param>
```



```

        <param-name>hstsMaxAgeSeconds</param-name>
        <param-value>31536000</param-value>
    </init-param>
    <init-param>
        <param-name>hstsIncludeSubDomains</param-name>
        <param-value>true</param-value>
    </init-param>
</filter>

<filter-mapping>
    <filter-name>httpHeaderSecurity</filter-name>
    <url-pattern>/*</url-pattern>
    <dispatcher>REQUEST</dispatcher>
</filter-mapping>

```

4 Save the file.

5 Start Tomcat. For example, `systemctl start netiq-tomcat`

For example, User Application URI: <https://ua.microfocus.com:8643/>, this is where User Application is running.

Update User Application Server Configuration

1 Stop Tomcat. For example, `systemctl stop netiq-tomcat`

2 Navigate to `<tomcat-install-directory>/conf/web.xml` or `<tomcat-install-directory>\conf\ directory`.

3 Add the following filter to the `web.xml` file:

```

<filter>
    <filter-name>httpHeaderSecurity</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</
filter-class>
    <async-supported>true</async-supported>
    <init-param>
        <param-name>antiClickJackingOption</param-name>
        <param-value>SAMEORIGIN</param-value>
    </init-param>
    <init-param>
        <param-name>hstsMaxAgeSeconds</param-name>
        <param-value>31536000</param-value>
    </init-param>
    <init-param>
        <param-name>hstsIncludeSubDomains</param-name>
        <param-value>true</param-value>
    </init-param>
</filter>

<filter-mapping>
    <filter-name>httpHeaderSecurity</filter-name>
    <url-pattern>/*</url-pattern>
    <dispatcher>REQUEST</dispatcher>
</filter-mapping>

```

4 Save the file.

5 Start Tomcat. For example, `systemctl start netiq-tomcat.service`

NOTE: As per [RFC 7034](#), the `ALLOW-FROM` parameter supports only a single domain. It does not support multiple domains. For example, if OSP, User Application, SSPR, and Identity Reporting are installed on different computers, this parameter does not work.

Rejecting Client-initiated SSL Renegotiation on Windows

Under certain circumstances, Identity Manager can be susceptible to a Denial of Service attack caused by a client initiated SSL renegotiation operation. To configure Identity Manager to reject this operation, perform the following actions on each computer running the identity applications:

- 1 Edit the `tomcat-install-directory>\bin\setenv.bat` file.
- 2 Add the following flag to the `CATALINA_OPTS` entry in the file:

```
"-Djdk.tls.rejectClientInitiatedRenegotiation=true"
```
- 3 Save the `setenv.bat` file.
- 4 Restart Tomcat.

Securing Connected Systems

Keep in mind that the connected systems that you are synchronizing data to might store or transport that data in a compromising manner.

Secure the systems with which you exchange passwords. For example LDAP, NIS, and Windows each have security concerns that you must consider before enabling password synchronization with those systems.

Many software vendors provide specific security guidelines that you should follow for their products.

Password Generation

Identity Manager includes a predefined password generation job for the Job Scheduler. The password generation job generates random passwords for a group of User objects in eDirectory, either periodically or on demand. This functionality is designed primarily to support products like NetIQ Certificate Login, but can also be used in other situations.

Invoking the password generation job initializes NMAS with the password policy, and the following occurs for each object in the specified job scope:

1. NMAS generates a random password consistent with the password policy specified in the job. Password policies are stored in `nspmPasswordPolicy` objects. Typically, each connected system has its own policy object. These policy objects can be stored in `DirXML-Driver` and `DirXML-DriverSet` objects.
2. Each generated password is submitted, one at a time, to the containing driver's Subscriber channel.

If the object has a non-disabled association for the driver then a `<generated-password>` event is submitted to the Subscriber channel event queue (cache) of the driver.

If the object has no association for the driver and the option to submit events for non-associated objects is selected, then a <generated-password> event is submitted to the Subscriber channel event queue (cache) of the driver.

3. It is up to the Subscriber channel policies to handle the generated passwords. The Job Scheduler is only responsible for generating the passwords and handing them off to the Subscriber channel.

Designer for Identity Manager

When using Designer for Identity Manager, consider the following issues:

- ♦ Monitor and control who has rights to create or modify an Identity Manager driver.
Administrative rights are needed to create Identity Manager objects and configure drivers.
- ♦ Before giving a consultant an Identity Vault administrator password, limit the rights assigned to that administrator to areas of the tree that the consultant must access.
- ♦ Delete the project files (.proj) or save them to a company directory.
Designer .proj files are to remain at the company's project site. A consultant does not take the files after completing a project.
- ♦ After project files, log files, and trace files are no longer needed, delete them.
- ♦ Before discarding or surplusing a laptop, verify that project files have been cleaned.
- ♦ Ensure that the connection from Designer to the Identity Vault server is physically secure. Otherwise, someone could monitor the wire and pull sensitive information.
- ♦ When you use Document Generator to create documents, be careful with those documents. These documents can contain passwords and sensitive data in clear text.
- ♦ If Designer needs to read or write to an eDirectory attribute, do not mark that attribute as encrypted. Designer is unable to read or write to encrypted attributes.
- ♦ Do not store passwords that are sensitive.

Currently, Designer projects are not encrypted. Passwords are only encoded. Therefore, do not share Designer projects that have saved passwords.

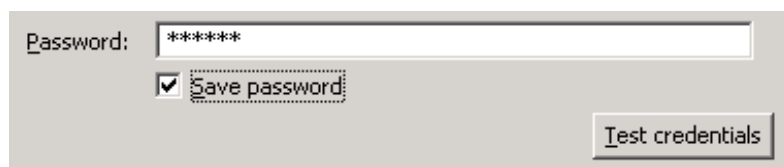
To save a password for a session, but not save it to the project:

1. In an expanded Outline view, right-click an Identity Vault.
2. Select **Properties**.
3. On the Configuration page, type a password, then click **OK**.

You can enter a password once per session. After you close the project, the password is lost.

To save a password to the hard drive, complete Steps 1-3, select **Save Password**, then click **OK**.

Figure 1-1 Save Password



Password: [*****]
 Save password
Test credentials

Industry Best Practices for Security

Follow industry best practices for security measures, such as blocking unused ports on the server.

Tracking Changes to Sensitive Information

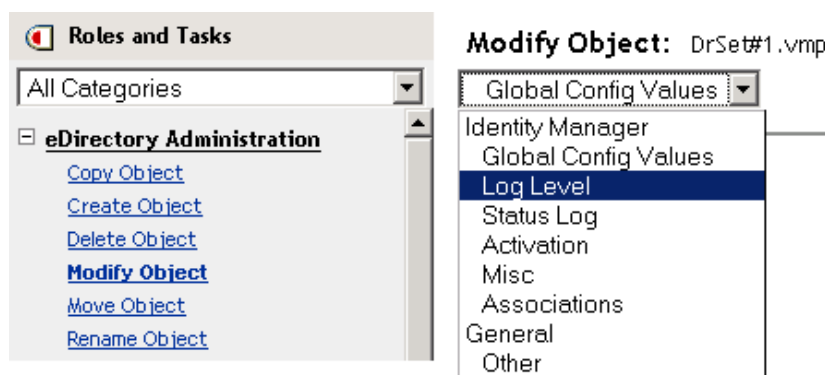
- ♦ “Using iManager to Log Events” on page 20
- ♦ “Using Designer to Log Events” on page 21

Using iManager to Log Events

You can use Audit to log events that you consider important for security.

For example, you could log password changes for a particular Identity Manager driver (or driver set) by doing the following:


- 1 In iManager, select **eDirectory Administration > Modify Object > Log Level**.



Select from the drop-down list or select a tab, depending on your version of iManager.

- 2 Select **Log Specific Events**.



- 3 To select the specific events, click the Log Events icon .
- 4 Enable the **Turn off logging to Driver Set, Subscriber and Publisher logs** option to prevent logging Identity Manager events to eDirectory.
Enabling this option improves the performance of the Identity Manager system.
- 5 On the Events page, select the following:

Operation Events		
<input type="checkbox"/> Search	<input type="checkbox"/> Add	<input type="checkbox"/> Remove
<input type="checkbox"/> Modify	<input type="checkbox"/> Rename	<input type="checkbox"/> Move
<input type="checkbox"/> Add Association	<input type="checkbox"/> Remove Association	<input type="checkbox"/> Query Schema
<input type="checkbox"/> Check Password	<input type="checkbox"/> Check Object Password	<input checked="" type="checkbox"/> Change Password
<input type="checkbox"/> Sync	<input type="checkbox"/> Clear Attribute	<input type="checkbox"/> Add Value
<input type="checkbox"/> Remove Value	<input type="checkbox"/> Merge Entry	

Transformation Events		
<input type="checkbox"/> Initial Document	<input type="checkbox"/> Input	<input type="checkbox"/> Output
<input type="checkbox"/> Event	<input type="checkbox"/> Placement	<input type="checkbox"/> Create
<input type="checkbox"/> Input Mapping	<input type="checkbox"/> Output Mapping	<input type="checkbox"/> Matching
<input type="checkbox"/> Command	<input type="checkbox"/> Driver Filter	<input type="checkbox"/> User Agent Request
<input type="checkbox"/> Resync Request	<input type="checkbox"/> Migrate Request	<input checked="" type="checkbox"/> Password Sync
<input checked="" type="checkbox"/> Password Set		

- ◆ In Operation Events, select **Change Password**.
This item monitors direct changes to the NDS password.
 - ◆ In Transformation Events, select **Password Set** and **Password Sync**. These two items monitor events for the Universal Password and Distribution Password.
- 6 Click **OK** twice.

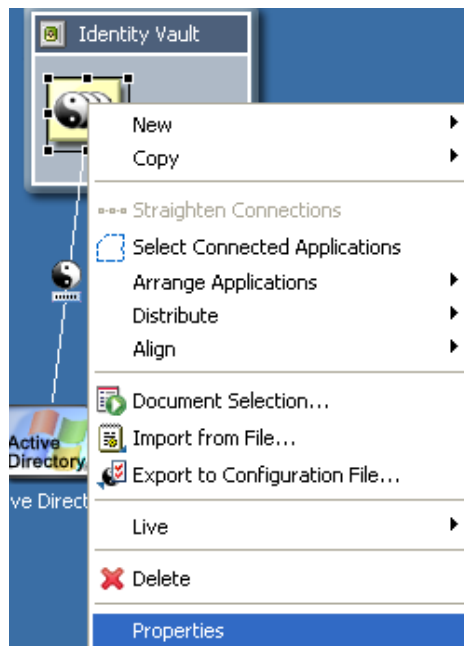
Using Designer to Log Events

You can log events that apply to a driver set or to a driver.

- ◆ [“Logging Events for a Driver Set” on page 21](#)
- ◆ [“Logging Events for a Driver” on page 23](#)

Logging Events for a Driver Set

- 1 In Designer, right-click a driver set, then select **Properties**.



- 2 Select **Driver Set Log Level**, then select **Log Specific Events**.
- 3 Click the **Select Events to Log** icon.
- 4 Enable the **Turn off logging to Driver Set, Subscriber and Publisher logs** option to prevent logging Identity Manager events to eDirectory.
Enabling this option improves the performance of the Identity Manager system.

5 Select events to log, then click **OK**.

The screenshot shows a dialog box titled 'Log Specific Events' with a light beige background. It is organized into four sections, each with a bold heading and a list of events with checkboxes. The 'Engine Events' section has three columns: the first column contains 'Start Driver' (checked) and 'Engine Warnings' (checked); the second column contains 'Stop Driver' (checked); the third column contains 'Engine Errors' (checked). The 'Status Events' section has three columns: the first column contains 'Success' (unchecked) and 'Error' (checked); the second column contains 'Retry' (unchecked) and 'Fatal' (checked); the third column contains 'Warning' (checked) and 'Other' (unchecked). The 'Operation Events' section has three columns: the first column contains 'Search' (unchecked), 'Modify' (unchecked), 'Add Association' (unchecked), 'Check Password' (unchecked), 'Sync' (unchecked), 'Add value (on add)' (unchecked), 'Get Named Password' (unchecked), and 'Set SSO Credential' (unchecked); the second column contains 'Add' (unchecked), 'Rename' (unchecked), 'Remove Association' (unchecked), 'Check Object Password' (unchecked), 'Custom Operation' (unchecked), 'Remove Value' (unchecked), 'Reset Attributes' (unchecked), and 'Clear SSO Credential' (unchecked); the third column contains 'Remove' (unchecked), 'Move' (unchecked), 'Query Schema' (unchecked), 'Change Password' (unchecked), 'Clear Attribute' (unchecked), 'Merge Entry' (unchecked), 'Add Value (on modify)' (unchecked), and 'Set SSO Passphrase' (unchecked). The 'Transformation Events' section has three columns: the first column contains 'Initial Document' (unchecked), 'Event' (unchecked), 'Input Mapping' (unchecked), 'Command' (unchecked), 'Resync Request' (unchecked), and 'Password Reset' (unchecked); the second column contains 'Input' (unchecked), 'Placement' (unchecked), 'Output Mapping' (unchecked), 'Driver Filter' (unchecked), and 'Migrate Request' (unchecked); the third column contains 'Output' (unchecked), 'Create' (unchecked), 'Matching' (unchecked), 'User Agent Request' (unchecked), and 'Password Sync' (unchecked).

Logging Events for a Driver

- 1 In Designer, right-click a driver, then select **Properties**.
- 2 Select **Driver Log Level**, then select **Log Specific Events**.
- 3 If you prefer, you can accept the settings for the driver set, then click **OK**.
or
Deselect **Use log settings from the Driver Set**, select **Log specific events**, then click **OK**.
- 4 Click the **Select Events to Log** icon.

5 Select events to log, then click **OK**.

Engine Events

Start Driver Stop Driver Engine Errors

Engine Warnings

Status Events

Success Retry Warning

Error Fatal Other

Operation Events

Search Add Remove

Modify Rename Move

Add Association Remove Association Query Schema

Check Password Check Object Password Change Password

Sync Custom Operation Clear Attribute

Add value (on add) Remove Value Merge Entry

Get Named Password Reset Attributes Add Value (on modify)

Set SSO Credential Clear SSO Credential Set SSO Passphrase

Transformation Events

Initial Document Input Output

Event Placement Create

Input Mapping Output Mapping Matching

Command Driver Filter User Agent Request

Resync Request Migrate Request Password Sync

Password Reset

Establishing a Security Equivalent User

Security Equivalence refers to an object being equivalent in rights to another object. You can define and deploy security equivalences objects for drivers in the Identity Vault. For example, an Oracle database driver contains a policy to create a user in the Identity Vault in a container every time a user is created in the database, but the driver doesn't have enough permissions on the container to create the user, thus the process fails.

The driver must run with Security Equivalence to a user with sufficient rights. You can set the driver equivalent to an Admin or a similar user. For stronger security, you can define a user with minimal rights necessary for the operations you want the driver to perform. The driver user must be a trustee of the containers where synchronized users and groups reside, with the rights listed in [Table 1-2](#). Inheritance must be set for [Entry Rights] and [All Attribute Rights].

Table 1-2 Base Container Rights Required by the Driver Security-Equivalent User

Operation	[Entry Rights]	[All Attribute Rights]
Subscriber notification of account changes (recommended minimum)	Browse	Compare and Read

Operation	[Entry Rights]	[All Attribute Rights]
Creating objects in the Identity Vault without group synchronization	Browse and Create	Compare and Read
Creating objects in the Identity Vault with group synchronization	Browse and Create	Compare, Read, and Write
Modifying objects in the Identity Vault	Browse	Compare, Read, and Write
Renaming objects in the Identity Vault	Browse and Rename	Compare and Read
Deleting objects from the Identity Vault	Browse and Erase	Compare, Read, and Write
Retrieving passwords from the Identity Vault	Browse and Supervisor	Compare and Read
Updating passwords in the Identity Vault	Browse and Supervisor	Compare, Read, and Write

If you do not set Supervisor for [Entry Rights], the driver will not have rights to set passwords. If you do not want to set passwords, you can set the `Subscribe` setting for the `User` class `nspmDistributionPassword` attribute to `Ignore` in the filter to avoid error messages. For details about accessing and editing the filter, see the appropriate policy publication on the [Identity Manager Documentation Web site](#). For complete information about rights, see “[Deploying a Driver to an Identity Vault](#)” in the *NetIQ Designer for Identity Manager Administration Guide*.

