# Security Guide

## Identity Manager 4.0.1

**April 15, 2011**

**Novell**.

## Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to the International Trade Services (http://www.novell.com/company/policies/trade_services) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2008-2011 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

*Online Documentation:* To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

## Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

## Third-Party Materials

All third-party trademarks are the property of their respective owners.

# Contents

# About This Guide

This guide contains information about security best practices you might want to implement in your Identity Manager environment. The guide is organized as follows:

◆ Chapter 1, "Security Best Practices," on page 7

**Audience**

This guide is intended for administrators, consultants, and network engineers who require a high-level introduction to Identity Manager business solutions, technologies, and tools.

**Documentation Updates**

For the most recent version of this document, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm401/index.html).

**Additional Documentation**

For documentation on other Identity Manager drivers, see the Identity Manager Drivers Web site (http://www.novell.com/documentation/idm401drivers/index.html).

# 1 Security Best Practices

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

## 1.1 Using SSL

Enable SSL for all transports, where it is available. Enable SSL for communication between the Metadirectory engine and Remote Loader and between the Metadirectory engine or Remote Loader and the connected systems. For information, see "Creating a Secure Connection" in the *Identity Manager 4.0.1 Remote Loader Guide*.

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

## 1.2 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 Metadirectory 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%200%2047832401).

**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

## 1.2.1 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* (http://www.novell.com/documentation/imanager27/imanager_admin_27/data/hk42s9ot.html).

# 1.3 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.

# 1.4   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 *Password Management 3.3 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 *Identity Manager 4.0.1 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 Novell syntax or the Microsoft Complexity Policy. For more information, see "Managing Passwords by Using Password Policies" in the *Novell Password Management 3.3 Administration Guide*.

For example, using Novell 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 *Novell eDirectory Administration Guide* (http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/afxkmdi.html).

## 1.5 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.

### 1.5.1 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 Novell 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.

## 1.6 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*

## 1.7  Industry Best Practices for Security

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

## 1.8  Tracking Changes to Sensitive Information

- Section 1.8.1, "Using iManager to Log Events," on page 12
- Section 1.8.2, "Using Designer to Log Events," on page 14

### 1.8.1  Using iManager to Log Events

You can use Novell 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*.
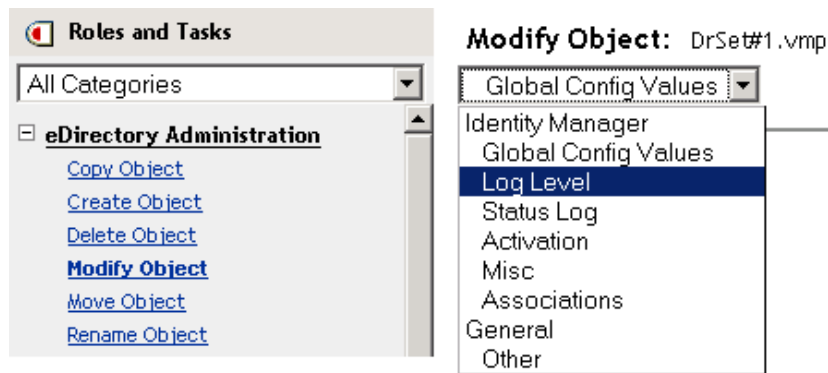
Select from the drop-down list or select a tab, depending on your version of iManager.

**2** Select *Log Specific Events*.
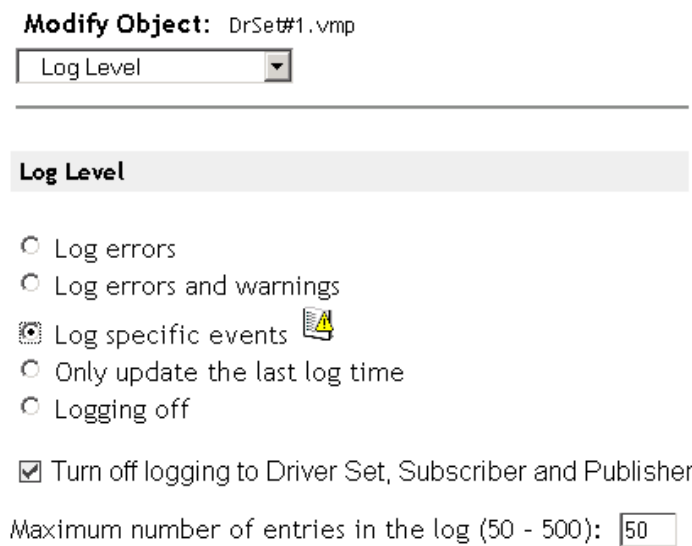


**3** To select the specific events, click the Log Events icon 🖹.

**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

| | | |
|---|---|---|
| ☐ Search | ☐ Add | ☐ Remove |
| ☐ Modify | ☐ Rename | ☐ Move |
| ☐ Add Association | ☐ Remove Association | ☐ Query Schema |
| ☐ Check Password | ☐ Check Object Password | ☑ Change Password |
| ☐ Sync | ☐ Clear Attribute | ☐ Add Value |
| ☐ Remove Value | ☐ Merge Entry | |

## 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 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.

## 1.8.2  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

**1** In Designer, right-click a driver set, then select *Properties*.
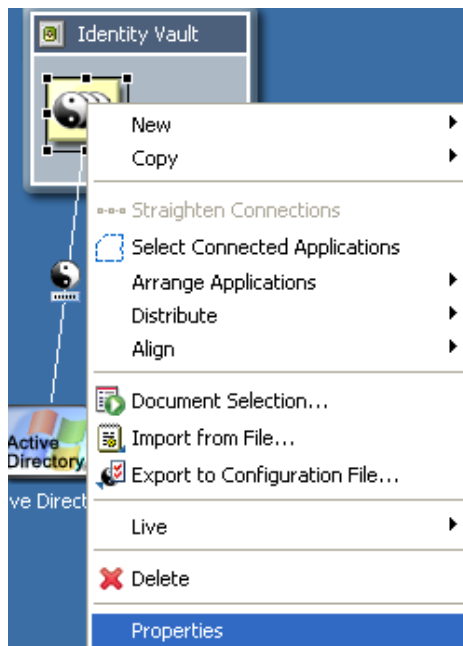
**2** Select *Driver Set Log Level*, then select *Log Specific Events*.
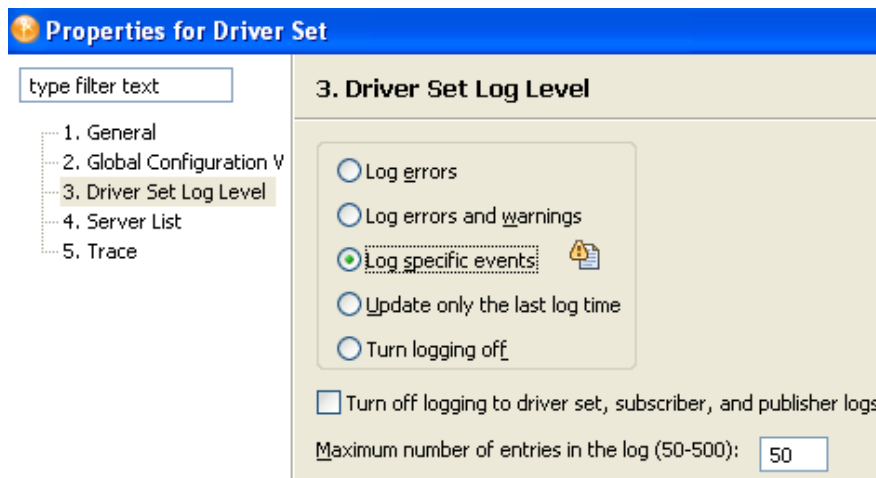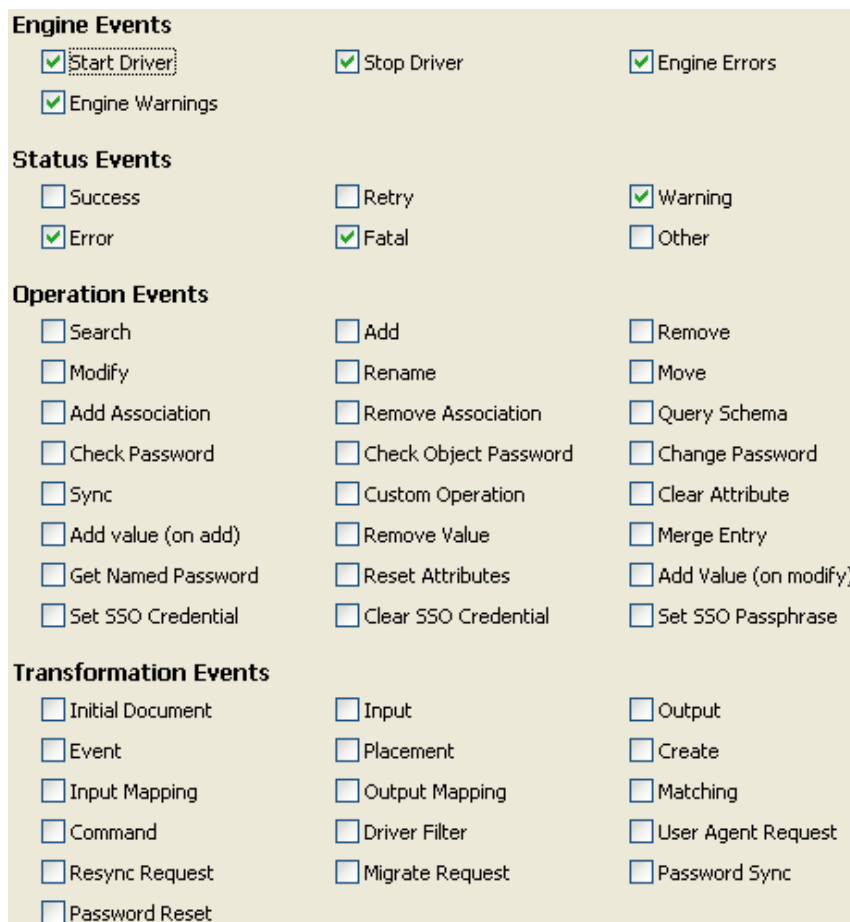


**3** Click the *Select Events to Log* icon.
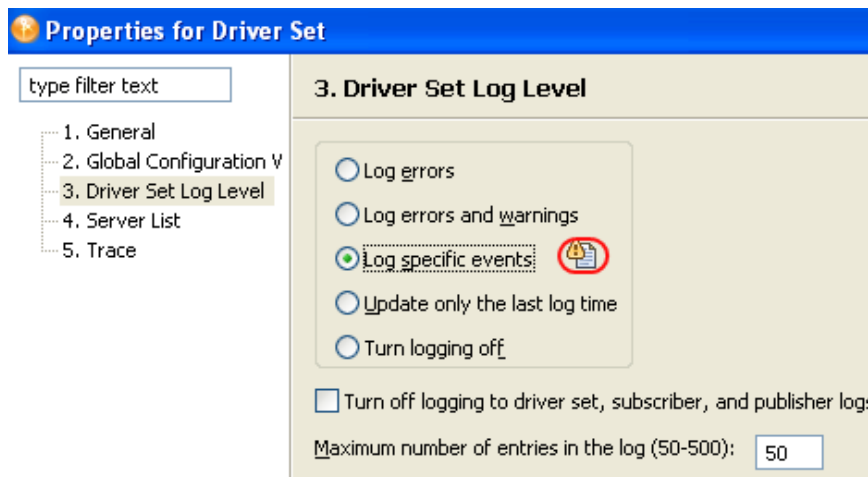
**4** Enable the *Turn off logging to Driver Set, Subscriber and Publisher logs* option to prevent logging Identity Manager events to eDirectory.

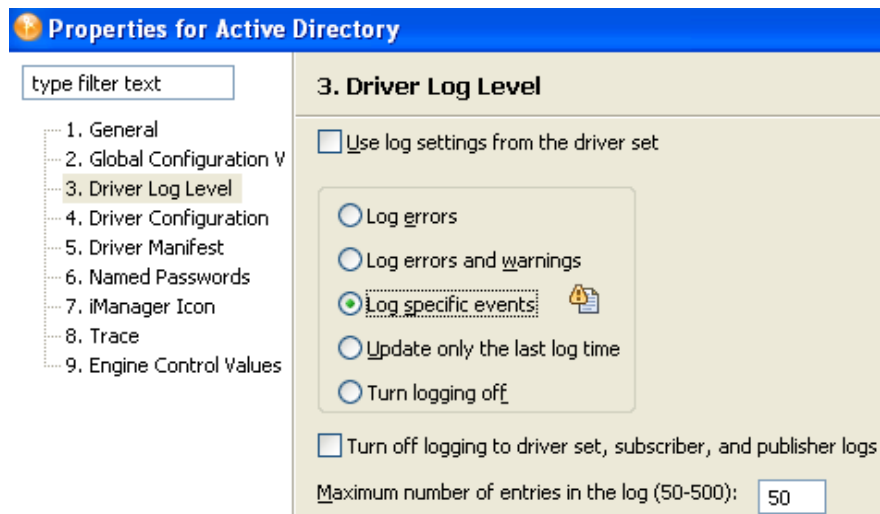Enabling this option improves the performance of the Identity Manager system.

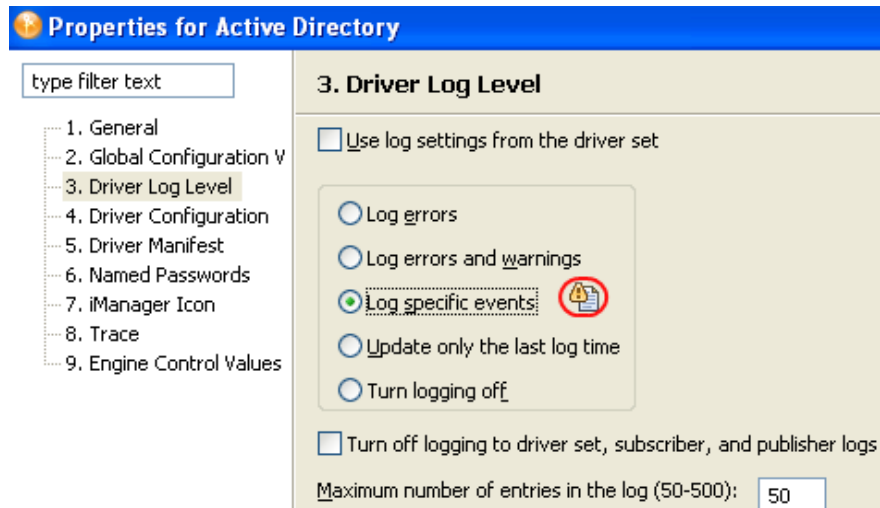**5** Select events to log, then click *OK*.

## 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