

---

# NetIQ® Identity Manager

## Administrator's Guide to Configure Auditing

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

<b>About this Book and the Library</b>	<b>5</b>
<b>About NetIQ Corporation</b>	<b>7</b>
<b>1 Overview</b>	<b>9</b>
Identity Manager Auditing Architecture . . . . .	9
Enabling Auditing . . . . .	10
<b>2 Configuring NetIQ Sentinel with Identity Manager</b>	<b>13</b>
<b>3 Installing and Configuring the Identity Manager Collector</b>	<b>15</b>
Installing and Configuring the Identity Manager Collector. . . . .	15
Installing and Configuring the SSPR and OSP Collectors . . . . .	16
<b>4 Installing the Audit and Syslog Connector</b>	<b>17</b>
Installing and Configuring the Audit Connector. . . . .	17
Installing and Configuring the Syslog Connector . . . . .	18
<b>5 Installing and Configuring the Platform Agent</b>	<b>21</b>
Installing the Platform Agent. . . . .	21
Configuring the Platform Agent Text File. . . . .	21
<b>6 Configuring Identity Manager Components to Log Audit Events in CEF Format</b>	<b>25</b>
Advantages of CEF. . . . .	25
Setting up CEF Configuration . . . . .	26
Configuring Identity Manager Engine. . . . .	26
Configuring Remote Loader. . . . .	27
Configuring .NET Remote Loader . . . . .	27
Configuring Java Remote Loader . . . . .	27
Configuring Fanout Agent . . . . .	27
Configuring Identity Applications . . . . .	28
Configuring Data Collection Services. . . . .	28
Configuring One SSO Provider . . . . .	29
<b>7 Securing the Logging System</b>	<b>31</b>
<b>8 Managing Identity Manager Events</b>	<b>33</b>
Selecting Events to Log . . . . .	33
Selecting Events for the User Application . . . . .	33
Selecting Events for the Driver Set . . . . .	35
Selecting Events for a Specific Driver . . . . .	35
Identity Manager Log Levels . . . . .	36
User-Defined Events. . . . .	37
Using Policy Builder to Generate Events . . . . .	37

Using Status Documents to Generate Events . . . . .	40
eDirectory Objects that Store Identity Manager Event Data . . . . .	40
<b>9 Using Status Logs</b>	<b>41</b>
Setting the Log Level and Maximum Log Size . . . . .	41
Setting the Log Level and Log Size for the Driver Set . . . . .	41
Setting the Log Level and Log Size for the Driver . . . . .	42
Viewing Status Logs . . . . .	43
Accessing the Driver Set Status Log . . . . .	43
Accessing the Publisher Channel and Subscriber Channel Status Logs . . . . .	44
<b>A Identity Manager Events</b>	<b>45</b>
CEF Events . . . . .	45
Event Structure . . . . .	49
Remote Loader Events . . . . .	49
Engine Events . . . . .	49
Fanout Agent Events . . . . .	52
User Application Events . . . . .	52
DCS Events . . . . .	55
<b>B Understanding the Properties Files for CEF Auditing</b>	<b>57</b>
Understanding the auditlogconfig.properties File . . . . .	57
Identity Manager Engine, Remote Loader, and .NET Remote Loader . . . . .	57
Java Remote Loader and Fanout Agent . . . . .	61
Understanding the idmuserapp_logging.xml File . . . . .	62
Understanding the idmrptdcs_logging.xml File . . . . .	64

# About this Book and the Library

The *Identity Manager - Configuring Auditing in Identity Manager Guide* provides the information necessary to set up Identity Manager components for auditing events. You can then integrate NetIQ Sentinel with Identity Manager to provide auditing and reporting services.

## 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.

<b>Worldwide:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>United States and Canada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

## 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](http://www.netiq.com/documentation). You can also email [Documentation-Feedback@netiq.com](mailto: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>.



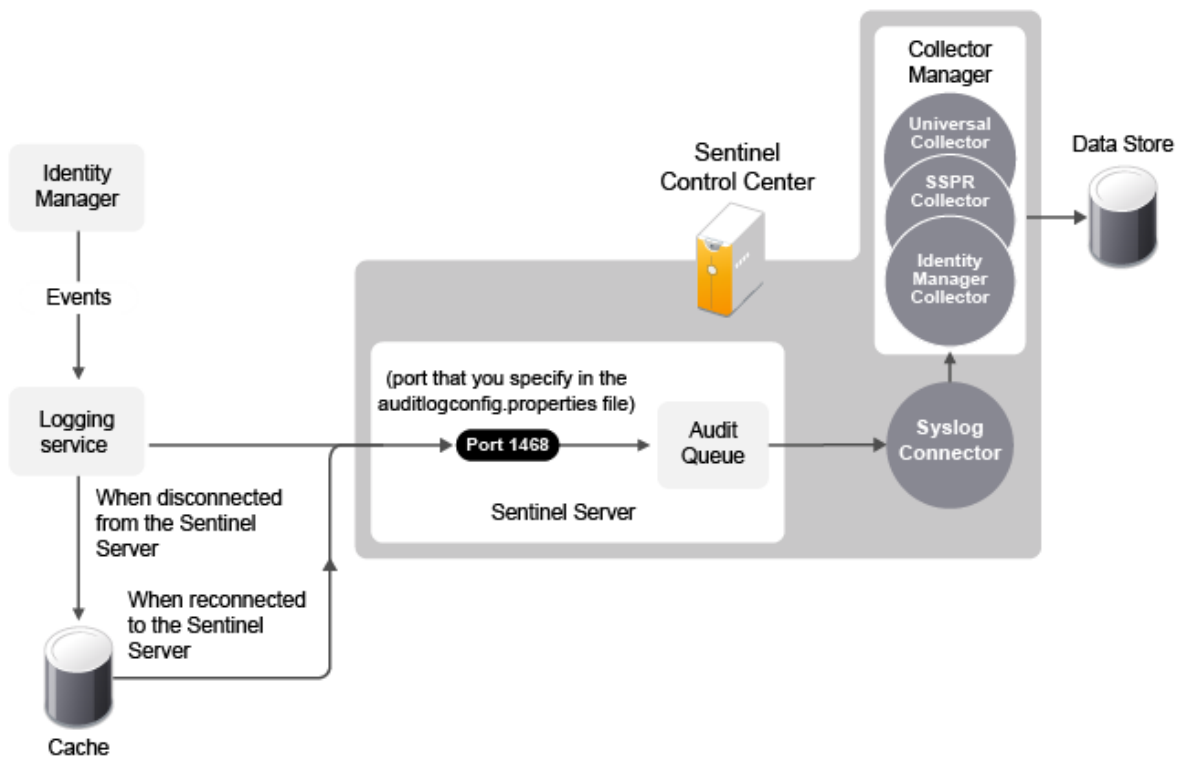
# 1 Overview

This guide helps you in implementing a uniform auditing across Identity Manager.

## Identity Manager Auditing Architecture

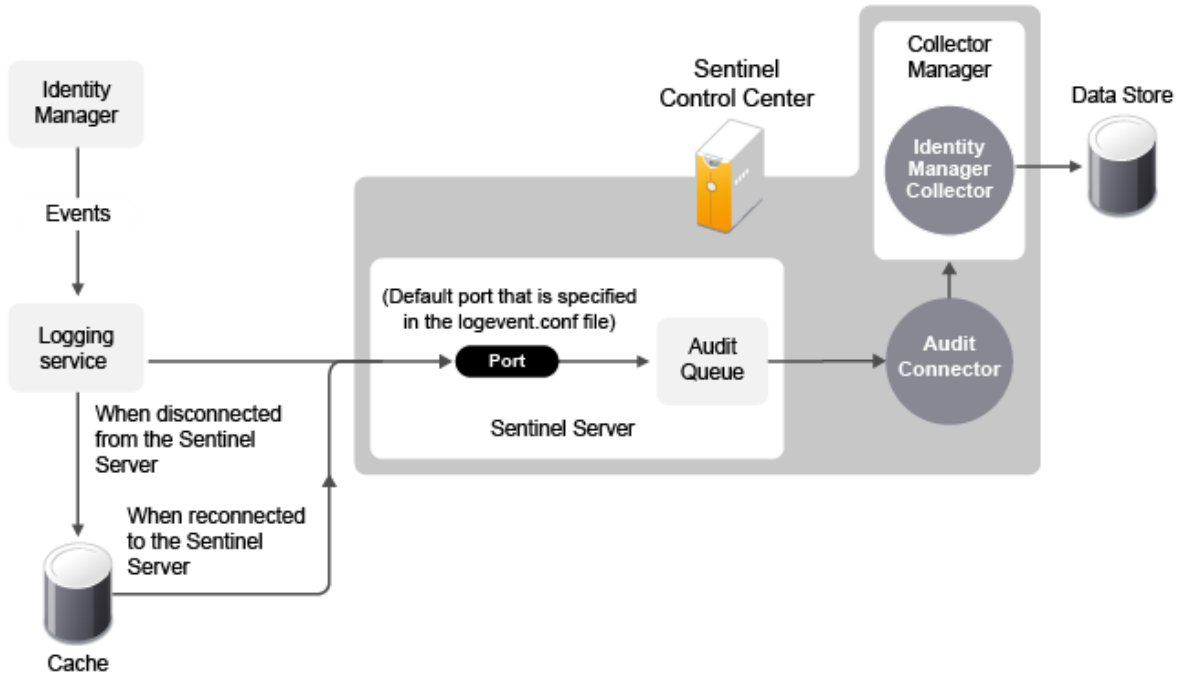
The following diagrams illustrate how different components work together to provide a uniform auditing infrastructure in Identity Manager. Sentinel is the preferred audit event destination for Identity Manager. Identity Manager provides event forwarding capabilities to Sentinel by configuring Sentinel Link using Sentinel Event Source Management (ESM).

*Figure 1-1 Auditing through CEF*



1. An Identity Manager event occurs and it is sent to the logging services.
2. (Conditional) If the logging services cannot connect to the Sentinel Server, the events are stored in cache until the connection is reestablished.
3. The logging services sends the events to the Sentinel Server, which stores the events in the audit queue.
4. The events in the audit queue are sent to the Syslog Connector.
5. The Syslog Connector sends the events to the Identity Manager Collector, which parses the information and then stores the parsed events in the data store.
6. (Optional) The stored events can be used for reports.

Figure 1-2 Auditing through Platform Agent



For a thorough discussion of the Sentinel architecture, see “Appendix A Sentinel Architecture” in the NetIQ Sentinel User’s Guide.

## Enabling Auditing

Auditing is not enabled by default. You must enable it after you have installed the Identity Manager components. NetIQ provides different auditing options for Identity Manager components as listed in the following table:

Table 1-1 Identity Manager Auditing Support

Component	Auditing Support
Identity Manager Engine, Remote Loader, Fanout Agent, and Identity Applications	<p>CEF and Platform Agent</p> <p>To enable CEF auditing for these components, see <a href="#">“Setting up CEF Configuration”</a> on page 26.</p> <p>To enable auditing through Platform Agent, see <a href="#">“Configuring the Platform Agent Text File”</a> on page 21.</p>
OSP	<p>CEF</p> <p>To enable CEF auditing for OSP, see <a href="#">“Configuring One SSO Provider”</a> on page 29.</p>

---

Component	Auditing Support
Identity Reporting	No auditing support in Identity Manager 4.7 Supports CEF (from Identity Manager 4.7.1 onwards). To enable CEF auditing for Identity Reporting, see the <a href="#">NetIQ Identity Manager 4.7 Service Pack 1 Release Notes</a> .

---



# 2 Configuring NetIQ Sentinel with Identity Manager

Use the following checklist to verify that all of the steps are completed to install and configure Sentinel with Identity Manager.

- Install and configure Sentinel. NetIQ recommends that you install Identity Manager and Sentinel on different servers. For more information, see the [NetIQ Sentinel Installation Guide](#).
- Install and configure the NetIQ Sentinel Identity Manager Collector. For more information, see [Chapter 3, "Installing and Configuring the Identity Manager Collector," on page 15](#).
- Install and configure the NetIQ Audit Connector. For more information, see [Chapter 4, "Installing the Audit and Syslog Connectors," on page 15](#).
- Install and configure the NetIQ Syslog Connector. For more information, see [Chapter 4, "Installing the Audit and Syslog Connector," on page 17](#).
- Configure Identity Manager components to use Common Event Format (CEF).  
For more information, see [Chapter 6, "Configuring Identity Manager Components to Log Audit Events in CEF Format," on page 25](#).
- (Optional) Secure the connection between Identity Manager and the Platform Agent.  
For more information, see the [Chapter 7, "Securing the Logging System," on page 31](#).
- Configure the Sentinel Control Center to access the predefined reports for Identity Manager.



# 3 Installing and Configuring the Identity Manager Collector

The Identity Manager Collector parses and normalizes the raw data passed to it by the Audit or Syslog Connector and converts the data into a Sentinel event. The Sentinel event can be visualized in the Active View, processed by the correlation engine, queried in a report, and added to an incident response workflow.

The Identity Manager Collector can also parse non-event data and transform the raw scan data into a format understood by Sentinel. Sentinel then stores the vulnerability data in the database and includes it in the Exploit Detection map. For more detailed information about Sentinel collectors, see the [Sentinel Collector Script User's Guide](#).

---

**NOTE:** After fresh installation of Sentinel with the required collectors and connectors installed and configured, restart Sentinel for the changes to take effect.

---

## Installing and Configuring the Identity Manager Collector

The Identity Manager Collector must be added to the Event Source Manager to be installed. This step is only done once. The Identity Manager Collector is then displayed as a collector to select during configuration.

To install the Identity Manager Collector,

- 1 Download the latest Identity Manager Collector (.zip file) from the NetIQ Downloads website.
- 2 Log in to the Sentinel Control Center.
- 3 Select the **Event Source Management > Live View**, then select **Tools > Import plugin**.
- 4 Browse to and select the .zip file you just downloaded, then click **Next**.
- 5 Follow the remaining prompts, then click **Finish**.

The Identity Manager Collector must be configured to work. To configure the Identity Manager Collector,

- 1 In the Event Source Management live view, right-click **Sentinel Server**, then click **Add Collector**.
- 2 Select **NetIQ** in the **Vendor** column.
- 3 Select **Identity Manager** in the **Name** column, then click **Next**.
- 4 From the **Installed Collectors** column, select **NetIQ\_Identity-Manager\_Collector\_Version**, then click **Next**. For example, `NetIQ_Identity-Manager_2011.1r5.clz.zip`.
- 5 Follow the prompts and click **Finish**.

The next step is to proceed to [Chapter 4, "Installing the Audit and Syslog Connector,"](#) on page 17.

# Installing and Configuring the SSPR and OSP Collectors

To install the SSPR or OSP Collector,

- 1 Download the latest SSPR or OSP Collector (.zip file) from the NetIQ Plug-ins website.

---

**NOTE:** OSP is bundled with Sentinel. Extract the .zip file and browse to **contents** to view the OSP collector.

---

- 2 Log in to the Sentinel Control Center.
- 3 Select the **Event Source Management > Live View**, then select **Tools > Import plugin**.
- 4 Browse to and select the .zip file you just downloaded, then click **Next**.
- 5 Follow the remaining prompts, then click **Finish**.

The SSPR or OSP Collector must be configured to work. To configure the SSPR or OSP Collector,

- 1 In the Event Source Management live view, right-click **Sentinel Server**, then click **Add Collector**.
- 2 Select **NetIQ** in the **Vendor** column.
- 3 Select **Identity Manager** in the **Name** column, then click **Next**.
- 4 From the **Installed Collectors** column, select **<Collector>\_<Collector\_Version>**, then click **Next**.  
For example: **SelfServicePasswordReset\_<Collector\_Version>** or **OneSSOProvider\_<Collector\_Version>**
- 5 Follow the prompts and click **Finish**.

For SSPR, the next step is to proceed to [“Installing and Configuring the Syslog Connector” on page 18](#).

For OSP, the next step is to proceed to [Chapter 4, “Installing the Audit and Syslog Connector,” on page 17](#).



# 4 Installing the Audit and Syslog Connector

The NetIQ Audit (erstwhile Novell Audit) and Syslog Connector facilitates integration between Identity Manager and Sentinel.

You must install and configure the Identity Manager Collector before you install and configure the Audit or Syslog Connector.

---

**NOTE:** After installing Sentinel with the required collectors and connectors installed and configured, restart Sentinel for the changes to take effect.

---

## Installing and Configuring the Audit Connector

To install the Audit Connector,

- 1 Download the latest Audit Connector (.zip file) from the [Sentinel Plug-ins Web site](#) to the server where the Sentinel Control Center is running.  
The Audit Connector is located under the **Connectors** tab.
- 2 Log in to the Sentinel Control Center.
- 3 Select **Event Source Management > Live View**, then select **Tools > Import plugin**.
- 4 Select **Import Collector Script or Connector plugin package file (.zip)** option, then click **Next**.
- 5 Browse to and select the .zip file you just downloaded, then click **Next**.  
You must use the latest plug-ins available from the [Sentinel Plug-ins Web site](#).
- 6 Follow the remaining prompts, then click **Finish**.

You must configure the Audit Connector to receive messages sent from Identity Manager to the Platform Agent. These events are then processed by the Identity Manager Collector.

There are multiple ways to configure the Audit Connector. The following procedure provides one of the way to configure the Audit Connector.

- 1 Right-click the Identity Manager Collector, then click **Add Connector**.
- 2 Select **View Compatible Connection Methods Only**.
- 3 Select **NetIQ Audit** from the list of installed connectors, then click **Next**.
- 4 Select the Event Source server to add to the Audit Connector, then click **Next**. Click **Add** to add an Event Source server manually.  
The Event Source server is the server that is running the Platform Agent and Identity Manager.
- 5 Use the default policy or create a custom policy to automatically add or exclude individual source devices, then click **Next**.  
For more information, see “Auto Configuring Event Sources” in the [Audit Connector Guide](#).
- 6 Finish the configuration of the connector with the following information, then click **Finish**.
  - ♦ **Name:** Specify a name for this connector.

- ♦ **Run:** Select whether the connector is started whenever the Collector Manager is started.
- ♦ **Alert if no data received in specified time period:** (Optional) Select this option to send the No Data Alert event to Sentinel if not data is received by the connector in the specified time period.
- ♦ **Limit Data Rate:** (Optional) Set a maximum limit on the rate of data the connector sends to Sentinel. If the data rate limit is reached, Sentinel throttles back on the source in order to limit the flow of data.
- ♦ **Set Filter:** (Optional) Specify a filter on the raw data passing through the connector.
- ♦ **Copy Raw Data to a File:** (Optional) Save the raw data passing through this connector to a file for further analysis.

Proceed to [Chapter 5, “Installing and Configuring the Platform Agent,”](#) on page 21.

## Installing and Configuring the Syslog Connector

To install the Syslog Connector,

- 1 Download the latest Syslog Connector (.zip file) from the [Sentinel Plug-ins Web site](#) to the server where the Sentinel Control Center is running.  
The Syslog Connector is located under the **Connectors** tab.
- 2 Log in to the Sentinel Control Center.
- 3 Select **Event Source Management > Live View**, then select **Tools > Import plugin**.
- 4 Select **Import Collector Script or Connector plugin package file (.zip)** option, then click **Next**.
- 5 Browse to and select the .zip file you just downloaded, then click **Next**.  
You must use the latest plug-ins available from the [Sentinel Plug-ins Web site](#).
- 6 Follow the remaining prompts, then click **Finish**.

For upgrading the Syslog Connector, see the [Sentinel Plug-ins Web site](#).

You can configure the `auditlogconfig.properties` file to enable the Syslog Connector to receive messages sent from Identity Manager. These events are then processed by the Identity Manager Collector.

There are multiple ways to configure the Syslog Connector. The following instructions use the right-click menu items on the Event Source Management Graph view.

- 1 Right-click the **<Name of the Collector>**, then click **Add Connector**.
- 2 Select **View Compatible Connection Methods Only**.
- 3 Select **Syslog** from the list of installed connectors, then click **Next**.
- 4 Select the Event Source Server (UDP, TCP, or SSL), then click **Next**. Click **Add** to add an Event Source server manually.
- 5 Finish the configuration of the connector with the following information, then click **Finish**.
  - ♦ **Name:** Specify a name for this connector.
  - ♦ **Run:** Select whether the connector is started whenever the Collector Manager is started.
  - ♦ **Alert if no data received in specified time period:** (Optional) Select this option to send the No Data Alert event to Sentinel if not data is received by the connector in the specified time period.

- ♦ **Limit Data Rate:** (Optional) Set a maximum limit on the rate of data the connector sends to Sentinel. If the data rate limit is reached, Sentinel throttles back on the source in order to limit the flow of data.
- ♦ **Set Filter:** (Optional) Specify a filter on the raw data passing through the connector.
- ♦ **Copy Raw Data to a File:** (Optional) Save the raw data passing through this connector to a file for further analysis.

By default, the Identity Manager installation process installs the required Syslog RPMs. For more information about enabling the Syslog Connector, see ["Understanding the auditlogconfig.properties File" on page 57](#).



# 5 Installing and Configuring the Platform Agent

The Platform Agent is the client portion of the Sentinel auditing system for Identity Manager. It receives logging information and system requests from Identity Manager and transmits the information to the NetIQ Audit Connector for NetIQ Sentinel.

- ♦ [“Installing the Platform Agent” on page 21](#)
- ♦ [“Configuring the Platform Agent Text File” on page 21](#)

## Installing the Platform Agent

The Platform Agent is automatically installed if **NetIQ Identity Manager Identity Manager Server**, **NetIQ Identity Manager Connected System**, or **Fanout Agent** option is selected during the Identity Manager installation.

The Platform Agent must be installed on every server running Identity Manager if you want to log Identity Manager events.

## Configuring the Platform Agent Text File

After you install Identity Manager, you can configure the Platform Agent. The Platform Agent’s configuration settings are stored in a simple, text-based `logevent` configuration file. By default, `logevent` file is located in the following directories:

*Table 5-1 Platform Agent Configuration File*

Operating System	File
Linux	<code>/etc/logevent.conf</code>
Solaris	<code>/etc/logevent.conf</code>
Windows	<code>\windows\logevent.cfg</code>

The following is a sample `logevent` file.

```

LogHost=127.0.0.1
LogCacheDir=c:\logcache
LogCachePort=1288
LogEnginePort=1289
LogCacheUnload=no
LogCacheSecure=yes
LogReconnectInterval=600
LogDebug=never
LogSigned=always
LogMaxBigData=3072
LogMaxCacheSize=2GB
LogCacheLimitAction=stop logging
ForceServerVersionNumber=1.0.0
LogJavaClassPath=/opt/novell/idm/rbpm/UserApplication/NAuditPA.jar

```

The entries in the `logevent` file are not case sensitive, entries can appear in any order, empty lines are valid, and any line that starts with a hash (#) is commented out.

You must add the following entry into the `logevent` file to log events for the User Application:

```
LogJavaClassPath=/opt/novell/idm/rbpm/UserApplication/NAuditPA.jar
```

The User Application installation copies this file into the correct directory, but the entry must be manually added to the `logevent` file.

The following table provides an explanation of each setting in the `logevent` file. The Platform Agent is used by Sentinel and Novell Audit. The documentation for the Platform Agent is in the [NetIQ Audit Administration Guide \(http://www.novell.com/documentation/novellaudit20/\)](http://www.novell.com/documentation/novellaudit20/).

---

**IMPORTANT:** You must restart the Platform Agent any time you make a change to the configuration.

---

*Table 5-2 logevent Settings*

Setting	Description
<code>LogHost=dns_name</code>	<p>The hostname or IP address of the Event Source Server where the Platform Agent sends events.</p> <p>In an environment where the Platform Agent connects to multiple hosts—for example, to provide load balancing or system redundancy—separate the IP address of each server with commas in the <code>LogHost</code> entry. For example,</p> <pre>LogHost=192.168.0.1,192.168.0.3,192.168.0.4</pre> <p>The Platform Agent connects to the servers in the order specified. If the first logging server goes down, the Platform Agent tries to connect to the second logging server, and so on.</p>
<code>LogCacheDir=path</code>	The directory where the Platform Agent stores the cached event information if the Event Source Server becomes unavailable.
<code>LogEnginePort=port</code>	The port at which the Platform Agent can connect to the Event Source Server. By default, this is port 1289.

Setting	Description
LogCachePort= <i>port</i>	<p>The port at which the Platform Agent connects to the Logging Cache Module. By default, this is port 1288.</p> <p>If the connection between the Platform Agent and the Event Source Server fails, Identity Manager continues to log events to the local Platform Agent. The Platform Agent simply switches into Disconnected Cache mode; that is, it begins sending events to the Logging Cache module (<i>lcache</i>). The Logging Cache module writes the events to the Disconnected Mode Cache until the connection is restored.</p> <p>When the connection to the Event Source Server is restored, the Logging Cache Module transmits the cache files to the Event Source Server. To protect the integrity of the data store, the Event Source Server validates the authentication credentials in each cache file before logging its events.</p>
LogCacheUnload=Y N	Set the parameter to <i>N</i> to prevent <i>lcache</i> from being unloaded.
LogCacheSecure=Y N	Set the parameter to <i>Y</i> to encrypt the local cache file.
LogReconnectInterval= <i>seconds</i>	The interval, in seconds, at which the Platform Agent and the Platform Agent Cache try to reconnect to the Event Source Server if the connection is lost. By default, this is 600.
LogDebug=Never Always	<p>The Platform Agent debug setting.</p> <ul style="list-style-type: none"> <li>◆ Set to <i>Never</i> to never log debug events.</li> <li>◆ Set to <i>Always</i> to always log debug events.</li> </ul>
LogSigned=Never Always	<p>The signature setting for Platform Agent events.</p> <p><b>IMPORTANT:</b> Sentinel can receive and map Audit signatures to a NetIQ Sentinel event field; however, Sentinel does not currently verify event signatures.</p> <ul style="list-style-type: none"> <li>◆ Set to <i>Never</i> to never sign or chain events.</li> <li>◆ Set to <i>Always</i> to always log events with a digital signature and to sequentially chain events.</li> </ul>
LogMaxBigData= <i>bytes</i>	The maximum size of the event data field. The default value is 3072 bytes. Set this value to the maximum number of bytes the client allows. Data that exceeds the maximum is truncated or not sent if the application doesn't allow truncated events to be logged.
LogMaxCacheSize= <i>bytes</i>	The maximum size, in bytes, of the Platform Agent cache file. By default, the maximum size is 2 GB. If this size is not specified, the log cache file continues to grow till 2 GB.
LogCacheLimitAction=stop logging drop cache	<p>The action that you want the cache module to take when it reaches the maximum cache size limit.</p> <ul style="list-style-type: none"> <li>◆ Set to <i>stop logging</i> if you want to stop collecting new events.</li> <li>◆ Set to <i>drop cache</i> if you want to delete the cache and start over with any new events that are generated.</li> </ul>

Setting	Description
ForceServerVersionNumber= <i>version number</i>	<p>To instruct the Platform Agent to use a particular Secure Log Server protocol version if events are logged to a log server from Nsure Audit version 1.0.x. The valid values are: 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.3.P1, 1.0.3.P2, and so on.</p> <p>If you are using patches from Nsure Audit 1.0.3, indicate the patch number being used, for example, P1, P2, P3, and so on. With Nsure Audit 1.0.3 Patch 2, the Secure Log Server properly reports the protocol in use and the NetIQ Audit 2.0.x Platform Agent automatically uses the protocol reported by the Secure Log Server.</p>
LogJavaClassPath	<p>The location of the NAuditPA.jar lcache file. For example:</p> <pre>LogJavaClassPath=/opt/novell/idm/rbpm/ UserApplication/NAuditPA.jar</pre>

---

**NOTE:** When you install and configure Identity Applications, by default, the `idmuserapp_logging.xml` file is created at `/opt/netiq/idm/apps/tomcat/conf` directory. You must manually add the following parameter in the file to ensure that the Naudit events for User Application are sent to Sentinel:

```
<param name="ApplicationDetail" value="DirXML"/>
```

---



# 6 Configuring Identity Manager Components to Log Audit Events in CEF Format

Identity Manager introduces Common Event Format (CEF), an open log management standard, for auditing events across all Identity Manager components. CEF enables you to use a common event log format so that auditing data can easily be collected and aggregated for further analysis. CEF format uses the Syslog message format as a transport mechanism.

The following Identity Manager components support auditing with CEF:

- ◆ Identity Vault (eDirectory)
- ◆ Identity Manager Engine
- ◆ Remote Loader
- ◆ .NET and Java Remote Loader
- ◆ Fanout Agent
- ◆ Identity Applications
- ◆ One SSO Provider (OSP)
- ◆ Self-Service Password Reset (SSPR)
- ◆ Data Collection Services (DCS)

---

**NOTE:** In Identity Manager 4.7, Identity Reporting does not support auditing through CEF and Platform Agent. Identity Reporting supports auditing through CEF from 4.7.1 onwards. For more information, see [Extended Support of Uniform Auditing for Identity Reporting](#) in the [NetIQ Identity Manager 4.7 Service Pack 1 Release Notes](#).

---

## Advantages of CEF

Previous versions of Identity Manager used a combination of different auditing solutions. Some components supported traditional auditing while others supported XDAS specification. Identity Manager 4.7 introduces CEF to provide a uniform auditing solution across all Identity Manager components that can help improve your experience of configuring and working with auditing.

CEF uses a standard Syslog message format that simplifies log management. This enables you to integrate disparate Identity Manager data in your enterprise. The new event format seamlessly integrates with Sentinel.

# Setting up CEF Configuration

After you install Identity Manager, ensure that all Identity Manager components are configured to generate the CEF events. To configure the components, see the following sections:

- ♦ “Configuring Identity Manager Engine” on page 26
- ♦ “Configuring Remote Loader” on page 27
- ♦ “Configuring .NET Remote Loader” on page 27
- ♦ “Configuring Java Remote Loader” on page 27
- ♦ “Configuring Fanout Agent” on page 27
- ♦ “Configuring Identity Applications” on page 28
- ♦ “Configuring Data Collection Services” on page 28
- ♦ “Configuring One SSO Provider” on page 29

---

**IMPORTANT:** If Identity Manager loses communication with the Sentinel server, Java Remote Loader, Fanout agent, and DCS events are not logged in the cache file for an approximate duration of two minutes. After the connection is restored, any cached events are sent to Sentinel after a delay of two minutes. There is no loss of events when Sentinel is normally shut down.

---

The CEF configuration settings are stored in a simple, text-based files for each component. For more information, see [Understanding the Properties Files for CEF Auditing](#).

Before configuring the Identity Manager components, ensure that the Identity Manager collector is configured in the Sentinel server. CEF support is introduced from Identity Manager collector version 2011.1r5 onwards. For information about installing and configuring the Identity Manager collector, see [Installing and Configuring the Identity Manager Collector](#).

## Configuring Identity Manager Engine


---

**NOTE:** After modifying the `auditlogconfig.properties` file, manually restart the Identity Vault.

---

The Identity Manager engine provides events for auditing.

To select events for auditing in CEF, use iManager.

- 1 Log in to iManager.
- 2 Select **Identity Manager Administration > Identity Manager Overview**.
- 3 Browse to and select the driver set object that contains the driver.
- 4 Select the driver set objects that contains the driver.
- 5 Click **Driver Set** and then click **Edit Driver Set properties**.
- 6 Click the **Log Level** tab, select the **Log specific events** radio button, and then click .
- 7 Select the **CEF** radio button.
- 8 Select the events you want to log and click **OK**.

By default, the `auditlogconfig.properties.template` for Identity Manager Engine is located in the following directories:

**Linux:** `/etc/opt/novell/eDirectory/conf/`

**Windows:** C:\netiq\edirectory

For the list of Identity Manager engine events, see [Engine Events](#).

## Configuring Remote Loader

By default, the `auditlogconfig.properties.template` for Remote Loader is located in the following directories:

**Linux:** `/etc/opt/novell/edirectory/conf/`

**Windows:** `\products\IDM\windows\setup\remoteloader\<processor_type>\`

---

**NOTE:** CEF logging in Remote Loader will be enabled only if the `auditlogconfig.properties` file exists.

---

For the list of Remote Loader events, see [Remote Loader Events](#).

## Configuring .NET Remote Loader

The .NET Remote Loader is applicable for Windows only.

By default, the `auditlogconfig.properties.template` for .NET Remote Loader is located at the `products\IDM\windows\setup\remoteloader.NET` directory.

## Configuring Java Remote Loader

---

**NOTE:** Ensure that the Rolling File Appender directory exists for Java Remote Loader. Otherwise, events are not logged.

---

The `auditlogconfig.properties.template` for Java Remote Loader is located in the following directories:

**Linux:** `<extracted loc of dirxml_jremote.tar.gz>/doc`

`dirxml_jremote.tar.gz` is located at `IDM/packages/java_remoteloader`

**Windows:** `<extracted loc of dirxml_jremote.tar.gz>/doc`

`dirxml_jremote.tar.gz` is located at `products/IDM/java_remoteloader`

To run the Java Remote Loader, specify the following command:

```
dirxml_jremote -config <Remote Loader configuration file> -auditlogfile /<PATH of the directory where auditlogconfig.properties file is located>/auditlogconfig.properties
```

For a list of Java Remote Loader events, see [Remote Loader Events](#).

## Configuring Fanout Agent

---

**NOTE:** Ensure that the Rolling File Appender directory exists for Fanout Agent. Otherwise, events are not logged.

---

When you run the Fanout agent for the first time, the `auditlogconfig.properties.template` file is created and located in the following directories:

**Linux:** `/opt/novell/dirxml/fanoutagent/config`

**Windows:** `<install-location>\FanoutAgent\config`

For the list of events, see [Fanout Agent Events](#).

## Configuring Identity Applications

The configuration settings for the identity applications logging are stored in the `idmuserapp_logging.xml` file, which is located by default in the following directories:

**Linux:** `/opt/netiq/idm/apps/tomcat/conf`

**Windows:** `C:\netiq\idm\apps\tomcat\conf`

---

**NOTE:** Restart Tomcat manually after configuring the `idmuserapp_logging.xml` file.

---

You must manually add the following in the `idmuserapp_logging.xml` file.

```
<appender class="com.netiq.idm.logging.syslog.CEFSyslogAppender" name="CEF">
  <param name="Threshold" value="ALL"/>
  <param name="Facility" value="user"/>
  <param name="SyslogHost" value="<IP address of your Sentinel server>"/>
  <param name="SyslogPort" value="<sentinel TCP port>"/>
  <param name="SyslogProtocol" value="ssl"/>
  <param name="SyslogSslKeystoreFile" value="/opt/netiq/idm/jre/lib/
security/cacerts"/>
  <param name="SyslogSslKeystorePassword" value="changeit"/>
  <param name="CacheDir" value="/opt/netiq/idm/apps/tomcat/cache"/>
  <param name="CacheRolloverSize" value="1024"/>
  <param name="ApplicationName" value="RBPM"/>
  <param name="EventPrefix" value="IDM:" />
</appender>
```

For the list of identity applications events, see [User Application Events](#).

## Configuring Data Collection Services

The configuration settings for DCS auditing is stored in the `idmrptdcs_logging.xml` file. By default, the file is located in the following directories:

---

**NOTE:** Once you configure the `idmrptdcs_logging.xml` file, restart Tomcat manually.

---

**Linux:** `/opt/netiq/idm/apps/tomcat/conf`

**Windows:** `C:\netiq\idm\apps\tomcat\conf`

---

**NOTE:** Ensure that you set the `novlua` permission for the Rolling File Appender directory and cache directory. Otherwise, Rolling File Appender or the cache directory will not work and no events will be logged. For example, you can change the permission and ownership of the directory using the `chown novlua:novlua <directorypath>` command, where `<directorypath>` is the Rolling File Appender path or cache file directory path.

---

For a list of DCS events, see [DCS Events](#).

## Configuring One SSO Provider

The configuration settings for OSP (One SSO Provider) must be performed through the configuration update utility. For more information on enabling CEF for OSP on Linux and Windows, see the following links:

- ◆ [Linux](#)
- ◆ [Windows](#)



# 7 Securing the Logging System

The Sentinel server and some of the Identity Manager components utilize embedded certificates generated by an internal Certificate Authority (CA). These SSL certificates ensure that communication between the Identity Manager instrumentation and the Sentinel server is secure.

To create a SSL certificate, perform the following actions:

- 1 Download the public certificate in `.der` format from the Sentinel server.

For example, if you are using Mozilla Firefox as your browser that already has a certificate, use the following procedure to download the certificate.

- 1a Launch the Sentinel Server in your browser.

- 1b Click **Show site information > View Certificate**.

- 1c Go to **Details** tab and export the certificate in `.der` format.

- 2 Add the certificate to the Java keystore.

For example, use the following command:

```
keytool -import -file PATH_OF_DERFile\PublicKeyCert.der -keystore  
KEYSTOERPATH\NAME.keystore -storepass keystorepass
```

The next step is to define which events to log. Proceed to [“Managing Identity Manager Events” on page 33](#).





# 8 Managing Identity Manager Events

The event information sent to NetIQ Sentinel is managed through product-specific instrumentations, or plug-ins. The Identity Manager Instrumentation allows you to configure which events are logged to your data store. You can select predefined log levels, or you can individually select the events you want to log. You can also add user-defined events to the Identity Manager schema.

The following sections review how to manage Identity Manager events:

- ◆ [“Selecting Events to Log” on page 33](#)
- ◆ [“User-Defined Events” on page 37](#)
- ◆ [“eDirectory Objects that Store Identity Manager Event Data” on page 40](#)

## Selecting Events to Log

The Identity Manager Instrumentation allows you to select events to be logged for the User Application, driver set, or a specific driver.

---

**NOTE:** Drivers can inherit logging configuration from the driver set.

---

- ◆ [Selecting Events for the User Application](#)
- ◆ [Selecting Events for the Driver Set](#)
- ◆ [Selecting Events for a Specific Driver](#)
- ◆ [Identity Manager Log Levels](#)

## Selecting Events for the User Application

The User Application enables you to change the log level settings of individual loggers and enable logging in Platform Agent and CEF format:

- 1 Log in to Identity Applications.
- 2 Select the **Application** tab.
- 3 Select the **Navigation and Access** link.
- 4 Click **Application Configuration** and then click **Logging**.

Alternatively, you can log in to the User Application (IDMPROV portal), select the **Administration** tab, and then click **Logging**.

### Logging Configuration

You can change the logging level by selecting a different level for the log and clicking the submit button.

Log Level	Log Name	Log Level	Log Name
Info ▼	com.novell	Info ▼	com.sssw
Info ▼	com.netiq	Info ▼	com.novell.afw.portal.aggregation
Info ▼	com.novell.afw.portal.persist	Info ▼	com.novell.afw.portal.portlet
Info ▼	com.novell.afw.portal.util	Info ▼	com.novell.afw.portlet.consumer
Info ▼	com.novell.afw.portlet.core	Info ▼	com.novell.afw.portlet.persist
Info ▼	com.novell.afw.portlet.producer	Info ▼	com.novell.afw.portlet.util
Info ▼	com.novell.afw.theme	Info ▼	com.novell.afw.util
Info ▼	com.novell.common.auth	Info ▼	com.novell.idm.security.authorization.service
Info ▼	com.novell.pwdmgt.actions	Info ▼	com.novell.pwdmgt.util
Info ▼	com.novell.pwdmgt.service	Info ▼	com.novell.pwdmgt.soap
Info ▼	com.novell.roa.resources	Info ▼	com.novell.soa.af.impl
Info ▼	com.novell.soa.script	Info ▼	com.novell.soa.ws.impl
Info ▼	com.novell.srvprv.apwa	Info ▼	com.novell.srvprv.impl.portlet
Info ▼	com.novell.srvprv.impl.portlet.util	Info ▼	com.novell.srvprv.impl.servlet
Info ▼	com.novell.srvprv.impl.uictrl	Info ▼	com.novell.srvprv.impl.vdata.model
Info ▼	com.novell.srvprv.impl.vdata.definition	Info ▼	com.novell.srvprv.spi
Info ▼	com.sssw.fw.cachemgr	Info ▼	com.sssw.fw.core
Info ▼	com.sssw.fw.directory	Info ▼	com.sssw.fw.event
Info ▼	com.sssw.fw.factory	Info ▼	com.sssw.fw.persist
Info ▼	com.sssw.fw.resource	Info ▼	com.sssw.fw.security
Info ▼	com.sssw.fw.server	Info ▼	com.sssw.fw.servlet
Info ▼	com.sssw.fw.session	Info ▼	com.sssw.fw.usermgr
Info ▼	com.sssw.fw.util	Info ▼	com.sssw.portal.manager
Info ▼	com.sssw.portal.persist	Info ▼	com.novell.idm.nrf.persist
Info ▼	com.novell.idm.nrf.service	Info ▼	com.novell.srvprv.impl.uictrl
Info ▼	com.novell.srvprv.spi.uictrl		

Add log level for package

Change log level of all above logs

Logging messages are being sent to audit service as well. Deselect the box below to stop sending logging messages to audit service.

Enable audit service

Select the box below to send logging messages in CEF format as well.

Enable CEF format

Select the box below to persist the logging changes.

Persist the logging changes

5 Select one of the following log levels for the listed logs.

Log Level	Description
Fatal	Writes Fatal level messages to the log.
Error	Writes Fatal and Error level messages to the log.
Warn	Writes Fatal, Error, and Warn level messages to the log.
Info	Writes Fatal, Error, Warn, and Info level messages to the log.
Debug	Writes Fatal, Error, Warn, Info, and debugging information to the log.
Trace	Writes Fatal, Error, Warn Info, debugging, and tracing information to the log.

- 6 Select the **Enable audit service** check box to send the events to Platform Agent.
- 7 Select **Enable CEF format** check box if you want to log the events in CEF format.  
For this option to work, you must add the Syslog appender in the `idmuserapplogging.xml` file during the installation of the User Application. For more information, see [Section 6, “Configuring Identity Manager Components to Log Audit Events in CEF Format,”](#) on page 25.
- 8 To save the changes for any subsequent application server restarts, select **Persist the logging changes**.
- 9 Click **Submit**.

The User Application logging configuration is saved in `/opt/netiq/idm/apps/tomcat/conf/idmuserapp_logging.xml`.

## Selecting Events for the Driver Set

- 1 In iManager, select **Identity Manager > Identity Manager Overview**.
- 2 Browse to and select the driver set object.
- 3 Click the driver set object in the list of driver sets, then click **Driver Set > Edit Driver Set properties**.
- 4 Click the **Log Level** tab, then select a log level for the driver set.  
For an explanation of each log level, see [Table 8-1, “Identity Manager Log Levels,”](#) on page 36.
- 5 Enable the **Turn off logging to Driver Set, Subscriber and Publisher logs** option to prevent logging audit events to eDirectory.  
Enabling this option improves the performance of the Identity Manager system.
- 6 Click **Apply** or **OK** to save your changes.

---

**NOTE:** Changes to configuration settings are logged by default.

---

## Selecting Events for a Specific Driver

- 1 In iManager, select **Identity Manager > Identity Manager Overview**.
- 2 Browse to and select the driver set object that contains the driver
- 3 Select the driver set from the list of driver sets.
- 4 Click the upper right corner of the driver icon, then select **Edit properties**.
- 5 Select the **Log Level** tab.

- 6 (Optional) By default, the Driver object is configured to inherit log settings from the Driver Set object. To select logged events for this driver only, deselect **Use log settings from the Driver Set**.

Use log settings from the Driver Set, DriverSet.novell

The following log settings are from the Driver Set and cannot be changed on this page. To modify the Driver Set's settings, [click here](#).

- 7 Enable the **Turn off logging to Driver Set, Subscriber and Publisher logs** option.  
Enabling this option improves the performance of the Identity Manager system.
- 8 Select a log level for the current driver.  
For an explanation of each log level, see [Table 8-1, "Identity Manager Log Levels," on page 36](#).
- 9 Click **Apply** or **OK** to save your changes.

---


**NOTE:** Changes to configuration settings are logged by default.

---

## Identity Manager Log Levels

The following table provides an explanation of the Identity Manager Instrumentation log levels:

*Table 8-1 Identity Manager Log Levels*

Option	Description
<b>Log errors</b>	<p>This is the default log level. The Identity Manager Instrumentation logs user-defined events and all events with an error status.</p> <p>You receive only events with a decimal ID of 196646 and an error message stored in the Text1 field.</p>
<b>Log errors and warnings</b>	<p>The Identity Manager Instrumentation logs user-defined events and all events with an error or warning status.</p> <p>You receive only events with a decimal ID of 196646 or 196647 and an error or warning message stored in the first text field.</p>
<b>Log specific events</b>	<p>This option allows you to select the Identity Manager events you want to log.</p> <p>Click  to select the specific events you want to log. After you select the events you want to log, click <b>OK</b>.</p> <p>To log events through Platform Agent, select the <b>Novell Audit</b> radio button. To log the events in CEF format, select the <b>CEF</b> radio button.</p> <p><b>NOTE:</b> User-defined events are always logged.</p> <p>For a list of all available events, see <a href="#">Appendix A, "Identity Manager Events," on page 45</a>.</p>
<b>Only update the last log time</b>	<p>The Identity Manager Instrumentation logs only user-defined events.</p> <p>When an event occurs, the last log time is updated so you can view the time and date of the last error in the status log.</p>
<b>Logging off</b>	<p>The Identity Manager Instrumentation logs only user-defined events.</p>

Option	Description
<b>Turn off logging to DriverSet, Subscriber and Publisher logs</b>	Turns off logging to the Driver Set object, Subscriber, and Publisher logs.
<b>Maximum Number of Entries in the Log</b>	This setting allows you to specify the maximum number of entries to log in the status logs.

## User-Defined Events

Identity Manager enables you to configure your own events to log to NetIQ Sentinel. Events can be logged by using an action in the Policy Builder, or within a style sheet. Any information you have access to when defining policies can be logged.

User-defined events are logged any time logging is enabled and are never filtered by the Identity Manager engine. There are two different ways to generate user-defined events:


- ◆ [“Using Policy Builder to Generate Events” on page 37](#)
- ◆ [“Using Status Documents to Generate Events” on page 40](#)

## Using Policy Builder to Generate Events

- 1 In the Policy Builder, define the condition that must be met to generate the event, then select the **Generate Event** action.
- 2 Specify an event ID.  
Event IDs between 1000 and 1999 are allotted for user-defined events. You must specify a value within this range for the event ID when defining your own events. This ID is combined with the Identity Manager application ID of 003.
- 3 Select a log level.

Log levels enable you to group events based on the type of event being logged. The following predefined log levels are available:

Log Level	Description
log-emergency	Events that cause the Identity Manager engine or driver to shut down.
log-alert	Events that require immediate attention.
log-critical	Events that can cause parts of the Identity Manager engine or driver to malfunction.
log-error	Events describing errors that can be handled by the Identity Manager engine or driver.
log-warning	Negative events not representing a problem.
log-notice	Positive or negative events an administrator can use to understand or improve use and operation.
log-info	Positive events of any importance.
log-debug	Events of relevance for support or for engineers to debug the Identity Manager engine or driver.

- 4 Click the  icon next to the **Enter Strings** field to launch the Named String Builder.  
In the Named String Builder, you can specify the string, integer, and binary values to include with the event.
- 5 Use the Named String Builder to define the event values.

Strings			
<a href="#">Edit</a>   <a href="#">Append New String</a>   <a href="#">Remove...</a>			
<input type="checkbox"/> Name:*	text1	 String value:*	Operation Attribute("Given Name")
<input type="checkbox"/> Name:*	text2	 String value:*	Operation()
<input type="checkbox"/> Name:*	value1	 String value:*	"1000"

The Identity Manager event structure contains a target, a subTarget, three strings (text1, text2, text3), two integers (value1, value3), and a generic field (data). The text fields are limited to 256 bytes, and the data field can contain up to 3 KB of information, unless a larger data field is enabled in your environment.

The following table provides an explanation of the Identity Manager event structure:

Field	Description
<b>target</b>	<p>This field captures the event target.</p> <p>All eDirectory events store the event's object in the <b>Target</b> field.</p>
<b>target-type</b>	<p>This field specifies which predefined format the target is represented in. Defined values for this type are as follows:</p> <ul style="list-style-type: none"> <li>◆ 0: None</li> <li>◆ 1: Slash Notation</li> <li>◆ 2: Dot Notation</li> <li>◆ 3: LDAP Notation</li> </ul>
<b>subTarget</b>	<p>This field captures the subcomponent of the target that was affected by the event.</p> <p>All eDirectory events store the event's attribute in the <b>SubTarget</b> field.</p>
<b>text1</b>	The value of this field depends upon the event. It can contain any text string up to 255 characters.
<b>text2</b>	The value of this field depends upon the event. It can contain any text string up to 255 characters.
<b>text3</b>	The value of this field depends upon the event. It can contain any text string up to 255 characters.
<b>value1</b>	The value of this field depends upon the event. It can contain any numeric value up to 32 bits.
<b>value3</b>	The value of this field depends upon the event. It can contain any numeric value up to 32 bits.
<b>data</b>	<p>The value of this field depends upon the event. The default size of this field is 3072 characters.</p> <p>You can configure the size of this field in the LogMaxBigData value in <code>logevent.cfg</code>. This value does not set the size of the <b>Data</b> field, but it does set the maximum size that the Platform Agent can log. For more information, see <a href="#">Chapter 5, "Installing and Configuring the Platform Agent,"</a> on page 21.</p> <p>The maximum size of the <b>Data</b> field is defined by the database where the data is logged, so the size varies for each database that is used. If the size of the <b>Data</b> field logged by the Platform Agent exceeds the maximum size allowed by the database, the channel driver truncates the data in the <b>Data</b> field.</p> <p>If an event has more data than can be stored in the <b>String</b> and <b>Numeric</b> value fields, it is possible to store up to 3 KB of binary data in the <b>Data</b> field.</p>

6 Click **OK** to return to the Policy Builder to construct the remainder of your policy.

For more information and examples of the Generate Event action, see "[Generate Event](#)" in the *NetIQ Identity Manager - Using Designer to Create Policies* guide.

## Using Status Documents to Generate Events

Status documents generated through style sheets using the `<xsl:message>` element are sent to Sentinel with an event ID that corresponds to the status document level attribute. The level attributes and corresponding event IDs are defined in the following table:

*Table 8-2 Status Documents*

Status Level	Status Event ID
Success	EV_LOG_STATUS_SUCCESS (1)
Retry	EV_LOG_STATUS_RETRY (2)
Warning	EV_LOG_STATUS_WARNING (3)
Error	EV_LOG_STATUS_ERROR (4)
Fatal	EV_LOG_STATUS_FATAL (5)
User Defined	EV_LOG_STATUS_OTHER (6)

The following example generates an event 0x004 and value1=7777, with a level of EV\_LOG\_STATUS\_ERROR:

```
<xsl:message>
  <status level="error" text1="This would be text1" value1="7777">This data would
be in the blob and in text 2, since no value is specified for text2 in the
attributes.</status>
</xsl:message>
```

The following example generates an event 0x004 and value1=7778, with a level of EV\_LOG\_STATUS\_ERROR:

```
<xsl:message>
  <status level="error" text1="This would be text1" text2="This would be text2"
value1="7778">This data would be in the blob only for this case, since a value for
text2 is specified in the attributes.</status>
</xsl:message>
```

## eDirectory Objects that Store Identity Manager Event Data

The Identity Manager events you want to log are stored in the DirXML-LogEvent attribute on the Driver Set object or Driver object. The attribute is a multi-value integer with each value identifying an event ID to be logged.

You do not need to modify these attributes directly, because these objects are automatically configured based on your selections in iManager.

Before logging an event, the engine checks the current event type against the content of the DirXML-LogEvent attribute to determine whether the event should be logged.

Drivers can inherit log settings from the driver set. The DirXML-DriverTraceLevel attribute of a Driver object has the highest precedence when determining log settings. If a Driver object does not contain a DirXML-DriverTraceLevel attribute, the engine uses the log settings from the parent driver set.



# 9 Using Status Logs

In addition to the functionality provided by Sentinel, Identity Manager logs a specified number of events on the driver set and the driver. These status logs provide a view of recent Identity Manager activity. After the log reaches the set size, the oldest half of the log is permanently removed to clear room for more recent events. Therefore, any events you want to track over time should be logged to Sentinel.

The following sections contain information on the Identity Manager logs:

- ♦ [“Setting the Log Level and Maximum Log Size” on page 41](#)
- ♦ [“Viewing Status Logs” on page 43](#)

## Setting the Log Level and Maximum Log Size

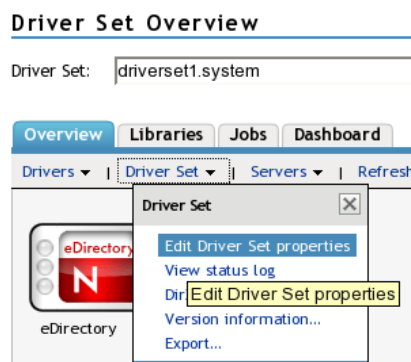
Status logs can be configured to hold between 50 and 500 events. This setting can be configured for the driver set to be inherited by all drivers in the driver set, or configured for each driver in the driver set. The maximum log size operates independently of the events you have selected to log, so you can configure the events you want to log for the driver set, then specify a different log size for each driver in the set.

This section reviews how to set the maximum log size on the driver set or an individual driver:

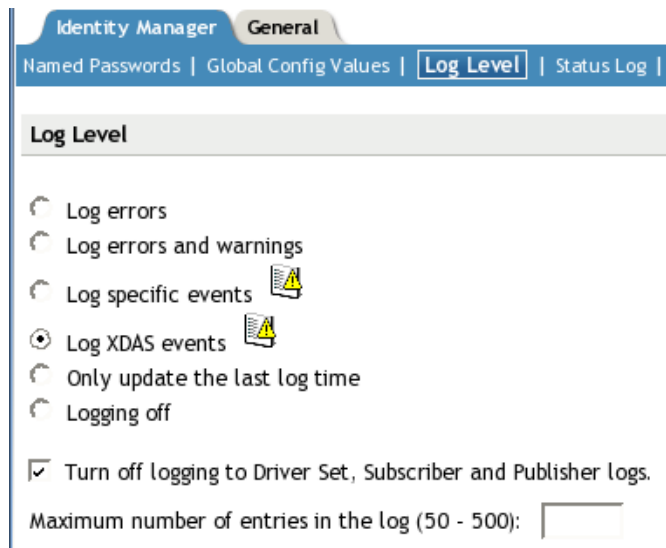
- ♦ [“Setting the Log Level and Log Size for the Driver Set” on page 41](#)
- ♦ [“Setting the Log Level and Log Size for the Driver” on page 42](#)

## Setting the Log Level and Log Size for the Driver Set

- 1 In iManager, select **Identity Manager > Identity Manager Overview**.
- 2 Browse to and select the driver set.
- 3 Click the driver set name to access the driver set overview page.
- 4 Select **Driver Set > Edit Driver Set properties**.



- 5 Select **Log Level**.



- 6 Enable the **Turn off logging to Driver Set, Subscriber and Publisher logs** option to prevent logging audit events to eDirectory.

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

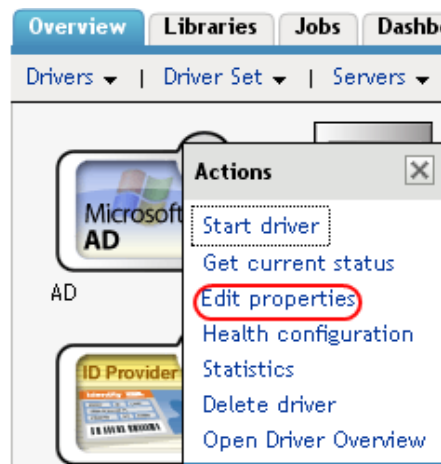
- 7 Specify the maximum log size in the **Maximum number of entries in the log** field:

Maximum number of entries in the log (50 - 500):

- 8 After you have specified the maximum number, click **OK**.

## Setting the Log Level and Log Size for the Driver

- 1 In iManager select **Identity Manager > Identity Manager Overview**.
- 2 Browse to and select the driver set.
- 3 Click the driver set to access the driver set overview page.
- 4 Click the upper right corner of the driver icon, then select **Edit properties**.



- 5 Select **Log Level**.

- 6 Deselect **Use log settings from the driver set** option, if it is selected.
- 7 Specify the maximum log size in the **Maximum number of entries in the log** field:

Maximum number of entries in the log (50 - 500):

- 8 After you have specified the maximum number, click **OK**.

## Viewing Status Logs

The status logs are short-term logs for the driver set, the Publisher channel, and the Subscriber channel. They are accessed through different locations in iManager.

- ♦ [“Accessing the Driver Set Status Log” on page 43](#)
- ♦ [“Accessing the Publisher Channel and Subscriber Channel Status Logs” on page 44](#)

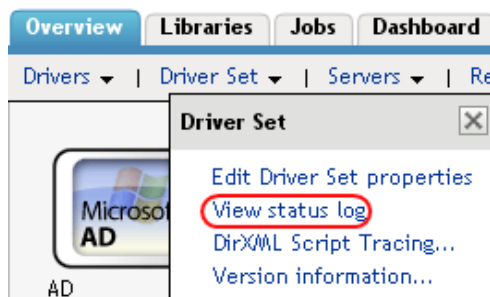
## Accessing the Driver Set Status Log

The status log for the driver set contains only messages generated by the engine, such as state changes for any drivers in the driver set. All engine messages are logged. There are two ways to access the driver set status log:

- ♦ [“Viewing the Log from the Driver Set Overview Page” on page 43](#)
- ♦ [“Viewing the Log from the Driver Overview Page” on page 43](#)

## Viewing the Log from the Driver Set Overview Page

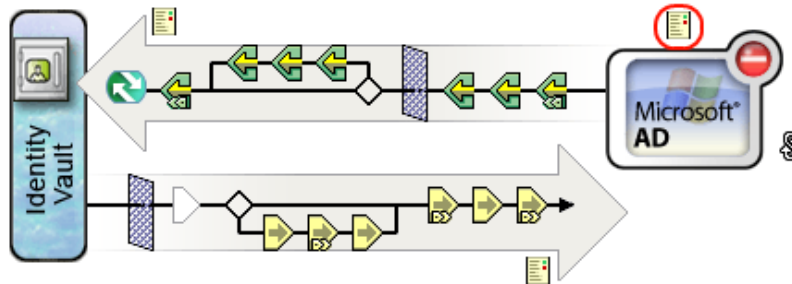
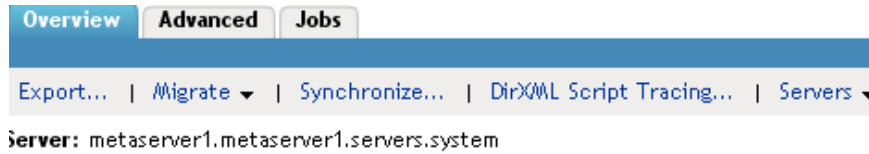
- 1 In iManager, select **Identity Manager > Identity Manager Overview**.
- 2 Browse to and select the driver set.
- 3 Click the driver set to access the driver set overview page.
- 4 Select **Driver Set > View status log**.



## Viewing the Log from the Driver Overview Page

- 1 In iManager, select **Identity Manager > Identity Manager Overview**.
- 2 Browse to and select the driver set.
- 3 Click the driver set to access the driver set overview page, then click any driver.  
The status log for the driver is stored on the driver overview page for each driver.

- 4 Click the Driver Set Status Log icon above the driver object.

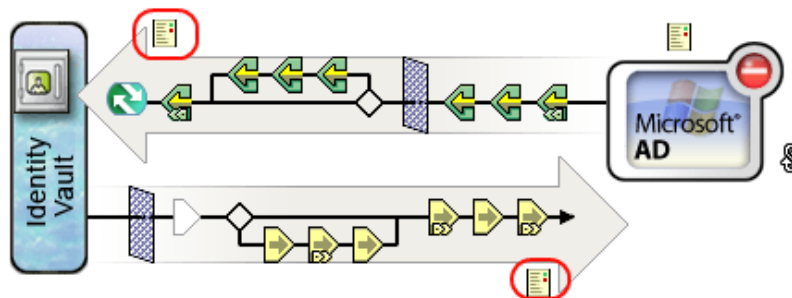
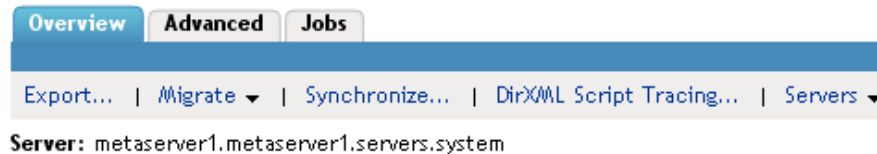


## Accessing the Publisher Channel and Subscriber Channel Status Logs

The status logs for the Publisher and Subscriber channels report channel-specific messages generated by the driver, such as an operation veto for an unassociated object.

To access the Publisher channel and the Subscriber channel logs:

- 1 In iManager, select **Identity Manager > Identity Manager Overview**.
- 2 Browse to and select the driver set.
- 3 Click the driver set to access the driver set overview page.
- 4 Click the desired driver object.
- 5 Click the Publisher channel or the Subscriber channel status log icon.



# A

## Identity Manager Events

This section provides a listing of all events logged by Identity Manager.

- ◆ [“CEF Events” on page 45](#)
- ◆ [“Event Structure” on page 49](#)
- ◆ [“Remote Loader Events” on page 49](#)
- ◆ [“Engine Events” on page 49](#)
- ◆ [“Fanout Agent Events” on page 52](#)
- ◆ [“User Application Events” on page 52](#)
- ◆ [“DCS Events” on page 55](#)

### CEF Events

The following table lists the CEF events that can be audited through Sentinel:

*Table A-1 CEF Events*

CEF Event ID	Description	Trigger
00030001	Status Success	Many different events can cause the status success event to occur. It usually signifies that an operation was successfully completed.
00030002	Status Retry	Many different events can cause the status retry event to occur. It signifies an operation was not completed and the operation must be tried again later.
00030003	Status Warning	Many different events can cause the status warning event to occur. It usually signifies that an operation was completed with minor problems.
00030004	Status Error	Many different events can cause the status error event to occur. It usually signifies that an operation was not completed successfully.
00030005	Status Fatal	Many different events can cause the status fatal event to occur. It usually signifies that an operation was not completed successfully and the engine or driver could not continue.

CEF Event ID	Description	Trigger
00030006	Status Other	Any status document processed with a level other than the five previously defined creates a status other event. These events can only be generated within a style sheet or rule.
00030026	DirXML Error	Generated whenever the engine throws an internal error.
00030027	DirXML Warning	Generated whenever the engine throws an internal warning.
00030028	Custom Operation	Occurs when an unknown operation appears in an input document. An example of known operations would be an add, delete, or modify.
00030008	Add Entry	Occurs when an object is added.
0003002F	Add Value - Add Entry	Occurs when a value is added during the creation of an object.
0003002E	Reset Attributes	Occurs when a Reset document is issued on the publisher or Subscriber channels.
0003002A	Add Value - Modify Entry	Occurs when a value is added during the modification of an object.
0003002B	Remove Value	Occurs when a modify operation contains a remove-value element.
00030029	Clear Attribute	Occurs when a modify operation contains a remove-all-value element.
00030009	Delete Entry	Occurs when an object is deleted.
000307DB	Cache Utility	
00030007	Search	Occurs when a query document is sent to the Identity Manager engine or driver.
0003000F	Query Schema	Occurs when a query schema operation is sent to the Identity Manager engine or driver.
0003000A	Modify Entry	Occurs when an object is modified.
0003000B	Rename Entry	Occurs when an object is renamed.
0003002C	Merge Entries	Occurs when two objects are being merged.
0003000C	Move Entry	Occurs when an object is moved.

CEF Event ID	Description	Trigger
0003000D	Add Association	Occurs when an association is added. It can happen on an add or a match.
0003000E	Remove Association	When an object is deleted, there is no remove association event. The remove association occurs when a User object is deleted in the disparate application, and the delete is then converted into a modify that removes the association.
00030020	Resync Driver	Occurs when a resync request is issued.
00030014	Input XML Document	Generated whenever an input document is created by the engine or driver.
00030015	Input Transformation Document	Generated after the input transformation policies are processed, allowing the user to view the transformed document.
00030016	Output Transformation Document	Generated after the output transformation policies are processed, allowing the user to view the transformed document.
00030017	Event Transformation Document	Generated after the event transformation policies are processed, allowing the user to view the transformed document.
00030018	Placement Rule Transformation Document	Generated after the Placement rule policies are processed, allowing the user to view the transformed document.
00030019	Create Rule Transformation Document	Generated after the Create rule policies are processed, allowing the user to view the transformed document.
0003001A	Input Mapping Rule Transformation Document	Generated after the Schema Mapping rules are processed which convert the document to the eDirectory schema.
0003001B	Output Mapping Rule Transformation Document	Generated after the Schema Mapping rules are processed which convert the document to the applications schema.
0003001C	Matching Rule Transformation Document	Generated after the Matching rule policies are processed, allowing the user to view the transformed document.

CEF Event ID	Description	Trigger
0003001D	Command Transformation Document	Generated after the command transformation policies are processed, allowing the user to view the transformed document.
0003001E	Publisher Filter Transformation Document	Generated after processing the notify filter on the Publisher channel, allowing the user to view the transformed document.
0003001F	User Agent Request	Occurs when a User Agent XDS command document is sent to the Driver on the Subscriber channel.
00030021	Migrate	Occurs when a migrate request is issued.
00030022	Driver Start	Occurs when a driver is started.
00030023	Driver Stop	Occurs when a driver is stopped.
00030010	Check Password	Manual function that is initiated via iManager to check the status of the user's password.
00030011	Check Object Password	Occurs when a request is issued to check an object's password, other than the driver.
00030013	Sync	Occurs when a sync event is requested.
0003002D	Get Named Password	Generated on a Get Named Password operation.
00030012	Change Password	Occurs when a request is issued to change the driver's password.
00030024	Password Sync	Generated when setting the distribution or simple password on an object.
00030025	Password Reset	Generated when resetting the connected application password after a failed password sync operation.
00030030	Set SSO Credential	Occurs when a driver policy executes the do-set-sso-credential action.
00030031	Clear SSO Credential	Occurs when a driver policy executes the do-clear-sso-credential action.
00030032	Set SSO Passphrase	Occurs when a driver policy executes the do-clear-sso-credential action.



# Event Structure

All events logged through Sentinel have a standardized set of fields. This allows Sentinel to log events to a structured database and query events across all logging applications.

Identity Manager events provide information in the following field structure:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature  
ID|Name|Severity|Extension
```

## Remote Loader Events

The following table lists the Remote Loader events that can be audited through Sentinel:

*Table A-2 Remote Loader Events*

Event ID	Description	Trigger
0030BB8	Remote Loader Start	Occurs when the Remote Loader starts.
0030BB9	Remote Loader Stop	Occurs when the Remote Loader stops.
0030BBA	Remote Loader Connection Established	Occurs when the engine establishes a TCP connection with the Remote Loader.
0030BBB	Remote Loader Connection Dropped	Occurs when the engine-to-Remote Loader connection is lost.
0030026	Command Port is already in use	Occurs when you try to start the remote loader when it is already running.
	Invalid Response to challenge during command authentication	Occurs when you specify an incorrect password.

## Engine Events

The following table lists the engine events that can be audited through Sentinel:

*Table A-3 Engine Events*

Event ID	Description	Trigger
0030001	Status Success	Many different events can cause the status success event to occur. It usually signifies that an operation was successfully completed.
0030002	Status Retry	Many different events can cause the status retry event to occur. It signifies an operation was not completed and the operation must be tried again later.
0030003	Status Warning	Many different events can cause the status warning event to occur. It usually signifies that an operation was completed with minor problems.
0030004	Status Error	Many different events can cause the status error event to occur. It usually signifies that an operation was not completed successfully.

<b>Event ID</b>	<b>Description</b>	<b>Trigger</b>
0030005	Status Fatal	Many different events can cause the status fatal event to occur. It usually signifies that an operation was not completed successfully and the engine or driver could not continue.
0030006	Status Other	Any status document processed with a level other than the five previously defined creates a status other event. These events can only be generated within a style sheet or rule.
0030007	Search	Occurs when a query document is sent to the Identity Manager engine or driver.
0030008	Add Entry	Occurs when an object is added.
0030009	Delete Entry	Occurs when an object is deleted.
003000A	Modify Entry	Occurs when an object is modified.
003000B	Rename Entry	Occurs when an object is renamed.
003000C	Move Entry	Occurs when an object is moved.
003000D	Add Association	Occurs when an association is added. It can happen on an add or a match.
003000E	Remove Association	When an object is deleted, there is no remove association event. The remove association occurs when a User object is deleted in the disparate application, and the delete is then converted into a modify that removes the association.
003000F	Query Schema	Occurs when a query schema operation is sent to the Identity Manager engine or driver.
0030010	Check User Password Status	Manual function that is initiated via iManager to check the status of the user's password.
0030011	Check Object Password	Occurs when a request is issued to check an object's password, other than the driver.
0030012	Change Password	Occurs when a request is issued to change the driver's password.
0030013	Sync	Occurs when a sync event is requested.
0030014	Input XML Document	Generated whenever an input document is created by the engine or driver.
0030015	Input Transformation Document	Generated after the input transformation policies are processed, allowing the user to view the transformed document.
0030016	Output Transformation Document	Generated after the output transformation policies are processed, allowing the user to view the transformed document.
0030017	Event Transformation Document	Generated after the event transformation policies are processed, allowing the user to view the transformed document.
0030018	Placement Rule Transformation Document	Generated after the Placement rule policies are processed, allowing the user to view the transformed document.
0030019	Create Rule Transformation Document	Generated after the Create rule policies are processed, allowing the user to view the transformed document.

Event ID	Description	Trigger
003001A	Input Mapping Rule Transformation Document	Generated after the Schema Mapping rules are processed which convert the document to the eDirectory schema.
003001B	Output Mapping Rule Transformation Document	Generated after the Schema Mapping rules are processed which convert the document to the applications schema.
003001C	Matching Rule Transformation Document	Generated after the Matching rule policies are processed, allowing the user to view the transformed document.
003001D	Command Transformation Document	Generated after the command transformation policies are processed, allowing the user to view the transformed document.
003001E	Publisher Filter Transformation Document	Generated after processing the notify filter on the Publisher channel, allowing the user to view the transformed document.
003001F	User Agent Request	Occurs when a User Agent XDS command document is sent to the Driver on the Subscriber channel.
0030020	Resync Driver	Occurs when a resync request is issued.
0030021	Migrate	Occurs when a migrate request is issued.
0030022	Driver Start	Occurs when a driver is started.
0030023	Driver Stop	Occurs when a driver is stopped.
0030024	Password Sync	Generated when setting the distribution or simple password on an object.
0030025	Password Reset	Generated when resetting the connected application password after a failed password sync operation.
0030026	DirXML Error	Generated whenever the engine throws an internal error.
0030027	DirXML Warning	Generated whenever the engine throws an internal warning.
0030028	Custom Operation	Occurs when an unknown operation appears in an input document. An example of known operations would be an add, delete, or modify.
0030029	Clear Attribute	Occurs when a modify operation contains a remove-all-value element.
003002A	Add Value - Modify Entry	Occurs when a value is added during the modification of an object.
003002B	Remove Value	Occurs when a modify operation contains a remove-value element.
003002C	Merge Entries	Occurs when two objects are being merged.
003002D	Get Named Password	Generated on a Get Named Password operation.
003002E	Reset Attributes	Occurs when a Reset document is issued on the publisher or Subscriber channels.
003002F	Add Value - Add Entry	Occurs when a value is added during the creation of an object.

Event ID	Description	Trigger
0030030	Set SSO Credential	Occurs when a driver policy executes the do-set-sso-credential action.
0030031	Clear SSO Credential	Occurs when a driver policy executes the do-clear-sso-credential action.
0030032	Set SSO Passphrase	Occurs when a driver policy executes the do-clear-sso-credential action.

## Fanout Agent Events

The following table lists the Fanout Agent events that can be audited through Sentinel:

*Table A-4 Fanout Agent Events*

Event ID	Description	Trigger
0030FA0	Fanout Agent Start	Occurs when the Fanout Agent starts.
0030FA1	Fanout Agent Stop	Occurs when the Fanout Agent stops.
0030FA2	Service Start, Instance Service	Occurs when the driver is started
0030FA3	Service Stop, Instance Service	Occurs when the driver is stopped.

## User Application Events

The following table lists the User Application events that can be audited through Sentinel:

*Table A-5 User Application Events*

Event ID	Description	Trigger
31400	Delete Entity	Occurs when an entity is deleted
31401	Update Entity	Occurs when an entity is updated
31410	Change Password Failure	Occurs when the password change fails
31411	Change Password Success	Occurs when the password change succeeds
31420	Forgotten Password Change Failure	Occurs when the forgotten password change fails
31421	Forgotten Password Change Success	Occurs when the forgotten password change succeeds
31550	Login Success	Occurs when the login succeeds
31551	Login Failure	Occurs when the login fails
31430	Search Request	Occurs when a search is initiated
31431	Search Saved	Occurs when a search is saved

<b>Event ID</b>	<b>Description</b>	<b>Trigger</b>
31440	Create Entity	Occurs when an entity is created
31450	Create Proxy Definition Success	Occurs when the creation of an entity definition succeeds
31451	Create Proxy Definition Failure	Occurs when the creation of an proxy definition fails
31452	Update Proxy Definition Success	Occurs when an update to the proxy definition fails
31453	Update Proxy Definition Failure	Occurs when an update to the proxy definition fails
31454	Delete Proxy Definition Success	Occurs when the proxy definition is deleted successfully
31455	Delete Proxy Definition Failure	Occurs when the proxy definition is not deleted successfully
31456	Create Delegatee Definition Success	Occurs when the creation of a delegatee definition succeeds
31457	Create Delegatee Definition Failure	Occurs when the creation of a delegatee definition fails
31458	Update Delegatee Definition Success	Occurs when an update to the delegatee definition succeeds
31459	Update Delegatee Definition Failure	Occurs when an update to the delegatee definition fails
003145A	Delete Delegatee Definition Success	Occurs when the delegatee definition is deleted successfully
003145B	Delete Delegatee Definition Failure	Occurs when the deletion of a delegatee definition fails
003145C	Create Availability Success	Occurs when the creation of an availability succeeds
003145D	Create Availability Failure	Occurs when the creation of an availability fails
3145	Delete Availability Success	Occurs when the deletion of an availability succeeds
003145F	Delete Availability Failure	Occurs when the deletion of an availability fails
31470	Digital Signature Verification Request	Occurs when a digital signature request is verified.
31471	Digital Signature Verification Failure	Occurs if a digital signature is invalid.
31472	Digital Signature Verification Success	Occurs upon successful verification of a digital signature.
31520	Workflow Error	Occurs when there is a workflow error
31521	Workflow Started	Occurs when the workflow starts
31522	Workflow Forwarded	Occurs when the workflow is forwarded

<b>Event ID</b>	<b>Description</b>	<b>Trigger</b>
31523	Workflow Reassigned	Occurs when the workflow is reassigned
31524	Workflow Approved	Occurs when the workflow is approved
31525	Workflow Refused	Occurs when the workflow is refused
31526	Workflow Ended	Occurs when the workflow ends
31527	Workflow Claimed	Occurs when the workflow is claimed
31528	Workflow Unclaimed	Occurs when the workflow is not claimed
31529	Workflow Denied	Occurs when the workflow is denied
003152A	Workflow Completed	Occurs when the workflow is completed
003152B	Workflow Timedout	Occurs when the workflow timed out
003152C	User Message	This is a user adhoc log message
003152D	Provision Error	Occurs when there is an error in the provisioning step
3152E	Provision Submitted	Occurs during the provisioning step on submission of entitlements.
003152F	Provision Success	Occurs during the provisioning step on successful completion of the step
31530	Provision Failure	Occurs during the provisioning step upon failure of the step
31531	Provision Granted	Occurs during the provisioning step on granting of an entitlement
31532	Provision Revoked	Occurs during the provisioning step on the revoking of an entitlement
31533	Workflow Retracted	Occurs when the workflow is retracted
31534	Workflow Escalated	Occurs when the workflow is escalated
31535	Workflow Reminder Sent	Occurs when reminders are sent to addressees of a workflow task
31536	Digital Signature	Occurs whenever a digital signature is passed to the workflow engine
31537	Workflow ResetPriority	Occurs when the priority of a workflow task is reset.
31538	Role Approved	Occurs when a role is approved
31539	Role Denied	Occurs when a role is denied
003153A	SOD Exception Approved	Occurs when an SOD exception is approved
003153B	SOD Exception Denied	Occurs when an SOD exception is denied
003153C	Start Correlated Workflow	Occurs when a correlated workflow is started
003153D	Role Request Submitted	Occurs when a role request is submitted
3153	Resource Approved	Occurs when a resource is approved
003153F	Resource Denied	Occurs when a resource is denied
31540	Provision Already Exists	
31541	Resource Request Submitted	Occurs when a request for a resource is submitted
31542	Resource Provisioning Workflow Submitted	Occurs when a resource provisioning workflow is submitted

Event ID	Description	Trigger
31543	Resource Provisioning Workflow Failed	Occurs when a resource provisioning workflow fails
31600	Role Provisioning	Occurs when a role is provisioned
31601	Role Provisioning Failure	Occurs when a role provisioning fails
31610	Role Request	Occurs when a role is requested
31611	Role Request Failure	Occurs when the request for a role fails
31612	Role Request Workflow	
31613	SOD Exception Auto Approval	Occurs when the SOD exception is auto approved
31614	Retract Role Request	Occurs when the role request is retracted
31615	Retract Role Request Failure	Occurs when the retraction of a role request fails
31620	Entitlement Grant	Occurs when the entitlement is granted
31621	Entitlement Grant Failure	Occurs when the entitlement grant fails
31622	Entitlement Revoke	Occurs when the entitlement is revoked
31623	Entitlement Revoke Failure	Occurs when the entitlement revoke fails

## DCS Events

The following table lists Data Collection Service events that can be audited through Sentinel:

*Table A-6 DCS Events*

Event ID	Description	Trigger
00031721	DCS Driver Registration Add	Occurs when the DCS driver is added
00031722	DCS Driver Registration Modify	Occurs when the DCS driver is modified
00031723	DCS Driver Collection enabled	Occurs when the data collection is enabled
00031724	DCS Driver Collection disabled	Occurs when the data collection is disabled
00031728	Data Collection Suspended	Occurs when the data collection is suspended
00031729	Data Collection Activated	Occurs when the data collection is activated
00031730	Data Collection Started	Occurs when the data collection is started
00031731	Data Collection Completed	Occurs when the data collection is completed
00031732	Data Collection Failed	Occurs when the data collection fails
00031733	Data Collection Requested	Occurs when the data collection is requested





# B Understanding the Properties Files for CEF Auditing

The appendix provides details about the properties files used by the different components of Identity Manager for auditing through CEF.

## Understanding the auditlogconfig.properties File

The following Identity Manager components use `auditlogconfig.properties` file to store the CEF configuration:

- ◆ Identity Vault
- ◆ Identity Manager Engine
- ◆ Java Remote Loader
- ◆ Fanout Agent

---

**NOTE:** Identity Vault and Identity Manager support only one Syslog method for auditing at a time. You can either use CEF or XDAS for auditing these components. NetIQ recommends you to use CEF instead of XDAS. XDAS will be deprecated in the future.

---

For information about the content of the audit properties file for each of these Identity Manager components, see the following sections:

- ◆ [“Identity Manager Engine, Remote Loader, and .NET Remote Loader” on page 57](#)
- ◆ [“Java Remote Loader and Fanout Agent” on page 61](#)

## Identity Manager Engine, Remote Loader, and .NET Remote Loader

---

**NOTE:** To generate XDAS events for Remote Loader and Fanout agent, you must rename the `auditlogconfig.properties` file to a different name. For example, `auditlogconfig.properties.temp`. If `auditlogconfig.properties` and `xdasconfig.properties` coexist on the same computer, only CEF events are generated for that component.

---

The following is a sample `auditlogconfig.properties` file for Identity Manager engine, Remote Loader, and .NET Remote Loader:

```

# Set the level of the root logger to DEBUG and attach appenders.
#log4j.rootLogger=debug, S, R

# Defines appender S to be a SyslogAppender.
#log4j.appender.S=org.apache.log4j.net.SyslogAppender

# Defines location of Syslog server.
#log4j.appender.S.Host=localhost
#log4j.appender.S.Port=port

# Specify protocol to be used (UDP/TCP/SSL)
#log4j.appender.S.Protocol=SSL

# Specify SSL certificate file for SSL connection.
# File path should be given with double backslash.
#log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem

# Minimum log-level allowed in syslog.
#log4j.appender.S.Threshold=INFO

# Defines the type of facility.
#log4j.appender.S.Facility=USER

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#log4j.appender.S.CacheEnabled=yes

# Cache location directory
# Directory should be available for creating cache files
#log4j.appender.S.CacheDir=/var/opt/novell/eDirectory

# Cache File Size
# Cache File size should be in the range of 50MB to 4000MB
#log4j.appender.S.CacheMaxFileSize=500MB

# Layout definition for appender Syslog S.
#log4j.appender.S.layout=org.apache.log4j.PatternLayout
#log4j.appender.S.layout.ConversionPattern=%c: %m%n

# Defines appender R to be a Rolling File Appender.
#log4j.appender.R=org.apache.log4j.RollingFileAppender

# Log file for appender R.
#log4j.appender.R.File=/var/opt/novell/eDirectory/log/cef-events.log

# Max size of log file for appender R.
#log4j.appender.R.MaxFileSize=100MB

# Set the maximum number of backup files to keep for appender R.
# Max can be 13. If set to zero, then there will be no backup files.
#log4j.appender.R.MaxBackupIndex=10

# Layout definition for appender Rolling log file R.
#log4j.appender.R.layout=org.apache.log4j.PatternLayout
#log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n

```

---

**NOTE:** By default, the appenders are disabled. You need to manually enable them.

---

Before using the `auditlogconfig.properties` file, NetIQ recommends you to review the following considerations:

- ◆ The letters S and R specify Syslog Appender and Rolling File Appender respectively.
- ◆ Entries in the `auditlogconfig.properties` file are not case sensitive.
- ◆ Entries in the `auditlogconfig.properties` file can appear in any order.
- ◆ Empty lines in the file are valid.
- ◆ Any line that starts with a hash (#) is commented out.

The following table provides an explanation of each property in the `auditlogconfig.properties` file:

Setting	Description
<code>log4j.rootLogger</code>	Sets the level of the root logger to debug and attaches an appender named R or S, where S specifies a Syslog appender and R specifies a Rolling File appender.
<code>log4j.appender.S</code>	Specifies the appender S to be a Syslog appender.
<code>log4j.appender.S.Host</code>	Specifies the location of the Syslog server where audit events are logged.
<code>log4j.appender.S.Port</code>	The port at which the Auditing server connects to the Syslog server.
<code>log4j.appender.S.Protocol</code>	If the connection between Auditing server and the Syslog server fails, Identity Manager cannot log events until the connection is restored.  Specifies the protocol to use. For example, UDP, TCP, or SSL. SSL is the default protocol. For enabling secure communication, see <a href="#">Chapter 7, "Securing the Logging System," on page 31</a> .
<code>log4j.appender.S.SSLCertFile</code>	Specifies the SSL certificate file for the SSL connection. Use double backslashes to specify the path of the file. This is an optional setting.
<code>log4j.appender.S.Threshold</code>	Specifies the minimum log level allowed in the Syslog appender. INFO is the only supported log level.
<code>log4j.appender.S.Facility</code>	Specifies the type of facility.
<code>log4j.appender.S.CacheEnabled</code>	Specifies caching for Syslog appender.
<code>log4j.appender.S.CacheDir</code>	Specifies the directory for storing the cache file.
<code>log4j.appender.S.CacheMaxFileSize</code>	Specifies the size of the cache file. The range is 50 MB to 4000 MB.
<code>log4j.appender.S.layout</code>	Layout setting for Syslog appender.
<code>log4j.appender.S.layout.ConversionPattern</code>	Layout setting for Syslog appender.
<code>log4j.appender.R</code>	Specifies appender R to be a Rolling File appender.
<code>log4j.appender.R.File</code>	The location of the log file for a Rolling File appender.

Setting	Description
log4j.appender.R.MaxFileSize	The maximum size, in MBs, of the log file for a Rolling File appender. Set this value to the maximum size that the client allows. This field accepts only integer value.  <b>NOTE:</b> The minimum size of the <code>MaxFileSize</code> parameter for the Rolling File appender is 50 MB.
log4j.appender.R.MaxBackupIndex	Specify the maximum number of backup files for a Rolling File appender. The maximum number of the backup files can be 10. A zero value means no backup files.
log4j.appender.R.layout	Layout setting for Rolling File appender.
log4j.appender.R.layout.ConversionPattern	Layout setting for Rolling File appender.

### Enabling the Syslog Appender

- 1 Change the following entry to S to attach a Syslog appender:

```
log4j.rootLogger=debug, S
```

- 2 Uncomment the following entries:

```
log4j.appender.S=org.apache.log4j.net.SyslogAppender
```

```
log4j.appender.S.Host=localhost
```

```
log4j.appender.S.Port=port
```

```
log4j.appender.S.Protocol=SSL
```

```
log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem
```

```
log4j.appender.S.Threshold=INFO
```

```
log4j.appender.S.Facility=USER
```

```
log4j.appender.S.layout=org.apache.log4j.PatternLayout
```

```
log4j.appender.S.layout.ConversionPattern%c: =%m%n
```

- 3 Log in to iManager and change the log events.

For more information on changing log levels by using iManager, see [“Setting the Log Level and Maximum Log Size” on page 41](#).

- 4 Restart eDirectory.

### Enabling the Rolling File Appender

The Rolling File appender is preferred, if the auditing solution is limited to an individual server. Rolling file appender is more reliable compared to the Syslog appender because it uses the file connector to send events from your local file system to the auditing server.

- 1 Change the following entry to R to attach a Rolling File appender:

```
log4j.rootLogger=debug, R
```

- 2 Uncomment the following entries:

```
log4j.appender.R=org.apache.log4j.RollingFileAppender
```

```
log4j.appender.R.File=/var/opt/novell/eDirectory/log/cef-events.log
```

```

log4j.appender.R.MaxFileSize=100MB
log4j.appender.R.MaxBackupIndex=10
log4j.appender.R.layout=org.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n

```

### 3 Log in to iManager and change log levels.

For more information on changing log levels by using iManager, see [“Setting the Log Level and Maximum Log Size” on page 41](#).

### 4 Restart eDirectory.

## Java Remote Loader and Fanout Agent

The following is a sample `auditlogconfig.properties` file for the Java Remote Loader and the Fanout agent.

```

# Defines location of Syslog server.
#SyslogHost=localhost
#SyslogPort=port

# Specify protocol to be used (UDP/TCP/SSL)
#SyslogProtocol=TCP

# Specify SSL keystore file for SSL connection.
# File path should be given with double backslash.
#SyslogSSLKeystoreFile=/opt/netiq/idm/jre/lib/security/cacerts

# Specify SSL keystore password for SSL connection.
#SyslogSSLKeystorePassword=password

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#CacheEnabled=yes

# Cache location directory
# Directory should be available for creating cache files
#CacheDir=/tmp/IDMcache

# Cache File Size
# Cache File size should be in the range of 50MB to 4000MB
#CacheRolloverSize=50

# Log file for appender
#FileAppenderFileName=/var/opt/novell/log/cef-events.log

```

The following table provides an explanation of each property in the `auditlogconfig.properties` file:

Setting	Description
SyslogHost	Specifies the location of the Syslog server where audit events are logged.

Setting	Description
SyslogPort	The port at which the Auditing server connects to the Syslog server.  If the connection between Auditing server and the Syslog server fails, Identity Manager cannot log events until the connection is restored.
SyslogProtocol	Specifies the protocol to use. For example, UDP, TCP, or SSL.
SyslogSSLKeystoreFile	Specifies the SSL certificate file for the SSL connection. Use double backslashes to specify the path of the file. This is an optional setting.
SyslogSSLKeystorePassword	Specifies the keystore password for the SSL connection.
CacheEnabled	Specifies caching for SyslogAppender. The values can be <b>yes</b> or <b>no</b> .
CacheDir	Specifies the directory for storing the cache file.
CacheRolloverSize	Specifies the size of the cache file. The range is 50 MB to 4000 MB.
FileAppenderFileName	Specifies the log file for appender.
AppendComponentName	Specifies whether you want to append the component name before the event message. You can set this option to <b>Yes</b> if you are using Sentinel as your auditing solution.

## Understanding the idmuserapp\_logging.xml File

The following is a sample of the `idmuserapp_logging.xml` file:

```
<logging xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="logging-config.xsd">

  <prefix>[RBPM]</prefix>

  <!-- example of enabling TRACE level -->
  <!--
  <logger name="com.novell.soa.af" additivity="true" level="TRACE"/>
  -->
  <!-- example of enabling Novell Audit Logging -->
  <!-- just add the Naudit appender to the level -->
  <!--
  <logger name="com.novell" additivity="true" level="INFO">
    <appender-ref ref="CONSOLE_DEBUG"/>
    <appender-ref ref="Naudit"/>
  </logger>
  -->

  <!-- Appender definitions -->
  <appenders>
    <!-- CONSOLE and FILE appender are defined in jboss-log4j.xml -->
    <!-- Novell Audit appender -->
    <appender class="com.netiq.logging.log4j.NauditLog4jAppender"
name="NAUDIT">
      <param name="Threshold" value="ALL"/>
    </appender>
  </appenders>
</logging>
```

```

        <param name="ApplicationDetail" value="DirXML"/>
    </appender>
    <!-- CEF appender -->
    <appender class="com.netiq.idm.logging.syslog.CEFSyslogAppender"
name="CEF">
        <param name="Threshold" value="ALL"/>
    </appender>
</appenders>

<!--
    Logger definitions

    NOTE: CONSOLE & FILE appenders should be defined in (jboss-)log4j.xml file.
    Additivity of true means the loggers defined below will inherit the
appenders.
-->
<loggers>
    <logger name="com.novell" level="INFO" additivity="true">
        <!-- remove this line to turn on Novell Audit
        <appender-ref ref="NAUDIT"/>
        remove this line to turn on Novell Audit -->
        <!-- remove this line to turn on CEF auditing
        <appender-ref ref="CEF"/>
        remove this line to turn on CEF auditing -->
    </logger>
    <logger name="com.sssw" level="INFO" additivity="true">
        <!-- remove this line to turn on Novell Audit
        <appender-ref ref="NAUDIT"/>
        remove this line to turn on Novell Audit -->
        <!-- remove this line to turn on CEF auditing
        <appender-ref ref="CEF"/>
        remove this line to turn on CEF auditing -->
    </logger>
    <logger name="com.netiq" level="INFO" additivity="true">
        <!-- remove this line to turn on Novell Audit
        <appender-ref ref="NAUDIT"/>
        remove this line to turn on Novell Audit -->
        <!-- remove this line to turn on CEF auditing
        <appender-ref ref="CEF"/>
        remove this line to turn on CEF auditing -->
    </logger>
    <logger name="com.novell.afw.portal.aggregation" level="INFO"
additivity="true"/>
    <logger name="com.novell.afw.portal.persist" level="INFO"
additivity="true"/>
    <logger name="com.novell.afw.portal.portlet" level="INFO"
additivity="true"/>
    <logger name="com.novell.afw.portal.util" level="INFO" additivity="true"/>
    <logger name="com.novell.afw.portlet.consumer" level="INFO"
additivity="true"/>
    <logger name="com.novell.afw.portlet.core" level="INFO" additivity="true"/>
    <logger name="com.novell.afw.portlet.persist" level="INFO"
additivity="true"/>
    <logger name="com.novell.afw.portlet.producer" level="INFO"
additivity="true"/>
    <logger name="com.novell.afw.portlet.util" level="INFO" additivity="true"/>
    <logger name="com.novell.afw.theme" level="INFO" additivity="true"/>
    <logger name="com.novell.afw.util" level="INFO" additivity="true"/>
    <logger name="com.novell.common.auth" level="INFO" additivity="true"/>
    <logger name="com.novell.idm.security.authorization.service" level="INFO"

```

```

additivity="true"/>
    <logger name="com.novell.pwdmgt.actions" level="INFO" additivity="true"/>
    <logger name="com.novell.pwdmgt.util" level="INFO" additivity="true"/>
    <logger name="com.novell.pwdmgt.service" level="INFO" additivity="true"/>
    <logger name="com.novell.pwdmgt.soap" level="INFO" additivity="true"/>
    <logger name="com.novell.roa.resources" level="INFO" additivity="true"/>
    <logger name="com.novell.soa.af.impl" level="INFO" additivity="true"/>
    <logger name="com.novell.soa.script" level="INFO" additivity="true"/>
    <logger name="com.novell.soa.ws.impl" level="INFO" additivity="true"/>
    <logger name="com.novell.srvprv.apwa" level="INFO" additivity="true"/>
    <logger name="com.novell.srvprv.impl.portlet" level="INFO"
additivity="true"/>
    <logger name="com.novell.srvprv.impl.portlet.util" level="INFO"
additivity="true"/>
    <logger name="com.novell.srvprv.impl.servlet" level="INFO"
additivity="true"/>
    <logger name="com.novell.srvprv.impl.uictrl" level="INFO"
additivity="true"/>
    <logger name="com.novell.srvprv.impl.vdata.model" level="INFO"
additivity="true"/>
    <logger name="com.novell.srvprv.impl.vdata.definition" level="INFO"
additivity="true"/>
    <logger name="com.novell.srvprv.spi" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.cachemgr" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.core" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.directory" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.event" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.factory" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.persist" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.resource" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.security" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.server" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.servlet" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.session" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.usermgr" level="INFO" additivity="true"/>
    <logger name="com.sssw.fw.util" level="INFO" additivity="true"/>
    <logger name="com.sssw.portal.manager" level="INFO" additivity="true"/>
    <logger name="com.sssw.portal.persist" level="INFO" additivity="true"/>
    <logger name="com.novell.idm.nrf.persist" level="INFO" additivity="true"/>
    <logger name="com.novell.idm.nrf.service" level="INFO" additivity="true"/>
    <logger name="com.novell.srvprv.impl.uictrl" level="INFO"
additivity="true"/>
    <logger name="com.novell.srvprv.spi.uictrl" level="INFO" additivity="true"/
>
    </loggers>
</logging>

```

## Understanding the idmrptdcs\_logging.xml File

The following is a sample of the idmrptdcs\_logging.xml file:



```

<logging>
<!--Defines location of Syslog server.-->
<!--
<SyslogHost>127.0.0.1</SyslogHost>
<SyslogPort>1468</SyslogPort>
-->

<!--Specify protocol to be used (UDP/TCP/SSL)-->
<!--
<SyslogProtocol>TCP</SyslogProtocol>
-->

<!--Specify SSL keystore file for SSL connection.
~ File path should be given with double backslash.
-->
!--
<SyslogSSLKeystoreFile>/opt/netiq/idm/jre/lib/security/cacerts</
SyslogSSLKeystoreFile>
-->

<!--Specify SSL keystore password for SSL connection. -->
<!--
<SyslogSSLKeystorePassword>password</SyslogSSLKeystorePassword>
-->

<!--Specify whether to append the component name before the event message
~ Inputs should be yes/no
~ If NetIQ Sentinel is the event listener, this option should be set to 'yes'
-->
<!--
<AppendComponentName>yes</AppendComponentName>
-->

<!--Defines caching for SyslogAppender.
~ Inputs should be yes/no
-->
<!--
<CacheEnabled>yes</CacheEnabled>
-->

<!--Cache location Directory
~ Directory should be available for creating cache files
~ Directory should have 'novlua' permission for caching to work correctly
-->
<!--
<CacheDir>/tmp/IDMcache</CacheDir>
-->

<!--Cache File Size
~ Cache File size should be in the range of 50MB to 4000MB
-->
<!--
<CacheRolloverSize>50</CacheRolloverSize>
-->

<!--Log file for appender

```

```
~ The directory containing the file specified should have 'novlua' permission to
work correctly.
-->
<!--
<FileAppenderFileName>/var/opt/netiq/idm/dcs-cache/cef-events.log</
FileAppenderFileName>
-->

<!--Max size of log file for file appender -->
<!--
<FileMaxRolloverSize>50</FileMaxRolloverSize>
-->

</logging>
```