AUTHORIZED DOCUMENTATION

Integration Guide For Novell Audit

Novell®
Identity Manager

3.6

July 23, 2008

www.novell.com

Legal Notices

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

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

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

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide 7

1 Overview 9

1.1 Novell Audit Integrated Architecture . . . 9

2 Installing and Configuring Novell Audit 11

2.1 Installing Novell Audit . . . 11
2.2 Configuring the Secure Logging Server . . . 11
2.3 Configuring the Data Store . . . 11
2.4 Configuring System Notifications . . . 11

3 Installing and Configuring the Platform Agent 13

3.1 Installing the Platform Agent . . . 13
3.2 Configuring the Platform Agent . . . 13

4 Managing Identity Manager Events 17

4.1 Selecting Events to Log . . . 17
4.1.1 Selecting Events for the User Application . . . 17
4.1.2 Selecting Events for the Driver Set . . . 19
4.1.3 Selecting Events for a Specific Driver . . . 20
4.1.4 Identity Manager Log Levels . . . 20
4.2 User-Defined Events . . . 21
4.2.1 Using Policy Builder to Generate Events . . . 21
4.2.2 Using Status Documents to Generate Events . . . 24
4.3 eDirectory Objects that Store Identity Manager Event Data . . . 25

5 Using Status Logs 27

5.1 Setting the Log Level and Maximum Log Size . . . 27
5.1.1 Setting the Log Level and Log Size for the Driver Set . . . 27
5.1.2 Setting the Log Level and Log Size for the Driver . . . 28
5.2 Viewing Status Logs . . . 29
5.2.1 Accessing the Driver Set Status Log . . . 29
5.2.2 Accessing the Publisher Channel and Subscriber Channel Status Logs . . . 30

6 Securing the Connection with Novell Audit 31

6.1 Updating the Novell Audit Certificate Infrastructure . . . 31
6.2 The Novell Audit AudCGen Utility . . . 32
6.3 Creating a Root Certificate for the Secure Logging Server . . . 35
6.3.1 Creating a Self-Signed Root Certificate for the Secure Logging Server . . . 35
6.3.2 Using a Third-Party Root Certificate for the Secure Logging Server . . . 35
6.4 Creating Logging Application Certificates . . . 36
6.4.1 Enabling the Identity Manager Instrumentation to Use a Custom Certificate . . . 36
6.5 Validating Certificates . . . 37

6.6 Securing Custom Certificates 37
6.6.1 Windows 38
6.6.2 Linux and Solaris 38

A Identity Manager Events 39

A.1 Event Structure 39
A.2 Error and Warning Events 39
A.3 Job Events 40
A.4 Remote Loader Events 40
A.5 Object Events 40
A.6 Password Events 41
A.7 Search List Events 41
A.8 Engine Events 41
A.9 Server Events 41
A.10 Security Events 41
A.11 Workflow Events 41
A.12 Driver Start and Stop Events 41

B Novell Audit Reports 43

B.1 Administrative Action Report 43
B.2 Historical Approval Flow Report 44
B.3 Resource Provisioning Report 46
B.4 Specific User Audit Trail Report I 48
B.5 Specific User Audit Trail Report II 50
B.6 Specific User Audit Trail III 52
B.7 Specific User Provisioning Report 54
B.8 User Provisioning Report 56

About This Guide

Welcome to the *Novell® Identity Manager Integration Guide for Novell Audit*. This guide provides the information necessary to integrate Novell Audit with Identity Manager to provide auditing and reporting services for Identity Manager.

- Chapter 1, “Overview,” on page 9
- Chapter 2, “Installing and Configuring Novell Audit,” on page 11
- Chapter 3, “Installing and Configuring the Platform Agent,” on page 13
- Chapter 4, “Managing Identity Manager Events,” on page 17
- Chapter 5, “Using Status Logs,” on page 27
- Chapter 6, “Securing the Connection with Novell Audit,” on page 31
- Appendix A, “Identity Manager Events,” on page 39
- Appendix B, “Novell Audit Reports,” on page 43

Audience

This guide is intended for network administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Identity Manager 3.6 Integration Guide for Novell Audit*, visit the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm36).

Additional Documentation

For the current Novell Audit documentation, see the Novell Audit Documentation Web site (http://www.novell.com/documentation/novellaudit20/index.html).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Overview

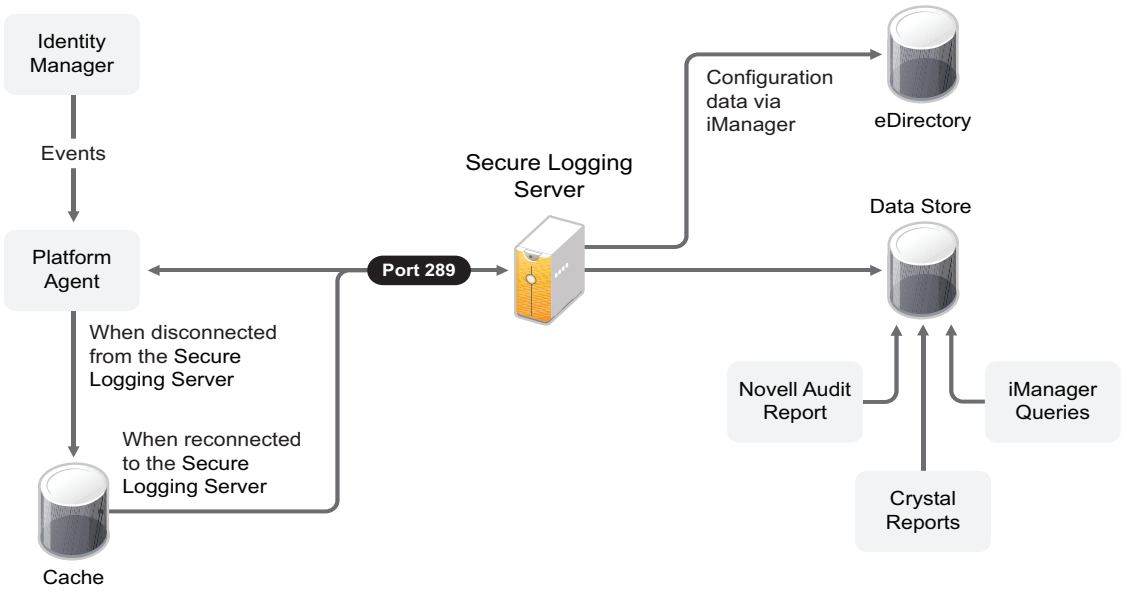
1

Adding Novell® Audit to you Identity Manager solution provides auditing and reporting services. By adding auditing and reporting, you can demonstrate that the business policies are implemented as designed with your Identity Manager solution.

1.1 Novell Audit Integrated Architecture

The following diagram illustrates the Identity Manager logging and reporting architecture when integrated with Novell Audit.

Figure 1-1 *Identity Manager and Novell Audit Integrated Architecture*



1. An Identity Manager event occurs and it is sent to the Platform Agent. To capture all Identity Manager events, the Platform Agent must be installed and configured on each Identity Manager server.
2. (Conditional) If the Platform Agent cannot connect to the Secure Logging Server, the events are stored in cache until the connection is reestablished.
3. The Platform Agents sends the event to the Secure Logging Server.
4. The Secure Logging Server sends the events to eDirectory™. Through iManager, you configure the objects that store the events.
5. The Secure Logging Server sends the event to the data store, which stores the events. The data store is a database that stores the events until they are needed.

   The stored events are displayed through Novell Audit reports and iManager queries.

For more information about the Novell Audit architecture, see "System Architecture" in the *Novell Audit 2.0 Administration Guide*.

Installing and Configuring Novell Audit

2

In order to audit the Identity Manager events, the Novell® Audit server must be installed into the same eDirectory™ tree. If you already have Novell Audit installed in your eDirectory tree, proceed to Section 2.2, "Configuring the Secure Logging Server," on page 11. If you do not have a Novell Audit server installed, continue with Section 2.1, "Installing Novell Audit," on page 11.

- Section 2.1, "Installing Novell Audit," on page 11
- Section 2.2, "Configuring the Secure Logging Server," on page 11
- Section 2.3, "Configuring the Data Store," on page 11
- Section 2.4, "Configuring System Notifications," on page 11

2.1 Installing Novell Audit

You should install Novell Audit on a different server than the server running Identity Manager. Auditing is an intensive process that depends upon how many events you are auditing and how many drivers are in your environment. For the installation instructions, see *Novell Audit 2.0 Installation Guide* (http://www.novell.com/documentation/novellaudit20/install/data/bktitle.html#bktitle).

2.2 Configuring the Secure Logging Server

Configure the Secure Logging Server to log Identity Manager events. For more information, see "Configuring the Secure Logging Server" (http://www.novell.com/documentation/novellaudit20/novellaudit20/data/al3p1eu.html#al3p1eu) in the *Novell Audit 2.0 Administration Guide*.

2.3 Configuring the Data Store

Configure the data store to store the Identity Manager events. For more information, see "Configuring the Data Store" (http://www.novell.com/documentation/novellaudit20/novellaudit20/data/al4gkai.html#al4gkai) in the *Novell Audit 2.0 Administration Guide*.

2.4 Configuring System Notifications

Novell Audit provides the ability to send a notification when a specific event occurs or does not occur. Notifications can be sent based on any value in one or more events. Notifications can be sent to any logging channel, enabling you to log notifications to a database, a Java* application or SNMP management system, or several other locations. For details on creating Novell Audit notifications based on Identity Manager events, see "Configuring Filters and Event Notifications" (http://www.novell.com/documentation/novellaudit20/index.html?page=/documentation/novellaudit20/novellaudit20/data/al0lg08.html#al0lg08) in the *Novell Audit 2.0 Administration Guide*.

Installing and Configuring the Platform Agent

3

The `logevent` Platform Agent is the client portion of the Novell® auditing system. It receives logging information and system requests from Identity Manager and transmits the information to either Novell Audit.

- Section 3.1, “Installing the Platform Agent,” on page 13
- Section 3.2, “Configuring the Platform Agent,” on page 13

3.1 Installing the Platform Agent

The Platform Agent is automatically installed if either the Novell *Identity Manager Metadirectory Server* or *Novell Identity Manager Connected System* option is selected during the Identity Manager installation. For more information on the Identity Manager installation, see the *Identity Manager 3.6 Installation Guide*.

IMPORTANT: The Platform Agent must be configured for every server running Identity Manager if you want to log Identity Manager events.

3.2 Configuring the Platform Agent

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` is located in the following directories:

Table 3-1 *Platform Agent Configuration File*

Operating System	File
Linux	`/etc/logevent.conf`
Solaris*	`/etc/logevent.conf`
Windows*	`\Windows_Directory\logevent.cfg` The `Windows_Directory` is usually `drive:\windows`.

The following is a sample `logevent.cfg` file.

```
LogHost=127.0.0.1
LogCacheDir=c:\logcache
LogCachePort=288
LogEnginePort=289
LogCacheUnload=no
LogReconnectInterval=600
LogDebug=never
LogSigned=always
```

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.

The following table provides an explanation of each setting in the `logevent` file.

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

Table 3-2 *logevent Settings*

Setting	Description
LogHost=*dns_name*	The hostname or IP address of the Novell Audit Secure Logging Server where the Platform Agent sends events. 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 LogHost entry. For example, `LogHost=192.168.0.1,192.168.0.3,192.168.0.4` 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. For more information on configuring multiple hosts, see "Configuring Multiple Secure Logging Servers" in the *Novell Audit 2.0 Administration Guide*.
LogCacheDir=*path*	The directory where the Platform Agent stores the cached event information if the Novell Audit Secure Logging Server becomes unavailable.
LogEnginePort=*port*	The port at which the Platform Agent can connect to the Novell Audit Secure Logging Server. By default, this is port 289.
LogCachePort=*port*	The port at which the Platform Agent connects to the Logging Cache Module. If the connection between the Platform Agent and the Secure Logging 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 (`lcache`). The Logging Cache module writes the events to the Disconnected Mode Cache until the connection is restored. When the connection to the Novell Audit Secure Logging Server is restored, the Logging Cache Module transmits the cache files to the Secure Logging Server. To protect the integrity of the data store, the Secure Logging Server validates the authentication credentials in each cache file before logging its events.
LogCacheUnload=Y|N	Set the parameter to `N` to prevent `lcache` from being unloaded.
LogCacheSecure=Y|N	Set the parameter to `Y` to encrypt the local cache file.

Setting	Description
LogReconnectInterval=*seconds*	The interval, in seconds, at which the Platform Agent and the Platform Agent Cache try to reconnect to the Novell Audit Secure Logging Server if the connection is lost.
LogDebug=Never|Always|Server	The Platform Agent debug setting. ◆ Set to `Never` to never log debug events. ◆ Set to `Always` to always log debug events. ◆ Leave out or set to `Server` to use the default setting provided by the *Log Debug Events* attribute in the Novell Audit Secure Logging Server *Configuration* page. **NOTE:** The `Server` option applies only to Novell Audit systems.
LogSigned=Never|Always|Server	The signature setting for Platform Agent events. ◆ Set to `Never` to never sign or chain events. ◆ Set to `Always` to always log events with a digital signature and to sequentially chain events. ◆ Leave out, or set to `Server` to use the default setting provided by the Sign Events attribute in the Novell Audit Secure Logging Server Configuration page. For more information on event signatures, see "Signing Events" in the *Novell Audit 2.0 Administration Guide*.
LogMaxBigData=*bytes*	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=*bytes*	The maximum size, in bytes, of the Platform Agent cache file.
LogCacheLimitAction=stop logging|drop cache	The action that you want the cache module to take when it reaches the maximum cache size limit. ◆ Set to `stop logging` if you want to stop collecting new events. ◆ Set to `drop cache` if you want to delete the cache and start over with any new events that are generated.

For complete information on the Novell Audit Platform Agent, see "Configuring the Platform Agent" in the *Novell Audit 2.0 Administration Guide*.

Managing Identity Manager Events

4

The event information sent to Novell® Audit ® 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:

- Section 4.1, “Selecting Events to Log,” on page 17
- Section 4.2, “User-Defined Events,” on page 21
- Section 4.3, “eDirectory Objects that Store Identity Manager Event Data,” on page 25

4.1 Selecting Events to Log

The Identity Manager Instrumentation allows you to select events to be logged for a driver set, a specific driver, or for the User Application. The User Application consists of the User Application driver, the Role Based Provisioning driver, and workflows.

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

The following sections document how to select events for the User Application, driver set, or a specific driver:

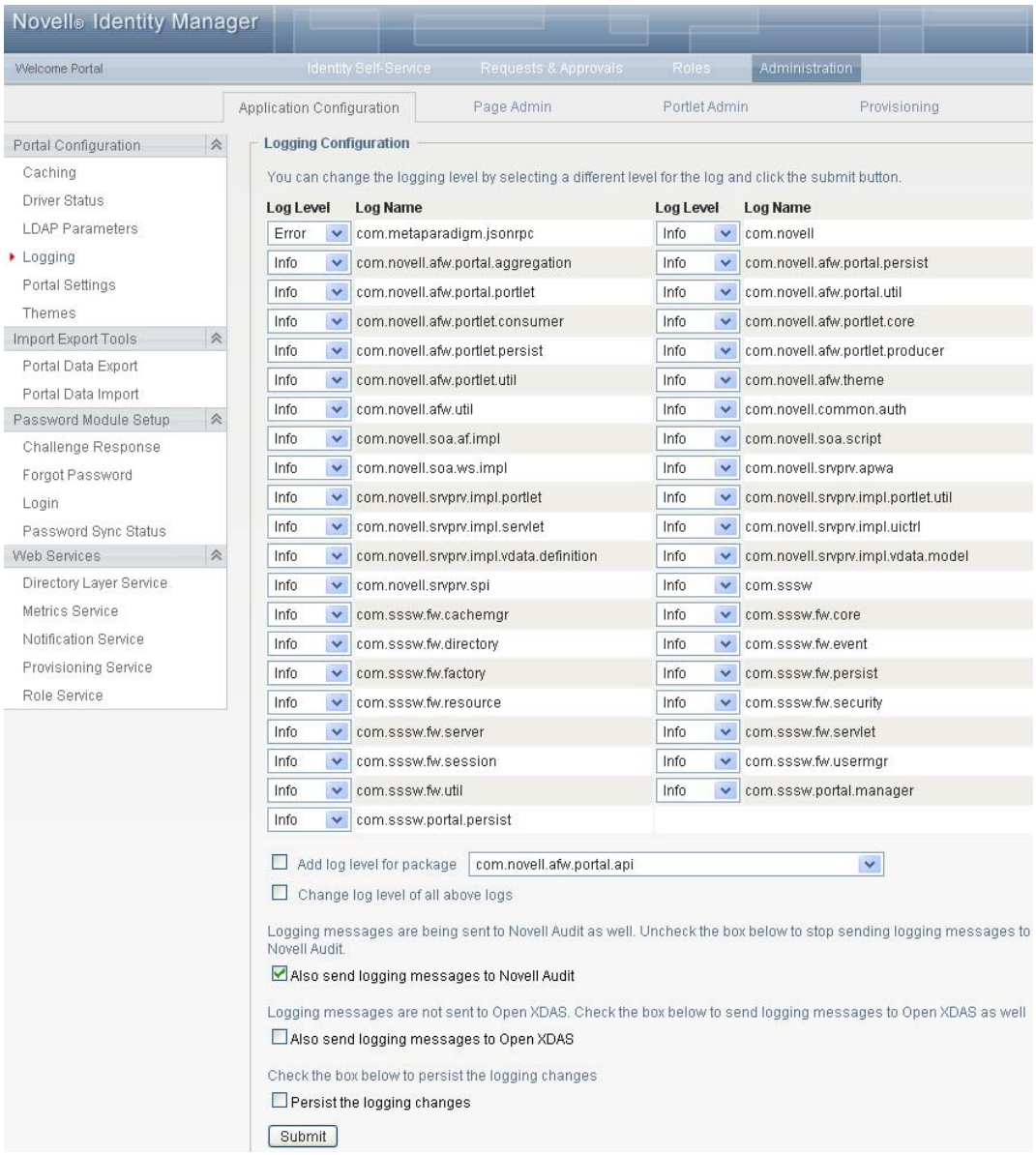
- “Selecting Events for the Driver Set” on page 19
- “Selecting Events for a Specific Driver” on page 20
- “Identity Manager Log Levels” on page 20

4.1.1 Selecting Events for the User Application

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

1. Log in to the User Application as the User Application Administrator.
2. Select the *Administration* tab.
3. Select the *Logging* link.

   The Logging Configuration page appears.



4 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.

5 Select the *Also send logging messages to Novell Audit* check box to send the events to the Platform Agent.

6 (Optional) Select *Also send logging messages to Open XDAS*, if you want to send the messages to Open XDAS.

For this option to work, you must select the open XDAS option during the installation of the User Application. For more information, see the *User Application Installation Guide* (http://www.novell.com/documentation/idmrbpm361/index.html).

7 To save the changes for any subsequent User Application server restarts, select *Persist the logging changes*.

8 Click *Submit*.

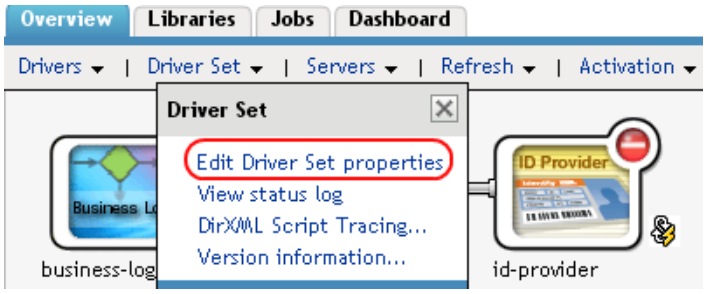
The User Application logging configuration is saved in `installdir/jboss/server/IDMProv/conf/idmuserapp_logging.xml`.

4.1.2 Selecting Events for the Driver Set

1 In iManager, select *Identity Manager* > *Identity Manager Overview*.

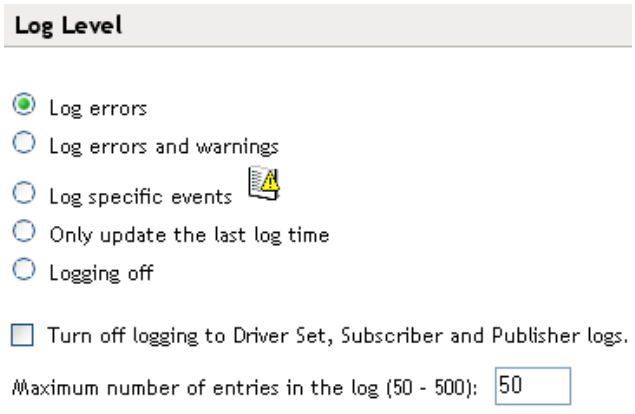
2 Browse to and select the driver set.

3 Click the driver set object in the list of driver sets, then click *Driver Set* > *Edit Driver Set properties*.



4 Select the *Log Level* tab, then select a log level for the driver set.

For an explanation of each log level, see "Identity Manager Log Levels" on page 20.

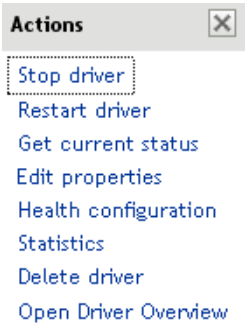


5 Click *Apply* or *OK* to save your changes.

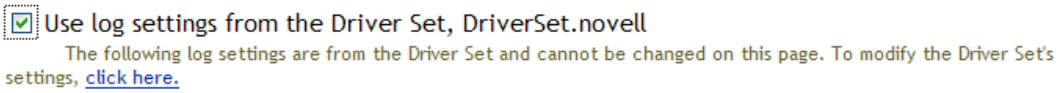
NOTE: Changes to configuration settings are logged by default.

4.1.3 Selecting Events for a Specific Driver

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



5. Select *Log Level* on the driver's properties page.
6. (Optional) By default, the Driver object is configured to inherit log settings from the Driver Set object. To log events for this driver only, deselect *Use log settings from the Driver Set*.



7. Select a log level for the current driver.

   For an explanation of each log level, see "Identity Manager Log Levels" on page 20.
8. Click *Apply* or *OK* to save your changes.

NOTE: Changes to configuration settings are logged by default.

4.1.4 Identity Manager Log Levels

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

Table 4-1 *Identity Manager Instrumentation Log Levels*

Option	Description
Log errors	This is the default log level. The Identity Manager Instrumentation logs user-defined events and all events with an error status. You receive only events with a decimal ID of 196646 and an error message stored in the Text1 field.

Option	Description
Log errors and warnings	The Identity Manager Instrumentation logs user-defined events and all events with an error or warning status. You receive only events with a decimal ID of 196646 or 196647 and an error or warning message stored in the first text field.
Log specific events	This option allows you to select the Identity Manager events you want to log. Click  to select the specific events you want to log. After you select the events you want to log, click *OK*. **NOTE:** User-defined events are always logged. For a list of all available events, see Appendix A, "Identity Manager Events," on page 39.
Only update the last log time	The Identity Manager Instrumentation logs only user-defined events. 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.
Logging off	The Identity Manager Instrumentation logs only user-defined events.
Turn off logging to DriverSet, Subscriber and Publisher logs	Turns off logging to the Driver Set object, Subscriber, and Publisher logs.
Maximum Number of Entries in the Log	This setting allows you to specify the maximum number of entries to log in the status logs. See Section 5.2, "Viewing Status Logs," on page 29 for details.

4.2 User-Defined Events

Identity Manager enables you to configure your own events to log to Novell Audit. 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 Metadirectory engine. There are two different ways to generate events:

- Section 4.2.1, "Using Policy Builder to Generate Events," on page 21
- Section 4.2.2, "Using Status Documents to Generate Events," on page 24

4.2.1 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.

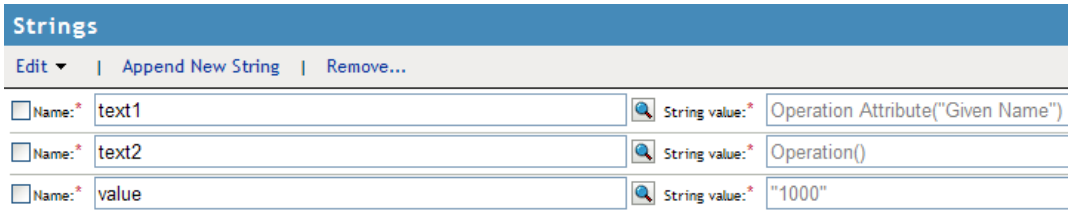
Log levels enable you to group events based on the type of event being logged. The following predefined log levels are available:

Log Level	Description
log-emergency	Events that cause the Metadirectory engine or driver to shut down.
log-alert	Events that require immediate attention.
log-critical	Events that can cause parts of the Metadirectory engine or driver to malfunction.
log-error	Events describing errors that can be handled by the Metadirectory 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 Metadirectory 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.



The Identity Manager event structure contains a target, a subTarget, three strings (text1, text2, text3), two integers (value, 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
target	This field captures the event target. All eDirectory™ events store the event's object in the *Target* field.
target-type	This field specifies which predefined format the target is represented in. Defined values for this type are as follows: ◆ 0: None ◆ 1: Slash Notation ◆ 2: Dot Notation ◆ 3: LDAP Notation
subTarget	This field captures the subcomponent of the target that was affected by the event. All eDirectory events store the event's attribute in the *SubTarget* field.
text1	The value of this field depends upon the event. It can contain any text string up to 255 characters. **NOTE:** The *Text1* field is vital to the function of the Novell Audit CVR driver. The CVR driver looks in the event's *Text1* and *Text2* fields to identify the defined attribute and object for a given policy. For more information, see "CVR" in the *Novell Audit 2.0 Administration Guide*.
text2	The value of this field depends upon the event. It can contain any text string up to 255 characters. **NOTE:** The *Text2* field is vital to the function of the Novell Audit CVR driver. The CVR driver looks in the event's *Text1* and *Text2* fields to identify the defined attribute and object for a given policy. For more information, see "CVR" in the *Novell Audit 2.0 Administration Guide*.
text3	The value of this field depends upon the event. It can contain any text string up to 255 characters.
value	The value of this field depends upon the event. It can contain any numeric value up to 32 bits.
value3	The value of this field depends upon the event. It can contain any numeric value up to 32 bits.

Field	Description
data	The value of this field depends upon the event. The default size of this field is 3072 characters. You can configure the size of this field in the LogMaxBigData value in `logevent.cfg`. This value does not set the size of the *Data* field, but it does set the maximum size that the Platform Agent can log. For more information, see Chapter 3, "Installing and Configuring the Platform Agent," on page 13. The maximum size of the *Data* 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 *Data* field logged by the Platform Agent exceeds the maximum size allowed by the database, the channel driver truncates the data in the *Data* field. If an event has more data than can be stored in the *String* and *Numeric* value fields, it is possible to store up to 3 KB of binary data in the *Data* field.

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 *Policies in Designer 3.0* guide.

4.2.2 Using Status Documents to Generate Events

Status documents generated through style sheets using the `<xsl:message>` element are sent to Novell Audit 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 4-2 *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" value="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 a Novell Audit 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>
```

4.3 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 or the driver. 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 contents 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 has the highest precedence when determining log settings. If a driver does not contain a DirXML-DriverTraceLevel attribute, the engine uses the log settings from the parent driver set.

Using Status Logs

5

In addition to the functionality provided by Novell® Audit, 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 Novell Audit.

The following sections contain information on the Identity Manager logs:

- Section 5.1, “Setting the Log Level and Maximum Log Size,” on page 27
- Section 5.2, “Viewing Status Logs,” on page 29

5.1 Setting the Log Level and Maximum Log Size

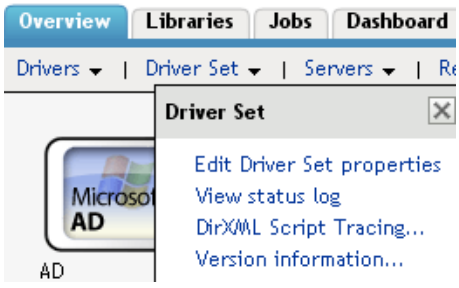
Status logs can be configured to hold between 50 and 500 events. This setting can be configured for the driver set to be inherited by all drivers in the driver set, or configured for each driver in the driver set. The maximum log size operates independently of the events you have selected to log, so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

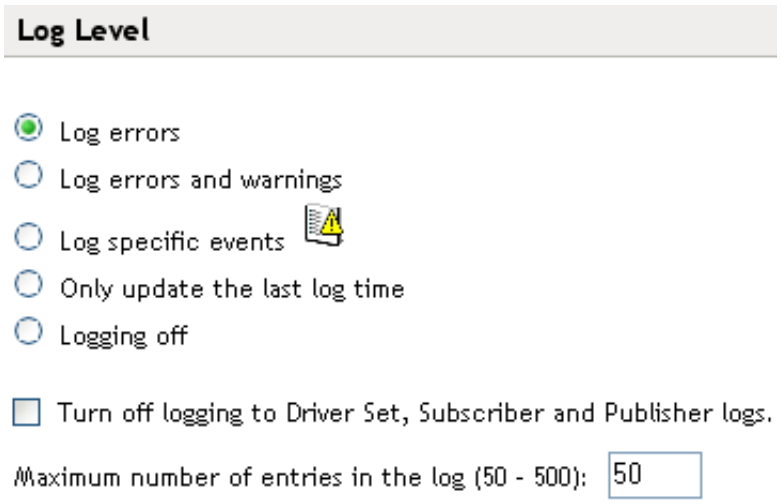
- Section 5.1.1, “Setting the Log Level and Log Size for the Driver Set,” on page 27
- Section 5.1.2, “Setting the Log Level and Log Size for the Driver,” on page 28

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

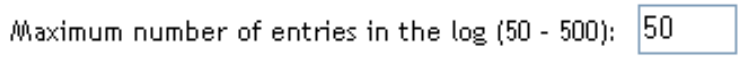
1. In iManager, select *Identity Manager* > *Identity Manager Overview*.
2. Browse to and select the driver set.
3. Click the driver set name to access the driver set overview page.
4. Select *Driver Set* > *Edit Driver Set properties*.



5. Select *Log Level*.



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



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

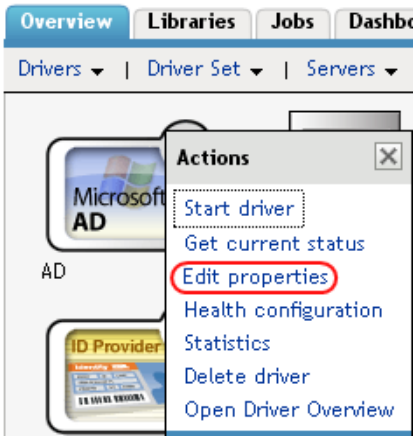
5.1.2 Setting the Log Level and Log Size for the Driver

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.

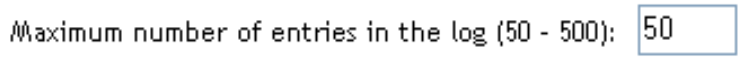
4 Click the upper right corner of the driver icon, then select *Edit properties*.



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:



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

5.2 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.

- Section 5.2.1, “Accessing the Driver Set Status Log,” on page 29
- Section 5.2.2, “Accessing the Publisher Channel and Subscriber Channel Status Logs,” on page 30

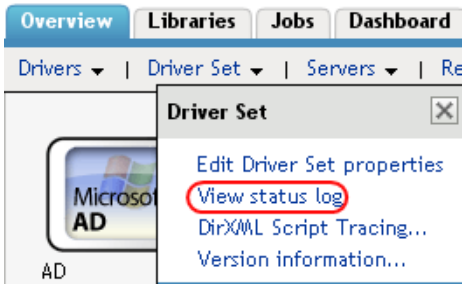
5.2.1 Accessing the Driver Set Status Log

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 29
- “Viewing the Log from the Driver Overview Page” on page 29

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*.

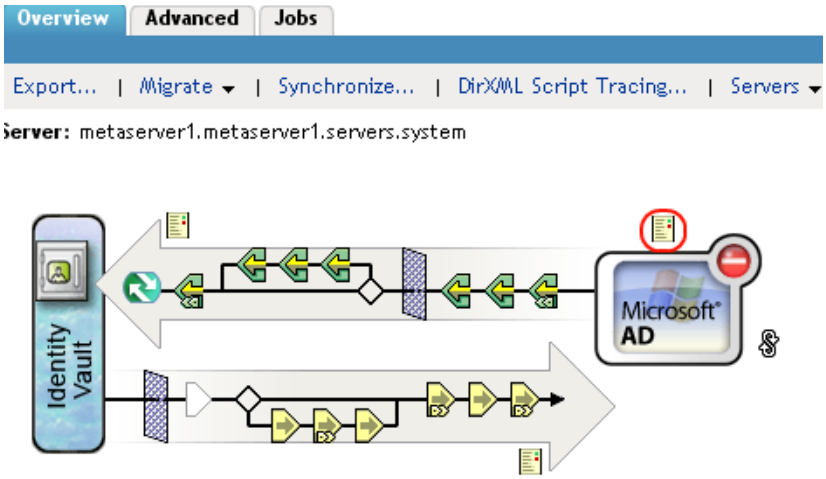


Viewing the Log from the Driver Overview Page

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.

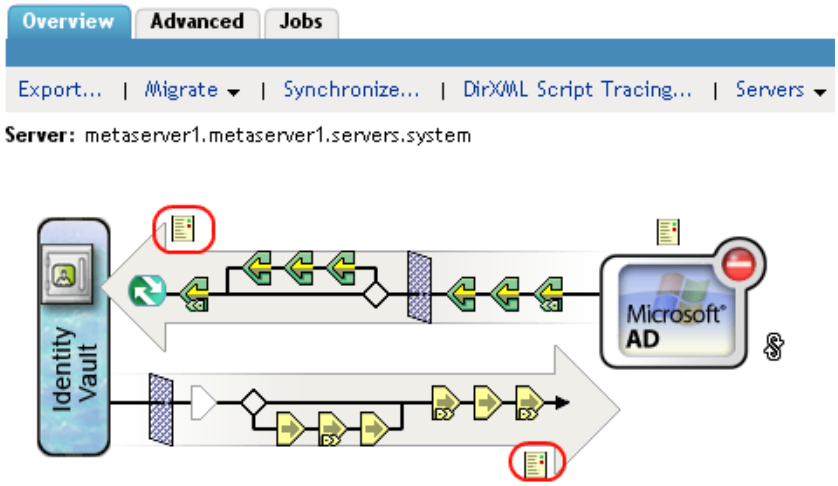


5.2.2 Accessing the Publisher Channel and Subscriber Channel Status Logs

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.



Securing the Connection with Novell Audit

6

Novell® Audit utilizes SSL certificates to ensure that communications between a logging application and the Secure Logging Server are secure. By default, the Secure Logging Server utilizes an embedded root certificate generated by an internal Novell Audit Certificate Authority (CA). Also, by default, the Identity Manager Instrumentation utilizes a public certificate that is signed by the Secure Logging Server root certificate. You can, however, configure Novell Audit to use certificates generated by an external CA.

The following sections review how to use custom certificates to secure the connection between Identity Manager and Novell Audit:

- Section 6.1, "Updating the Novell Audit Certificate Infrastructure," on page 31
- Section 6.2, "The Novell Audit AudCGen Utility," on page 32
- Section 6.3, "Creating a Root Certificate for the Secure Logging Server," on page 35
- Section 6.4, "Creating Logging Application Certificates," on page 36
- Section 6.5, "Validating Certificates," on page 37
- Section 6.6, "Securing Custom Certificates," on page 37

6.1 Updating the Novell Audit Certificate Infrastructure

You can change the internal Novell Audit CA and embedded product certificates to certificates signed by your enterprise CA so you can integrate Novell Audit with your enterprise security infrastructure.

WARNING: Although the process of using certificates signed by external CAs is relatively simple, the consequences of failing to change all required components are serious. Logging applications might fail to communicate with your Secure Logging Server, so events are not recorded.

To update your Novell Audit certificate infrastructure with a custom certificate:

1. Identify all Secure Logging Servers and Identity Manager servers where certificates are located.
2. Use AudCGen to generate a CSR for the Secure Logging Server.

   For information on generating a CSR with AudCGen, see "Creating Logging Application Certificates" on page 36.
3. Have the CSR signed by your enterprise CA.

   If necessary, convert the returned certificate to a Base64-encoded `.pem` file.
4. Shut down all Secure Logging Servers and Identity Manager servers.
5. Delete and purge all application cache (`lcache`) files.

6 In iManager, update the *Secure Logging Certificate File* and *Secure Logging Privatekey File* properties in the Secure Logging Server configuration to point to the new, signed root certificate key pair:

6a In iManager select *Auditing and Logging* > *Logging Server Options*.

6b Select the *General* tab, then select the *Configuration* tab.

6c Update the path in the *Secure Logging Certificate File* field.

6d Update the path in the *Secure Logging Privatekey File* field, then click *OK* to save the changes.

For more information on the Secure Logging Server configuration, see "Logging Server Object Attributes " in the *Novell Audit 2.0 Administration Guide*.

7 Use AudCGen to generate a new public certificate for Identity Manager.

IMPORTANT: The certificate signed by your enterprise CA must be used as the authoritative root certificate.

For information on generating a certificate for Identity Manager, see "Creating Logging Application Certificates" on page 36.

8 Update the Identity Manager Instrumentation so it uses the public certificate signed by the Secure Logging Server's root certificate key pair. For more information, see "Enabling the Identity Manager Instrumentation to Use a Custom Certificate" on page 36.

9 Restart eDirectory™ or the Remote Loader.

After you update your Novell Audit certificate infrastructure with a custom certificate, the only required maintenance is to update the certificate when it expires.

6.2 The Novell Audit AudCGen Utility

IMPORTANT: There are many versions of the AudCGen utility. This section documents the version of AudCGen that is available with Novell Audit 2.0.2 FP2. If you are using a different version of AudCGen, refer to the help file for that version.

The AudCGen utility must be used to create and sign Novell Audit certificates. The following table describes the AudCGen command parameters:

Table 6-1 *AudCGen Command Parameters*

Parameter	Description
app	Generates a certificate key pair for instrumented applications. It creates the `/app_cert.pem` and `/app_pkey.pem` files.
–appcert:*filename*	The output path and filename for the logging application's certificate. The default filename is `app_cert.pem`. The default path is platform-specific and can be changed by using the `-base` parameter.

Parameter	Description
–apppkey:*filename*	The output path and filename for the logging application's private key. The default filename is `app_pkey.pem`. The default path is platform-specific and can be changed by using the `–base` parameter.
–base	The base path used when reading from or writing to files. The default path is platform-specific.
–bits:*RSA_key_size*	The number of encryption bits used during certificate creation. Values of 384-4096 are accepted. The default value is 1024.
–cacert:*filename*	The path and filename to the public certificate used by the Novell Audit Secure Logging Server. The Secure Logging Server's certificate key pair must be provided when generating a certificate key pair for a logging application. The default filename is `ca_cert.pem`. The default path is platform-specific and can be changed by using the –base parameter.
–capkey:*filename*	The path and filename to the private key used by the Novell Audit Secure Logging Server. The Secure Logging Server certificate key pair must be provided when generating a certificate key pair for a logging application. The default filename is `ca_pkey.pem`. The default path is platform-specific and can be changed by using the –base parameter.
csr:*filename*	Generates a Certificate Signing Request (CSR) for the Novell Audit Secure Logging Server that can be signed by a third-party CA. It also generates the certificate private key. The default CSR filename is `ca_csr.pem`. The default private key filename is `ca_pkey.pem`. The default path is platform-specific and can be changed by using the –base parameter.
–csrfile:*filename*	The filename of the CSR for the Novell Audit Secure Logging Server. The default CSR filename is `ca_csr.pem`.
–csrpkey:*filename*	The filename of the private key used with the signed CSR for the Novell Audit Secure Logging Server. The default private key filename is `ca_pkey.pem`
–f	Force overwrite. AudCGen overwrites any existing certificates or private keys of the same name (for example, `app_cert.pem` or `appp_key.pem`) in the output directory. This parameter is optional. If you do not use the -f parameter and there is an existing file, AudCGen aborts creation of the certificate.

Parameter	Description
–h|?	Provides the AudCGen help screen.
–name:application_identifier	**IMPORTANT:** This parameter is required when creating certificates for logging applications like Identity Manager. The logging application's application identifier. The application identifier is the application name that appears in the first line of the application's corresponding `.lsc` file. **NOTE:** This value matches the Application Identifier stored in Identity Manager's Application object. For example, the first line of the `.lsc` file for Identity Manager is `#^Identity Manager^0003^DirXML^EN` The application identifier is the name after the third carat in this line. The application identifier for Identity Manager is DirXML.
–sn:*number*	This parameter creates a serial number for the generated certificate. This can be useful in maintaining and tracking your system's certificates. This parameter is optional.
ss	Generates a self-signed root certificate key pair for the Novell Audit Secure Logging Server. This option uses the internal Novell Audit CA. **NOTE:** Do not use this option if you want to use a certificate signed by a third-party CA.
–valid:*number*	Specifies the number of days for which the generated public certificate will be valid (in days). The default value is 10 years.
–verbose	Displays the contents of the certificates.
verify	Verifies the certificate signing chain between the root certificate used by the Secure Logging Server and Identity Manager certificates. **NOTE:** This option performs only partial verification when verifying third-party certificates. For additional information, see "Validating Certificates" on page 37.

6.3 Creating a Root Certificate for the Secure Logging Server

The certificate key pair used by the Secure Logging Server is the logging system's Certificate Authority (CA); that is, it is the trusted root certificate that is used to validate all other Novell Audit logging application certificates. By default, this certificate is self-signed. However, you can use a certificate signed by a third-party CA.

The following sections review the process required to generate a self-signed root certificate and how to use a third-party root certificate for the Secure Logging Server.

- Section 6.3.1, "Creating a Self-Signed Root Certificate for the Secure Logging Server," on page 35
- Section 6.3.2, "Using a Third-Party Root Certificate for the Secure Logging Server," on page 35

6.3.1 Creating a Self-Signed Root Certificate for the Secure Logging Server

To generate a self-signed root certificate for the Secure Logging Server by using the internal Novell Audit CA, use the following AudCGen command:

```
audcgen ss [-cacert:filename] [-capkey:filename] [-bits:number] [-f]
```

For example:

```
audcgen ss -cacert:slscert.pem -capkey:slspkey.pem -bits:512 -f
```

The -ss parameter creates a self-signed root certificate that can then be used to generate the certificate key pair for each logging application. For more information on generating the key pair, see "Creating Logging Application Certificates" on page 36.

6.3.2 Using a Third-Party Root Certificate for the Secure Logging Server

To use a certificate signed by a third-party CA, you must do the following:

1. Use AudCGen to generate a CSR that can be signed by a third-party CA:

   The command syntax is as follows:

   ```
   audcgen csr [-csrfile:filename] [-csrpkey:filename]
   [-bits:RSA_key_size]
   ```

   For example:

   ```
   audcgen csr -bits:512 -csrfile:slscsr.pem -csrpkey:slspkey.pem
   ```

   For more information, see Section 6.2, "The Novell Audit AudCGen Utility," on page 32.

2. Take the `slscsr.pem` file and submit it to a third-party CA for signature, or sign it by using your internal certificate server.

IMPORTANT: The Novell Audit Secure Logging Server requires two Base64-encoded `.pem` files: one for the public certificate and one for the private key. Some CAs might generate files that require additional conversion steps.

3 Configure the Secure Logging Certificate File and Secure PrivateKey File attributes on the Logging Server object to enable the Secure Logging Server to use the third-party certificate and private key.

For more information, see "Logging Server Object Attributes " in the *Novell Audit 2.0 Administration Guide*.

4 Use the Secure Logging Server's third-party certificate to generate the certificate key pair for each logging application.

For more information on this procedure, see "Creating Logging Application Certificates" on page 36.

IMPORTANT: If you use a third-party certificate, your logging applications can no longer communicate with the Secure Logging Server by using their default certificates. You must create a new certificate key pair for each logging application by using AudCGen and the new root certificate key pair.

6.4 Creating Logging Application Certificates

IMPORTANT: In Novell Audit, all logging application certificates must be signed by the Secure Logging Server root certificate and they must contain an Application Identifier.

The following AudCGen command generates a public certificate and private key for your logging application:

```
audcgen app [cacert:filename] [-capkey:filename] [-appcert:filename]
[-apppkey:filename] -name:application_identifier
[-bits:RSA_key_size] [-sn:number] [-valid:number] [-f]
```

NOTE: This command is used to generate logging application certificates by using either the internal Novell Audit CA or one signed by a third-party CA. Use the `-cacert` and `-capkey` parameters to specify the root certificate used by your Secure Logging Server.

The following sample command creates a logging application certificate for Identity Manager:

```
audcgen app -cacert:slscert.pem -capkey:slspkey.pem
-appcert:IDMcert.pem -apppkey:IDMpkey.pem -name:DirXML -bits:512
-sn:123
```

For more information, see Section 6.2, "The Novell Audit AudCGen Utility," on page 32.

6.4.1 Enabling the Identity Manager Instrumentation to Use a Custom Certificate

To enable the Identity Manager Instrumentation to use a custom certificate key pair, the path and filename for the certificate and private key files must be as follows:

Table 6-2 *Identity Manager Certificate and Key Paths and Filenames*

Platform	Certificate Path and Filename	PrivateKey Path and Filename
Windows	*windows_directory*\dxicert.pem	*windows_directory*\dxipkey.pem
Linux and Solaris	/etc/dxicert.pem	/etc/dxipkey.pem

NOTE: If you are using the pure Java remote loader (`dirxml_jremote`), the above locations work. However, if `dirxml_jremote` is running on a non-UNIX-like platform, you must add the following to the Java invocation line in the `dirxml_jremote` script:

```
-Dnovell.dirxml.remoteloader.audit_key_directory=<directory_name>
```

6.5 Validating Certificates

In Novell Audit, all logging application certificates must be signed by the Secure Logging Server root certificate and they must contain an application identifier.

Use the following AudCGen command to determine whether a certificate is valid:

```
audcgen -cacert:filename -capkey:filename -verify -appcert:filename
```

When you use the `-verify` command, AudCGen checks the integrity of the target certificate. It determines if the target certificate is derived from the Secure Logging Server root certificate (trusted) and returns the logging application's application identifier.

The following sample command verifies the certificate for the Identity Manager Instrumentation:

```
audcgen -cacert:cacert.pem -capkey:capkey.pem -verify
-appcert:c:\windows\dxicert.pem
```

For more information, see Section 6.2, "The Novell Audit AudCGen Utility," on page 32.

NOTE: Novell Audit 2.0.2 verifies only the Secure Logging Server and logging application certificates. It does not verify any other certificates in the certificate chain. Consequently, if the third-party CA expires or invalidates the Secure Logging Server certificate, AudCGen does not identify the problem in the certificate chain and still trusts the Secure Logging Server root certificate and its associated logging application certificates.

6.6 Securing Custom Certificates

If you generate a custom certificate and private key for the Identity Manager Instrumentation, it is important to protect them because the location and name of the custom certificates are hardcoded. The certificate and key files should only be accessible by the Identity Manager Instrumentation, which loads locally on the server.

The following sections review the steps to protect custom certificates on each Novell Audit server platform.

- Section 6.6.1, "Windows," on page 38
- Section 6.6.2, "Linux and Solaris," on page 38

6.6.1 Windows

On Windows, the custom certificate and private key files are also protected by file system trustees. The eDirectory instrumentation certificate files to protect are `\windows_directory\dxicert.pem` and `\windows_directory\dxipkey.pem`.

To limit access to the private key files:

1. Grant the auditor user full object rights to the key files.
2. Give the SYSTEM account read rights to the key files.
3. Do not allow inherited rights from any file to be propagated to the key files.

NOTE: The owner of a file can always change the rights. System administrators can take ownership of a file. Do not grant excessive numbers of users Administrator rights to the server.

6.6.2 Linux and Solaris

On Linux and Solaris, the private key is stored in `/etc/dxipkey.pem`.

To limit access to the private key file:

1. Grant the root user rights to the file.

   You can also grant rights to the auditor and the `root` group. Do not grant read rights to other users of the system.
2. Assign mode 0400 to the file; verify that the owner of the file is `root`.

   If you have granted rights to the auditor and the `root` group, assign mode 0440 to the file.

Identity Manager Events

A

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

- Section A.1, “Event Structure,” on page 39
- Section A.2, “Error and Warning Events,” on page 39
- Section A.3, “Job Events,” on page 40
- Section A.4, “Remote Loader Events,” on page 40
- Section A.5, “Object Events,” on page 40
- Section A.6, “Password Events,” on page 41
- Section A.7, “Search List Events,” on page 41
- Section A.8, “Engine Events,” on page 41
- Section A.9, “Server Events,” on page 41
- Section A.10, “Security Events,” on page 41
- Section A.11, “Workflow Events,” on page 41
- Section A.12, “Driver Start and Stop Events,” on page 41

NOTE: Novell Audit provides the ability to send a notification when a specific event occurs or does not occur. Notifications can be sent based on any value in one or more events. Notifications can be sent to any logging channel, enabling you to log notifications to a database, a Java application or SNMP management system, or several other locations. For details on creating Novell Audit notifications based on Identity Manager events, see “Configuring Filters and Event Notifications” in the *Novell Audit 2.0 Administration Guide*.

A.1 Event Structure

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

Identity Manager events provide information in the following field structure:

EventID, Description, Originator Title, Target Title, Subtarget Title, Text1 Title, Text2 Title, Text3 Title, Value1 Title, Value1 Type, Value2 Title, Value2 Type, Value3 Title, Value3 Type, Group Title, Group Type, Data Title, Data Type, Display Schema.

For a complete explanation of the event structure, see “Event Structure ” in the *Novell Audit 2.0 Administration Guide*

A.2 Error and Warning Events

Identity Manager generates an event whenever an error or warning is encountered. The following table lists the Identity Manager error and warning events:

Table A-1 *Error and Warning Events*

Event	Log Level	Information
DirXML_Error	LOG_ERROR	All Identity Manager errors log this event. The actual error code encountered is stored in the event. To log errors, select the *Log Errors* or *Log Errors and Warnings* log level on the driver set or the individual driver. You can also select the *Log Specific Events* option and select this event. For more information, see Section 5.1, "Setting the Log Level and Maximum Log Size," on page 27.
DirXML_Warning	LOG_WARNING	All Identity Manager warnings log this event. The actual warning code encountered is stored in the event. To log errors, select the *Log Errors* or *Log Errors and Warnings* log level on the driver set or the individual driver. You can also select the *Log Specific Events* option and select this event. For more information, see Section 5.1, "Setting the Log Level and Maximum Log Size," on page 27.

A.3 Job Events

The following link lists the Job events that can be audited through Novell Audit or Novell Sentinel™:

Identity Manager Job Events (../samples/idm_combo_events.xls)

A.4 Remote Loader Events

The following link lists the Remote Loader events that can be audited through Novell Audit or Novell Sentinel:

Identity Manager Remote Loader Events (../samples/idm_combo_events.xls)

IMPORTANT: To log these events, you must select the *Log Specific Events* log level and select the events you want to log. For more information, see Section 5.1, "Setting the Log Level and Maximum Log Size," on page 27.

A.5 Object Events

The following link lists the object events that can be audited through Novell Audit or Novell Sentinel:

Identity Manager Detail Events (../samples/idm_combo_events.xls)

A.6 Password Events

The following link lists the change password events that can be audited through Novell Audit or Novell Sentinel:

Identity Manager Password Events (../samples/idm_combo_events.xls)

A.7 Search List Events

The following link lists search list events that can be audited through Novell Audit or Novell Sentinel:

Identity Manager Search List Events (../samples/idm_combo_events.xls)

A.8 Engine Events

The following link lists the engine events that can be audited through Novell Audit or Novell Sentinel:

Identity Manager Engine Events (../samples/idm_engine_events.xls)

A.9 Server Events

The following link lists the server events that can be audited through Novell Audit or Novell Sentinel:

Identity Manager Server Events (../samples/idm_server_events.xls)

A.10 Security Events

The following link lists security events that can be audited through Novell Audit or Novell Sentinel:

Identity Manager Security Events (../samples/idm_security_events.xls)

A.11 Workflow Events

The following link lists User Application events that can be audited through Novell Audit or Novell Sentinel:

Identity Manager Work Flow Events (../samples/idm_workflow_events.xls)

A.12 Driver Start and Stop Events

Identity Manager can generate an event whenever a driver starts or stops. The following table contains details about these events:

Table A-2 *Driver Start and Stop Events*

Event	Log Level	Information
EV_LOG_DRIVER_START	LOG_INFO	To log driver starts, select the *Log Specific Events* log level and specify this event. For more information, see Section 5.1, “Setting the Log Level and Maximum Log Size,” on page 27
EV_LOG_DRIVER_STOP	LOG_WARNING	To log driver stops, select the *Log Errors and Warnings* log level, or select the *Log Specific Events* log level and specify this event. For more information, see Section 5.1, “Setting the Log Level and Maximum Log Size,” on page 27.

Novell Audit Reports

B

This section provides examples of the following Novell® Audit reports for Identity Manager and the events associated with each report:

- Section B.1, “Administrative Action Report,” on page 43
- Section B.2, “Historical Approval Flow Report,” on page 44
- Section B.3, “Resource Provisioning Report,” on page 46
- Section B.4, “Specific User Audit Trail Report I,” on page 48
- Section B.5, “Specific User Audit Trail Report II,” on page 50
- Section B.6, “Specific User Audit Trail III,” on page 52
- Section B.7, “Specific User Provisioning Report,” on page 54
- Section B.8, “User Provisioning Report,” on page 56

B.1 Administrative Action Report

The Administrative Action Report is generated from the events listed in the following table. For more information on the events, see Appendix A, “Identity Manager Events,” on page 39.

Table B-1 *Administration Action Events*

Event ID	Description	Trigger
31400	Delete_Entity	Occurs when an object is deleted.
31401	Update_Entity	Occurs when an object is modified.

Figure B-1 *Administrative Action Report*

Novell® Audit Report for Identity Manager

Administrative Action Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 5

Total # Events: 121

Report Period: - 10/13/2005 8:43:50AM

Date / Time	Administrator	Subject	Action
8/18/2005 5:45:17PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:07:40PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:09:05PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:12:50PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:13:39PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/23/2005 4:56:39PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Deleted
8/31/2005 12:01:55PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:02:18PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:07PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:31PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:27:58PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:28:22PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 2:59:39PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 3:24:30PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 8:11:59PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=testCreateUser,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:23PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:55PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
8/31/2005 8:13:03PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
9/1/2005 10:29:53AM	cn=admin,ou=idmsample-Jeff,o=novell	cn=aa,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
9/1/2005 11:31:45AM	cn=admin,ou=idmsample,o=novell	cn=asoprano,ou=users,ou=idmsample,o=novell	Entity Created

Page 1 of 5 Administrative Action Report

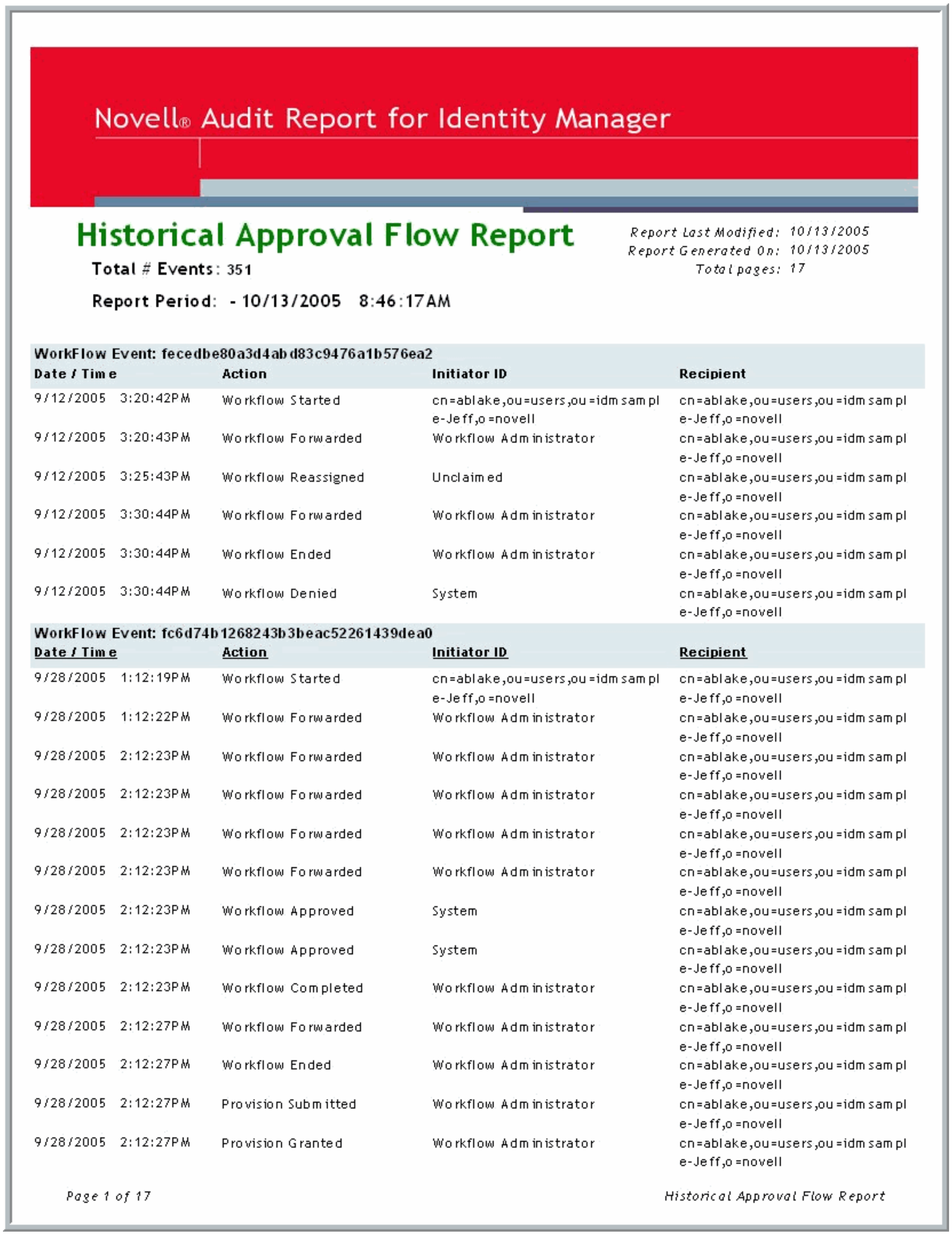
B.2 Historical Approval Flow Report

The Historical Approval Report is generated from the events listed in the following table. For more information on the events, see Appendix A, “Identity Manager Events,” on page 39.

Table B-2 *Historical Approval Events*

Event ID	Description	Trigger
31520	Workflow_Error	Occurs when there is a workflow error. Many errors can trigger this event.
31521	Workflow_Started	Occurs when the workflow starts.
31522	Workflow_Forwarded	Occurs when the workflow is forwarded.
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.
3152A	Workflow_Completed	Occurs when the workflow is completed.
3152B	Workflow_Timedout	Occurs when the workflow timed out.
31533	Workflow_Retracted	Occurs when the workflow is retracted.

Figure B-2 Historical Approval Flow Report



Novell® Audit Report for Identity Manager

Historical Approval Flow Report

Total # Events: 351

Report Period: - 10/13/2005 8:46:17AM

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 17

WorkFlow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID	Recipient
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Denied	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

WorkFlow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID	Recipient
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Page 1 of 17 Historical Approval Flow Report

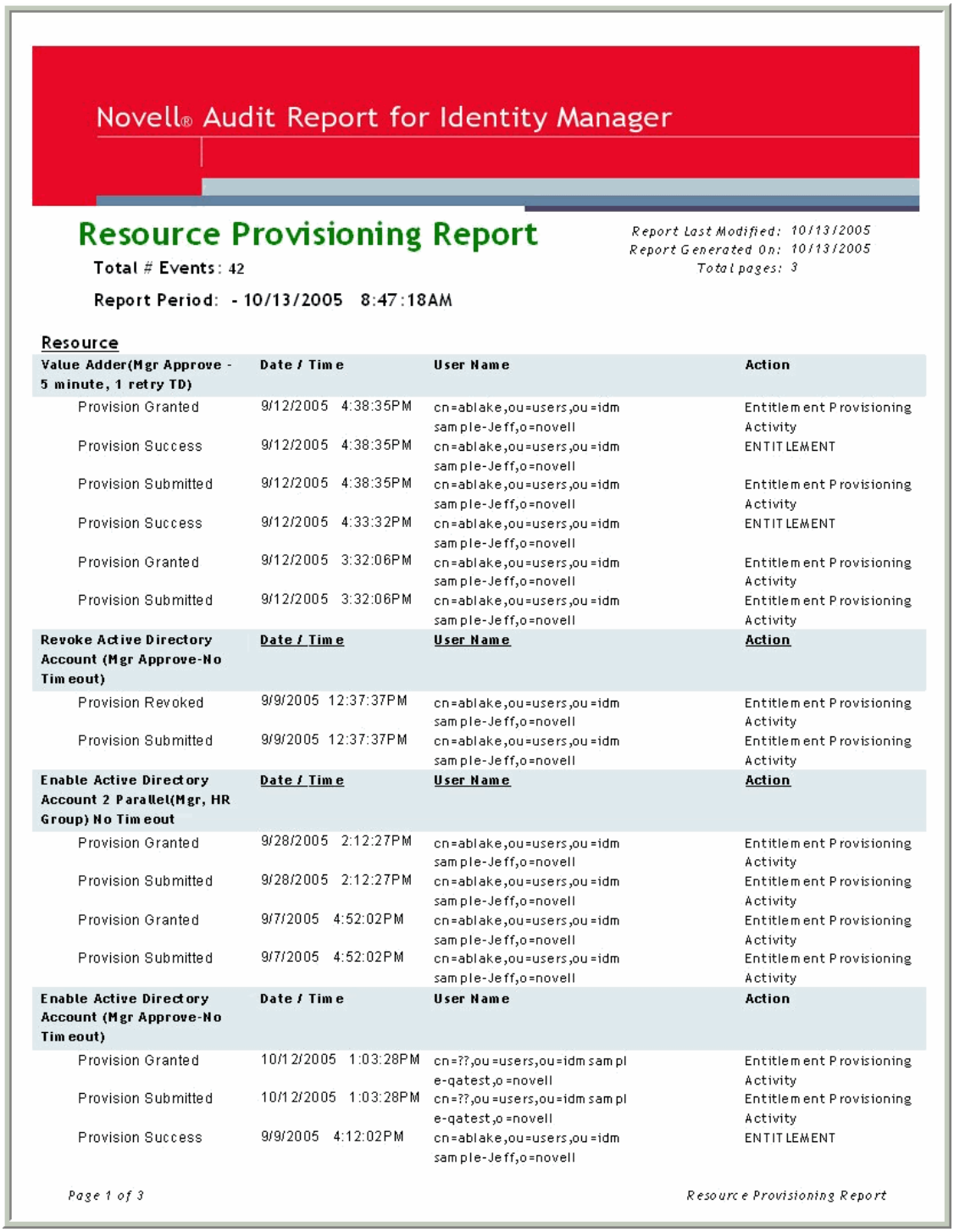
B.3 Resource Provisioning Report

The Resource Provisioning Report is generated from the events listed in the following table. For more information on the events, see Appendix A, “Identity Manager Events,” on page 39.

Table B-3 *Provisioning Events*

Event ID	Description	Trigger
3152D	Provision_Error	Occurs when there is an error in the provisioning step.
3152E	Provision_Submitted	Occurs on submission of entitlements during the provisioning step.
3152F	Provision_Success	Occurs on successful completion of the step during the provisioning step.
31530	Provision_Failure	Occurs upon failure of the step during the provisioning step.
31531	Provision_Granted	Occurs on granting of an entitlement during the provisioning step.
31532	Provision_Revoked	Occurs on the revoking of an entitlement during the provisioning step.

Figure B-3 *Resource Provisioning Report*



Novell® Audit Report for Identity Manager

Resource Provisioning Report

Total # Events: 42

Report Period: - 10/13/2005 8:47:18AM

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

Resource

Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Date / Time	User Name	Action
Provision Granted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Revoke Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Revoked	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	**Date / Time**	**User Name**	**Action**
Provision Granted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Granted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Granted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Submitted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT

Page 1 of 3

Resource Provisioning Report

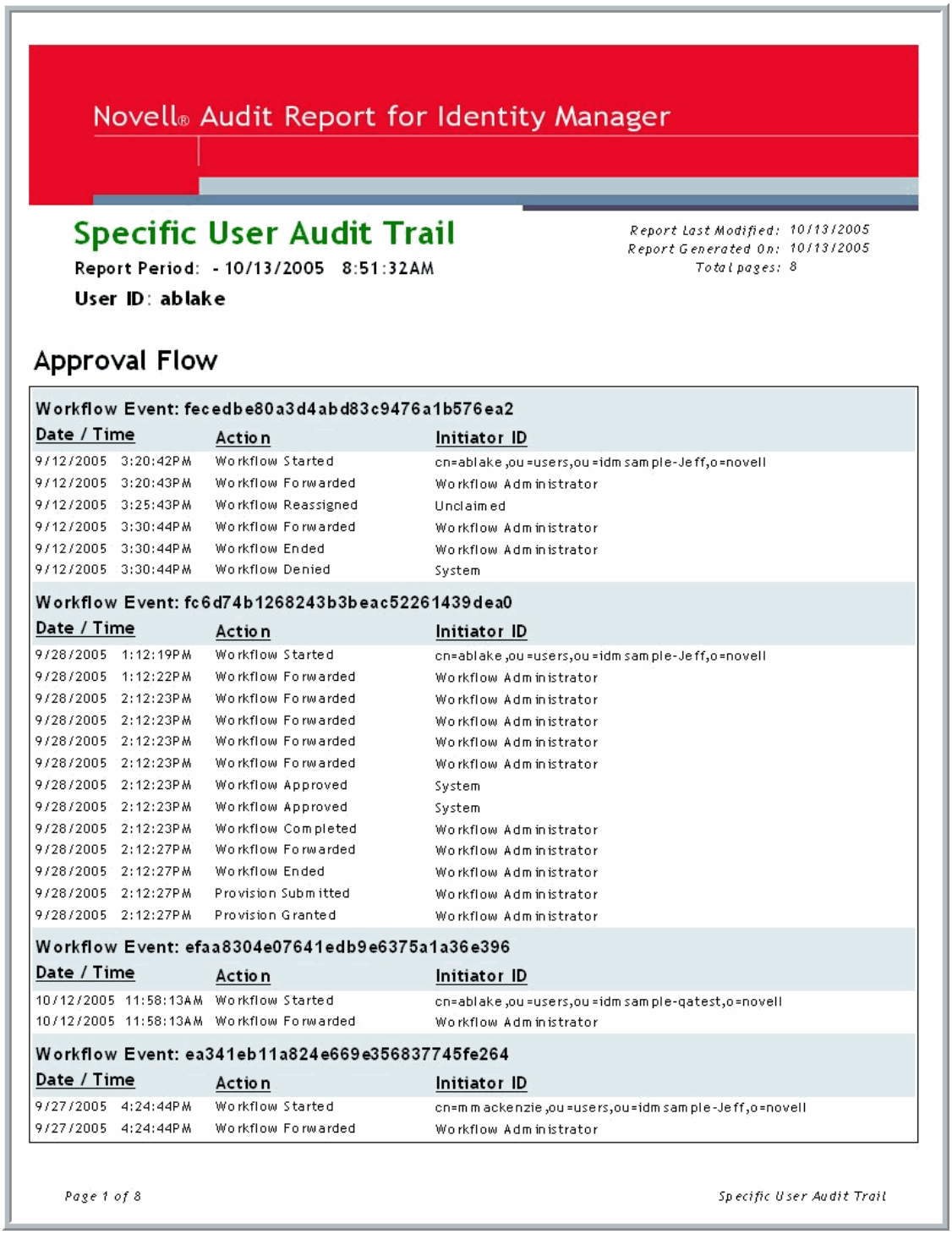
B.4 Specific User Audit Trail Report I

The Specific User Audit Trail Report I is generated from the events listed in the following table. For more information on the events, see Appendix A, “Identity Manager Events,” on page 39.

Table B-4 *User Audit Trail Events*

Event ID	Description	Trigger
31520	Workflow_Error	Occurs when there is a workflow error. Many errors can trigger this event.
31521	Workflow_Started	Occurs when the workflow starts.
31522	Workflow_Forwarded	Occurs when the workflow is forwarded.
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.
3152A	Workflow_Completed	Occurs when the workflow is completed.
3152B	Workflow_Timedout	Occurs when the workflow timed out.
31533	Workflow_Retracted	Occurs when the workflow is retracted.

Figure B-4 *Specific User Audit Trail 1*



Novell® Audit Report for Identity Manager

Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 8

Approval Flow

Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

Workflow Event: efaa8304e07641edb9e6375a1a36e396

Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idmsample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

Page 1 of 8

Specific User Audit Trail

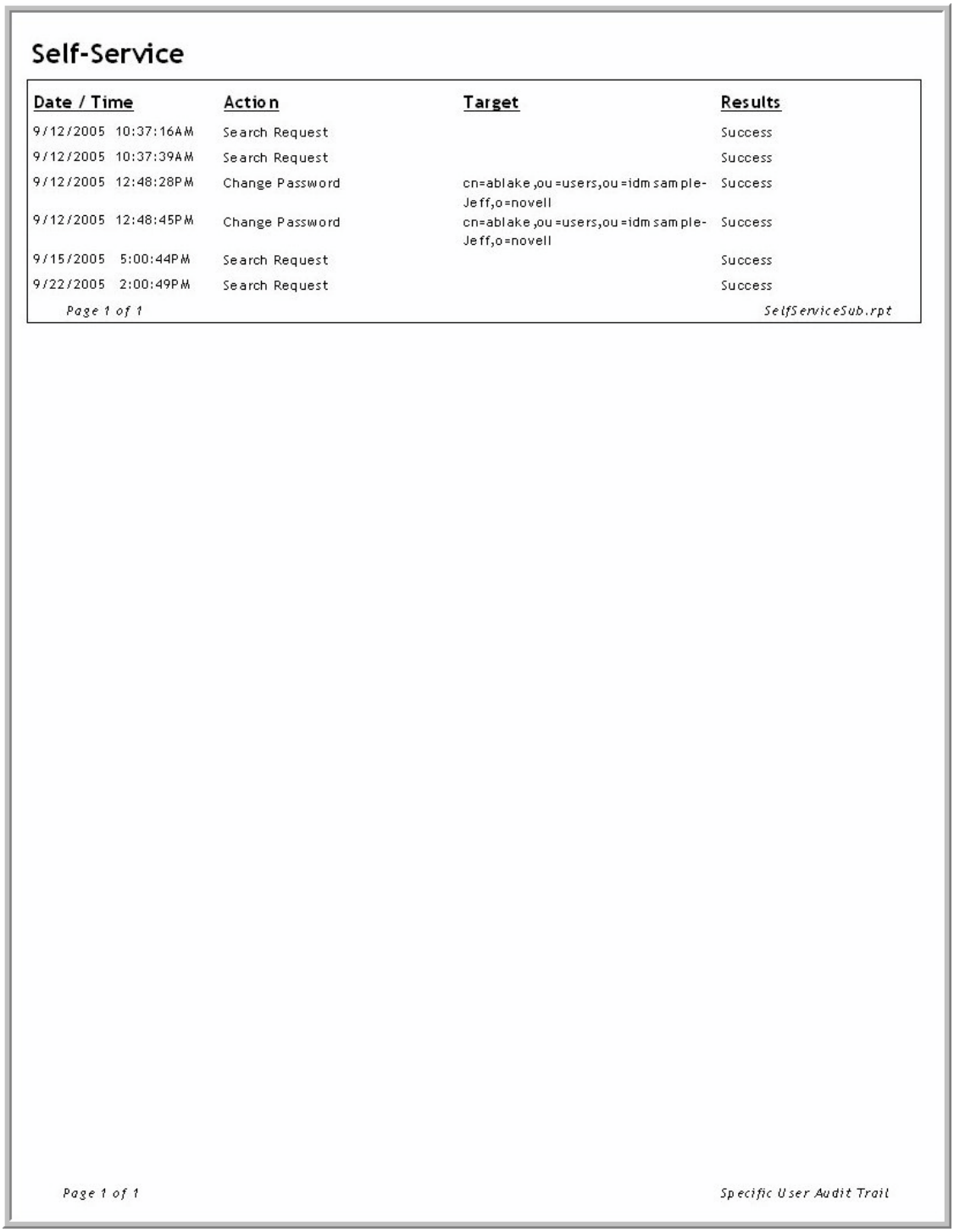
B.5 Specific User Audit Trail Report II

The Specific User Audit Trail Report II is generated from the events listed in the following table. For more information on the events, see Appendix A, “Identity Manager Events,” on page 39.

Table B-5 *User Audit Trail Events*

Event ID	Description	Trigger
30007	Search	Occurs when a query document is sent to the Metadirectory engine or driver.
31410	Change_Password_Failure	Occurs when a password change fails.
31411	Change_Password_Success	Occurs when a password change is successful.
31420	Forgot_Password_Change_Failure	Occurs when the Forgot Password change fails.
31421	Forgot_Password_Change_Success	Occurs when the Forgot Password change is successful.

Figure B-5 *Specific User Audit Trail 2*



Self-Service

Date / Time	Action	Target	Results
9/12/2005 10:37:16AM	Search Request		Success
9/12/2005 10:37:39AM	Search Request		Success
9/12/2005 12:48:28PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/12/2005 12:48:45PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/15/2005 5:00:44PM	Search Request		Success
9/22/2005 2:00:49PM	Search Request		Success

Page 1 of 1 SelfServiceSub.rpt

Page 1 of 1 Specific User Audit Trail

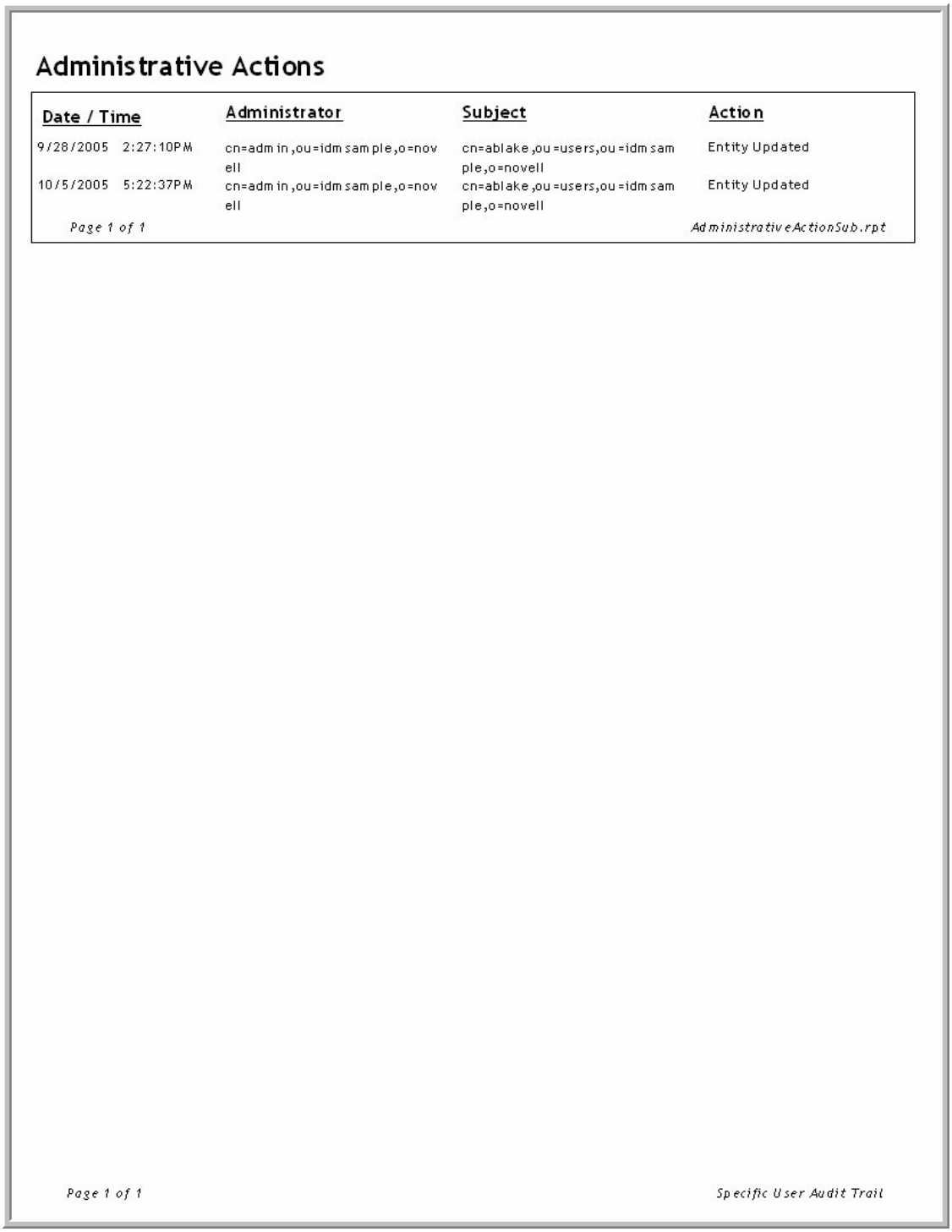
B.6 Specific User Audit Trail III

The Specific User Audit Trail III Report is generated from the events listed in the following table. For more information on the events, see Appendix A, “Identity Manager Events,” on page 39.

Table B-6 *Administration Action Events*

Event ID	Description	Trigger
31400	Delete_Entity	Occurs when an object is deleted.
31401	Update_Entity	Occurs when an object is modified.

Figure B-6 *Specific User Audit Trail 3*



Administrative Actions

Date / Time	Administrator	Subject	Action
9/28/2005 2:27:10PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated
10/5/2005 5:22:37PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated

Page 1 of 1 AdministrativeActionSub.rpt

Page 1 of 1 Specific User Audit Trail

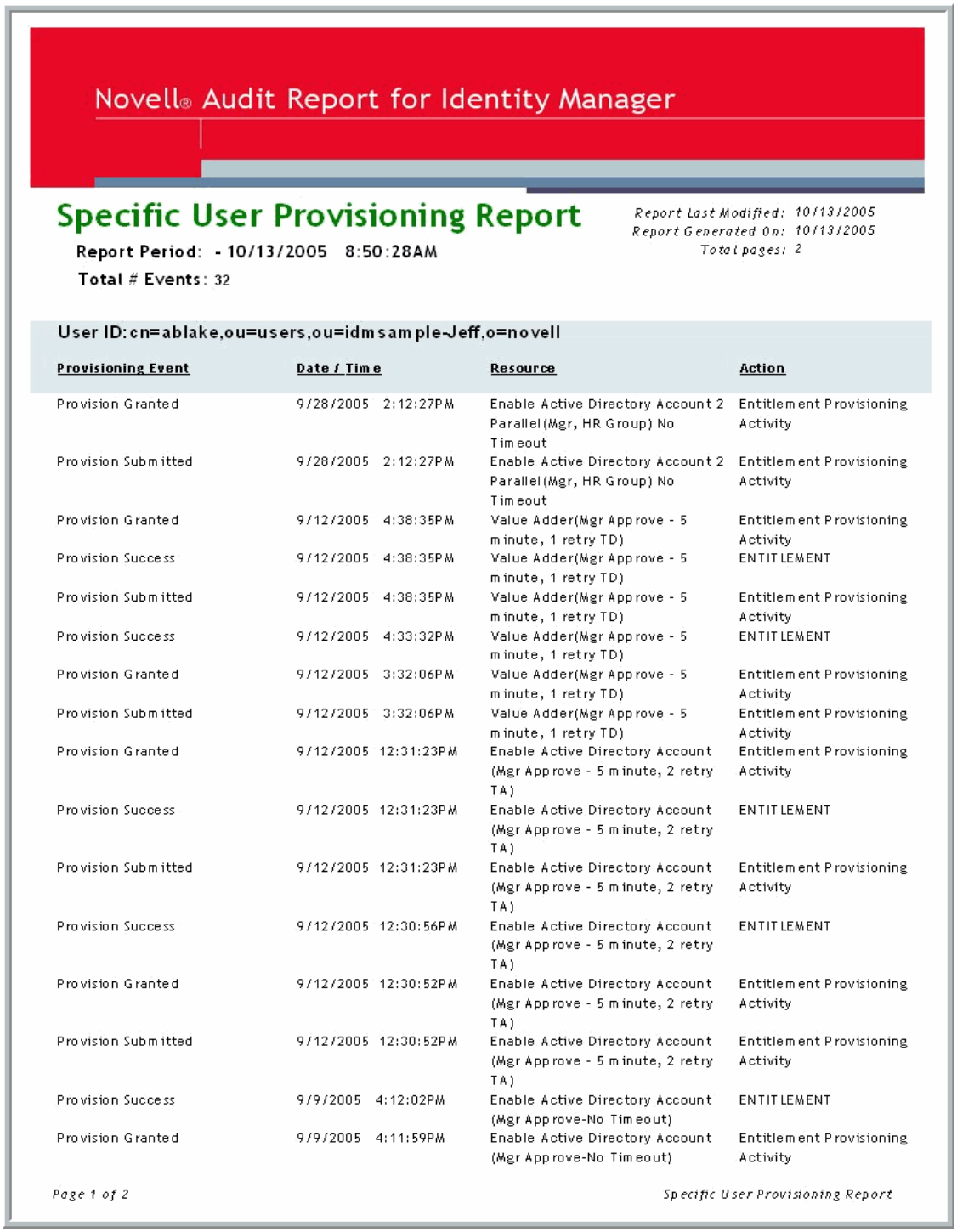
B.7 Specific User Provisioning Report

The Specific User Provisioning Report is generated from the events listed in the following table. For more information on the events, see Appendix A, “Identity Manager Events,” on page 39.

Table B-7 *Provisioning Events*

Event ID	Description	Trigger
3152D	Provision_Error	Occurs when there is an error in the provisioning step.
3152E	Provision_Submitted	Occurs on submission of entitlements during the provisioning step.
3152F	Provision_Success	Occurs on successful completion of the step during the provisioning step.
31530	Provision_Failure	Occurs upon failure of the step during the provisioning step.
31531	Provision_Granted	Occurs on granting of an entitlement during the provisioning step.
31532	Provision_Revoked	Occurs on the revoking of an entitlement during the provisioning step.

Figure B-7 *Specific User Provisioning Report*



Novell® Audit Report for Identity Manager

Specific User Provisioning Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 2

Report Period: - 10/13/2005 8:50:28AM

Total # Events: 32

User ID: cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Provisioning Event	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel (Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel (Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 2

Specific User Provisioning Report

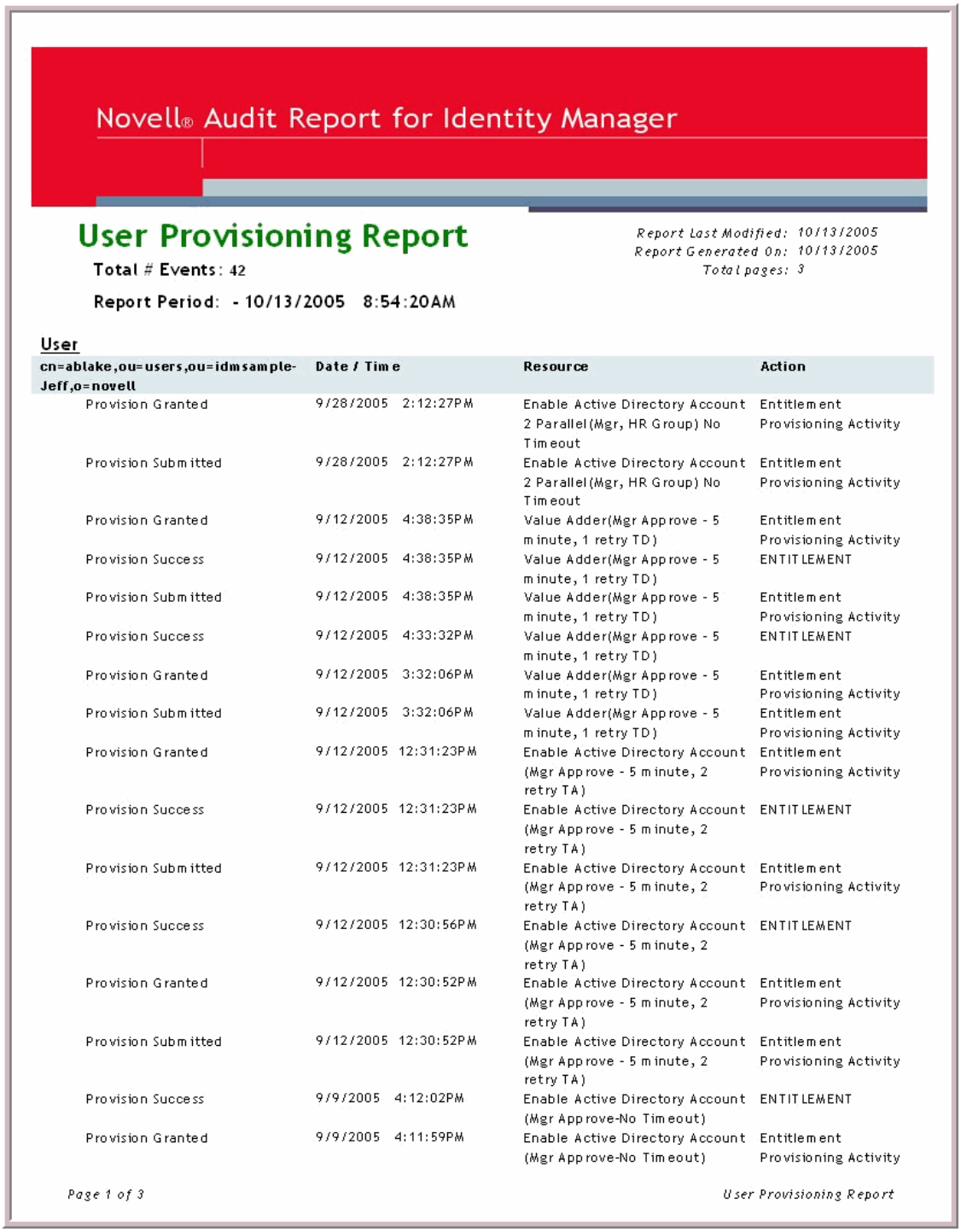
B.8 User Provisioning Report

The User Provisioning Report is generated from the events listed in the following table. For more information on the events, see Appendix A, “Identity Manager Events,” on page 39.

Table B-8 *Provisioning Events*

Event ID	Description	Trigger
3152D	Provision_Error	Occurs when there is an error in the provisioning step.
3152E	Provision_Submitted	Occurs on submission of entitlements during the provisioning step.
3152F	Provision_Success	Occurs on successful completion of the step during the provisioning step.
31530	Provision_Failure	Occurs upon failure of the step during the provisioning step.
31531	Provision_Granted	Occurs on granting of an entitlement during the provisioning step.
31532	Provision_Revoked	Occurs on the revoking of an entitlement during the provisioning step.

Figure B-8 *User Provisioning Report*



Novell® Audit Report for Identity Manager

User Provisioning Report

Total # Events: 42

Report Period: - 10/13/2005 8:54:20AM

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

User

cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 3 *User Provisioning Report*