Novell Identity Manager

3.5.1

www.novell.com

LOGGING AND REPORTING

September 28, 2007

Novell®

Legal Notices

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

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

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. 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

Third-Party Materials

Contents

About This Guide

Welcome to the *Novell® Identity Manager Auditing and Reporting Guide*. This guide provides the information necessary to integrate Novell Audit™ or Novell® Sentinel™ with Identity Manager to provide auditing and reporting services.

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 3.5.1 Logging and Reporting Guide*, visit the Novell Documentation Web site, (http://www.novell.com/documentation/idm35/idm_log/index.html).

Additional Documentation

For documentation on Identity Manager, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm35/).

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.

Integrating Identity Manager with Novell Audit

1

NOTE: Reporting and Notification Service (RNS) is deprecated in the current version of Identity Manager, although the Metadirectory engine continues to process RNS functions if you are currently using RNS. Nevertheless, we strongly recommend that you move to Novell® Audit or Novell® Sentinel™ because these auditing and reporting systems expand the functionality provided by RNS and RNS might not be supported in a future release of Identity Manager. For RNS documentation, see the *DirXML 1.1a Administration Guide* (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html).

Novell Audit is a centralized, cross-platform auditing service that is integrated with Identity Manager to provide detailed information about driver and engine activity. Using Novell Audit with Identity Manager, you can monitor real-time Identity Manager events, send e-mail notifications for any Identity Manager event, and generate reports of Identity Manager activity.

The following sections provide information needed to integrate Identity Manager with Novell Audit:

- Section 1.1, "Integrated Architecture," on page 9
- Section 1.2, "Steps to Integration," on page 10
- Section 1.3, "Registering Identity Manager with Novell Audit," on page 11

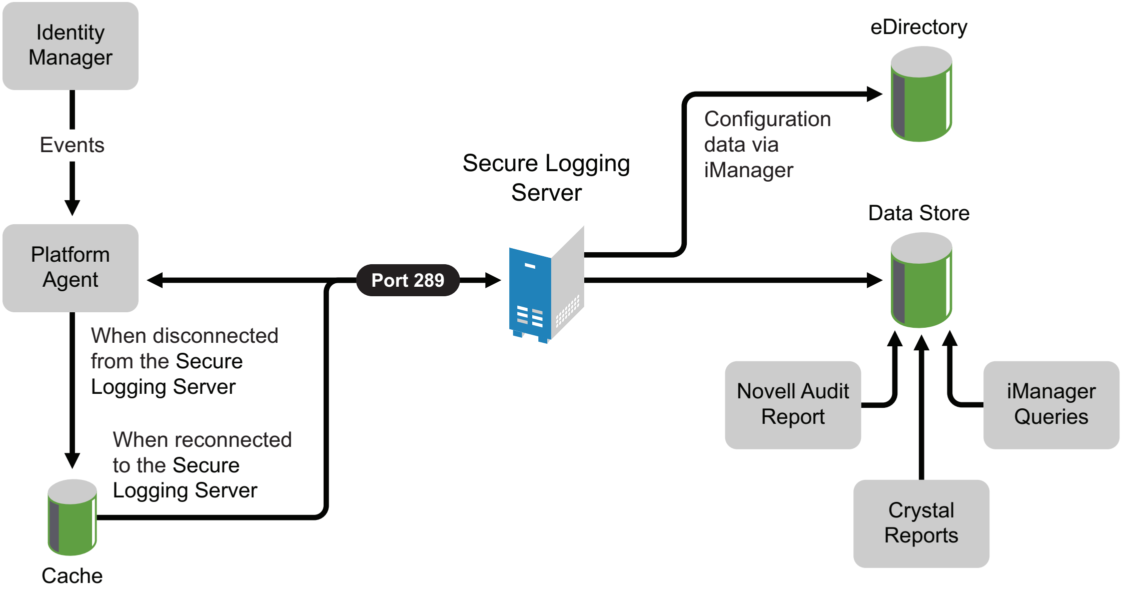
1.1 Integrated Architecture

To log Identity Manager events to Novell Audit and generate reports of Identity Manager activity, you must install and configure the following Novell Audit components:

- Identity Manager
- Platform Agent
- Secure Logging Server
- Data Store
- Novell Audit Report

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



1.2 Steps to Integration

To enable Identity manager to log events to Novell Audit, you must do the following:

1. Install and configure Novell Audit on your system. You must have a functioning Secure Logging Server (`lengine`) and data store to log Identity Manager events.

   The following links provide the information you need to install and configure Novell Audit in your network environment:

   - For complete information on installing Novell Audit, see the *Novell Audit 2.0 Installation Guide*.
   - For a discussion of the Novell Audit architecture, see "System Architecture" in the *Novell Audit 2.0 Administration Guide*.
   - For information on configuring the Secure Logging Server, see "Configuring the Secure Logging Server" in the *Novell Audit 2.0 Administration Guide*.
   - For information on configuring the data store, see "Configuring the Data Store " in the *Novell Audit 2.0 Administration Guide*.

2. Install and configure the Platform Agent.

   The Platform Agent (`logevent`) is the client piece of the Novell auditing architecture. It is automatically installed if either the Novell *Identity Manager Metadirectory Server* or Novell *Identity Manager Connected System* option is selected during the Identity Manager install. For more information in installing and configuring the Platform Agent, see Chapter 3, "Installing and Configuring the Platform Agent," on page 17.

3. Extend the eDirectory™ schema to include the Identity Manager auditing components and register Identity Manager with the Secure Logging Server. For more information, see Section 1.3, "Registering Identity Manager with Novell Audit," on page 11.

4. Select which Identity Manager events you want to log to Novell Audit. For more information, see Chapter 4, "Managing Identity Manager Events," on page 21.

5. (Optional) Configure your 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" in the *Novell Audit 2.0 Administration Guide*.

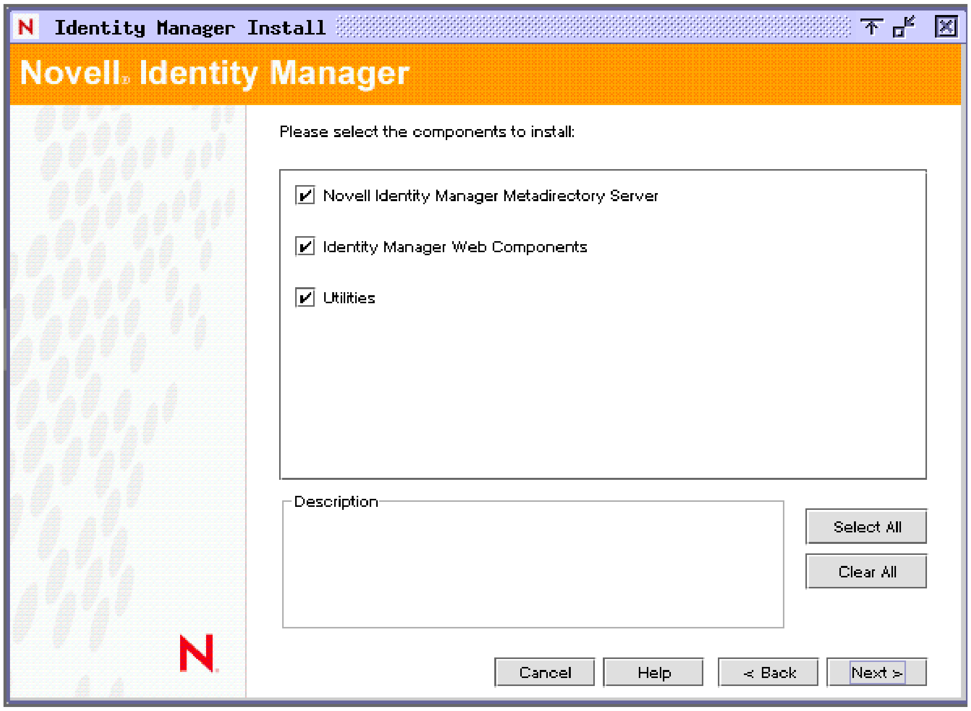
6. (Optional) Secure the connection between Identity Manager and the Platform Agent. For more information, see "Securing the Connection with Novell Audit" on page 31.

1.3 Registering Identity Manager with Novell Audit

The option to register Identity Manager with the Secure Logging Server is available when you select the *Utilities* component in the Identity Manager installation program.

NOTE: For complete information on installing Identity Manager, see the *Identity Manager 3.5.1 Installation Guide*.

Figure 1-2 *Identity Manager Installation*



Please select the components to install:

☑ Novell Identity Manager Metadirectory Server

☑ Identity Manager Web Components

☑ Utilities

After you select *Utilities*, you can choose the option to *Register the Novell Audit System Component for Identity Manager*.

IMPORTANT: To complete this operation, Novell eDirectory version 8.7 or 8.8 must be installed on the current system and the Secure Logging Server must be installed in the tree.

Figure 1-3 Identity Manager Utilities Options

When the Identity Manager installation program completes this operation, it extends the eDirectory schema to include the Identity Manager instrumentation and events and it registers the Identity Manager application object with the Secure Logging Server.

Integrating Identity Manager with Novell Sentinel

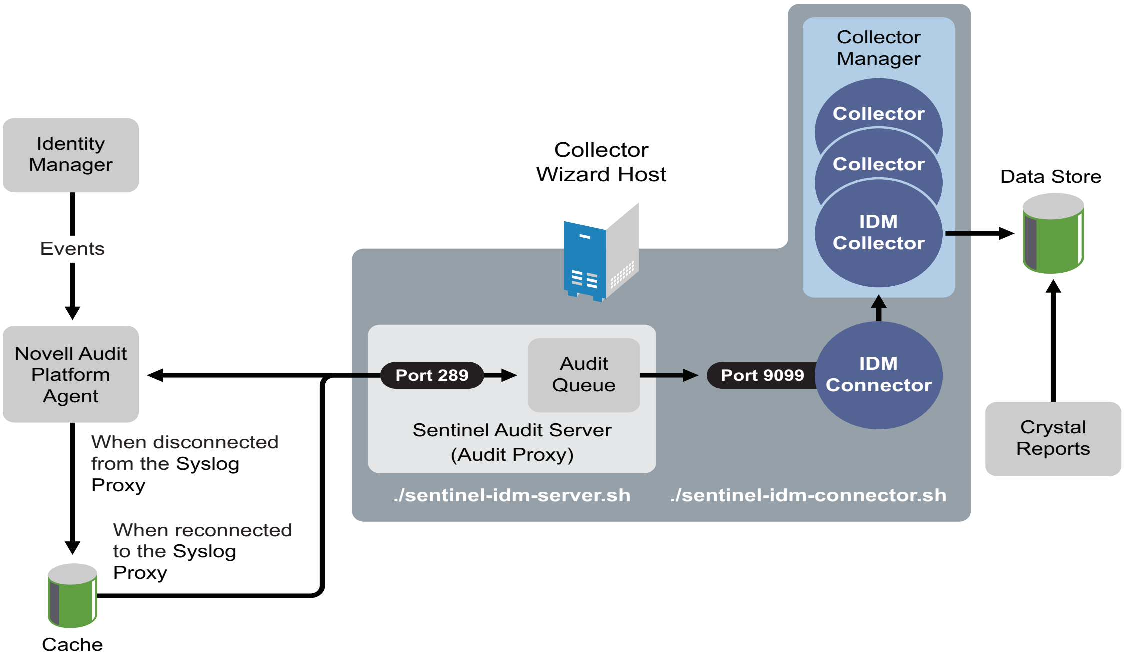
2

NOTE: Reporting and Notification Service (RNS) is deprecated in the current version of Identity Manager, although the Metadirectory engine continues to process RNS functions if you are currently using RNS. Nevertheless, we strongly recommend that you move to Novell® Audit or Novell® Sentinel™ because these auditing and reporting systems expand the functionality provided by RNS and RNS might not be supported in a future release of Identity Manager. For RNS documentation, see the *DirXML 1.1a Administration Guide* (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html).

Novell Sentinel 5.*x* is a security information management and compliance monitoring solution that monitors, responds to, and reports on security and compliance events. Novell Sentinel easily integrates with Novell Identity Manager so you get automated, real-time security management and compliance monitoring across all systems and networks. The Novell Sentinel-Identity Manager framework provides automatic documenting and reporting of security, systems, and access events across the enterprise; built-in incident management and remediation; and the ability to demonstrate and monitor compliance with internal policies and government regulations.

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

Figure 2-1 *Identity Manager and Novell Sentinel Integrated Architecture*



To enable Identity Manager to log events to Novell Sentinel, you must do the following:

1. Install and configure the Novell Sentinel server and Collector Wizard on your system.

For complete information on installing the Novell Sentinel server and Collector Wizard, see the *Novell Sentinel Installation Guide* (http://www.novell.com/documentation/sentinel5/pdfdoc/sentinel_install/NOV_vol_I_Sentinel_Install.pdf)

For a thorough discussion of the Novell Sentinel architecture, see "Sentinel Introduction" in the *Novell Sentinel User's Guide* (http://www.novell.com/documentation/sentinel5/pdfdoc/sentinel_scc_guide/NOV_vol_II_Sentinel_SCC_Guide.pdf).

For information on configuring the Novell Sentinel server, see the *Novell Sentinel User's Guide* (http://www.novell.com/documentation/sentinel5/pdfdoc/sentinel_scc_guide/NOV_vol_II_Sentinel_SCC_Guide.pdf) .

For information on using the Novell Sentinel Collector Wizard, see the *Novell Sentinel Wizard User's Guide* (http://www.novell.com/documentation/sentinel5/pdfdoc/sentinel_wizard_guide/NOV_vol_III_Sentinel_Wizard_Users_Guide.pdf).

2. Install the Novell Sentinel IDM Content Package (`Sentinel_IDM_Content_Package.zip`).

   The Novell Sentinel IDM Content package is available at Sentinel Collectors download site (http://support.novell.com/products/sentinel/collectors.html).

   For installation instructions, see the *Novell Sentinel IDM Content Package Installation Guide* (http://support.novell.com/products/sentinel/doc/Sentinel_IDM_Content_Package_Installation_Guide.pdf).

   For information about the Novell Audit Collector, see the *Novell Identity Manager 3 LOG 520 Collector Guide* (Novell_Identity_Manager_3_LOG_520.pdf), provided in the `\docs` directory of the Novell Sentinel IDM Content package.

   NOTE: The automatic installation installs the Novell Sentinel IDM Server, IDM Connector, and IDM Collector on the same machine. If you want to install the Novell Sentinel IDM Server on a different machine than the IDM Collector, you must modify the `sentinel-idm-connector.bat` file.

   For more information, see "Collector Pre-requisites" in the *Novell Identity Manager 3 LOG 520 Collector Guide (Novell_Identity_Manager_3_LOG_520.pdf)*.

3. Configure the Novell Audit Collector.

   The Novell Audit Collector is installed with the Novell Sentinel IDM Content Package. This Collector parses Identity Manager events received through the Novell Sentinel IDM Connector.

   For information about the Novell Audit Collector, see the *Novell Identity Manager 3 LOG 520 Collector Guide* (Novell_Identity_Manager_3_LOG_520.pdf)

4. Configure the Novell Sentinel Audit Server (Audit Proxy) and IDM Connector.

   The Novell Sentinel Audit Server (`sentinel-idm-server.sh`) and IDM Connector (`sentinel-idm-connector.sh`) are automatically installed with the Novell Sentinel IDM Content Package.

   For more information on installing Novell Sentinel Audit Server and IDM Connector, see Appendix E, "Sentinel IDM Connector" in the *Novell Identity Manager 3 LOG 520 Collector Guide* (Sentinel_IDM_Content_Package_Installation_Guide.pdf).

5. Install and configure the Platform Agent.

   The Platform Agent (`logevent`) is the client piece of the Novell auditing architecture.It is automatically installed if either the Novell *Identity Manager Metadirectory Server* or *Novell Identity Manager Connected System* option is selected during the Identity Manager install.

For more information on installing and configuring the Platform Agent, see Chapter 3, “Installing and Configuring the Platform Agent,” on page 17.

6. Select which Identity Manager events you want to log to Novell Audit.

   For more information, see Chapter 4, “Managing Identity Manager Events,” on page 21.

7. (optional) Secure the connection between Identity Manager and the Platform Agent.

   For more information, see “Securing the Connection with Novell Sentinel” on page 38.

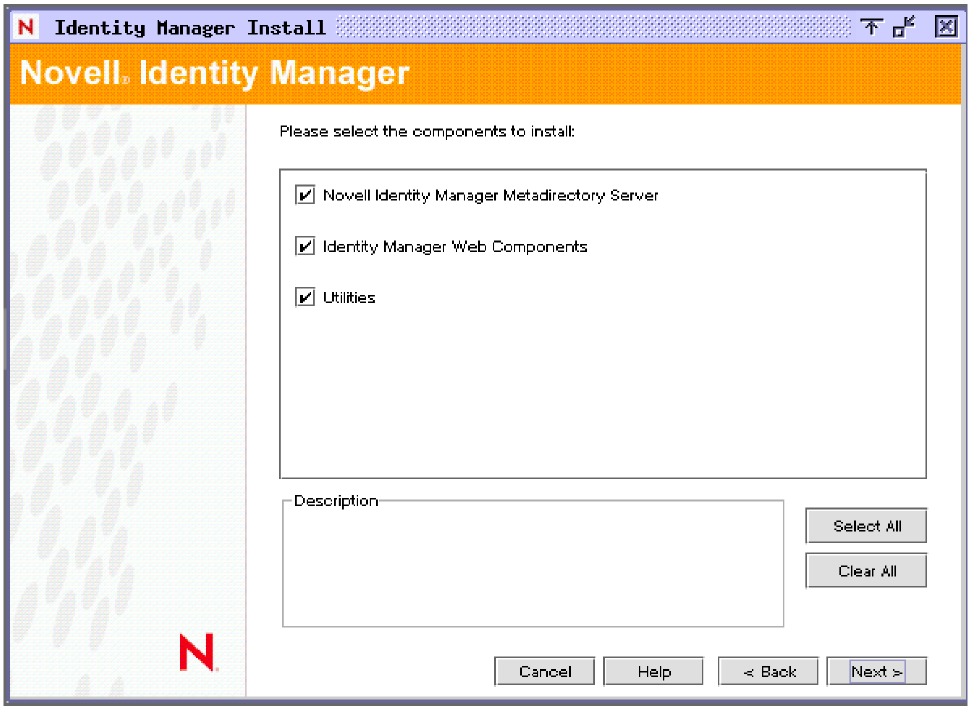
3 Installing and Configuring the Platform Agent

The Platform Agent, `logevent`, 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 or Novell® Sentinel™.

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 install. For more information on the Identity Manager installation, see the *Identity Manager 3.5.1 Installation Guide*.

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

Figure 3-1 *Identity Manager Installation*



Please select the components to install:

☑ Novell Identity Manager Metadirectory Server

☑ Identity Manager Web Components

☑ Utilities

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

Table 3-1 *Platform Agent Configuration File*

Operating System	File
NetWare®	SYS:/etc/logevent.cfg
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 host name or IP address of the Novell Audit Secure Logging Server or the Novell Sentinel Audit 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. Therefore, 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*.

Setting	Description
LogCacheDir=*path*	The directory where the Platform Agent stores the cached event information if the Novell Audit Secure Logging Server or Novell Sentinel Audit Server becomes unavailable.
LogEnginePort=*port*	The port at which the Platform Agent can connect to the Novell Audit Secure Logging Server or the Novell Sentinel Audit 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 or Novell Sentinel Audit 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 or the Novell Sentinel Audit 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 to `N` to prevent `lcache` from being unloaded.
LogCacheSecure=Y|N	Set the parameter to `Y` to encrypt the local cache file.
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 or Novell Sentinel Audit 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.

Setting	Description
LogSigned=Never|Always|Server	The signature setting for Platform Agent events. **IMPORTANT:** Novell Sentinel can receive and map Audit signatures to a Novell Sentinel event field; however, Novell Sentinel does not currently verify event signatures. ◆ 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. **NOTE:** The `Server` option applies only to Novell Audit systems. 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 or Novell® 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:

- Section 4.1, “Selecting Events to Log,” on page 21
- Section 4.2, “User-Defined Events,” on page 26
- Section 4.3, “eDirectory Objects that Store Identity Manager Event Data,” on page 29

4.1 Selecting Events to Log

The Identity Manager Instrumentation allows you to select events for a workflow, driver set, or a specific driver.

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

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

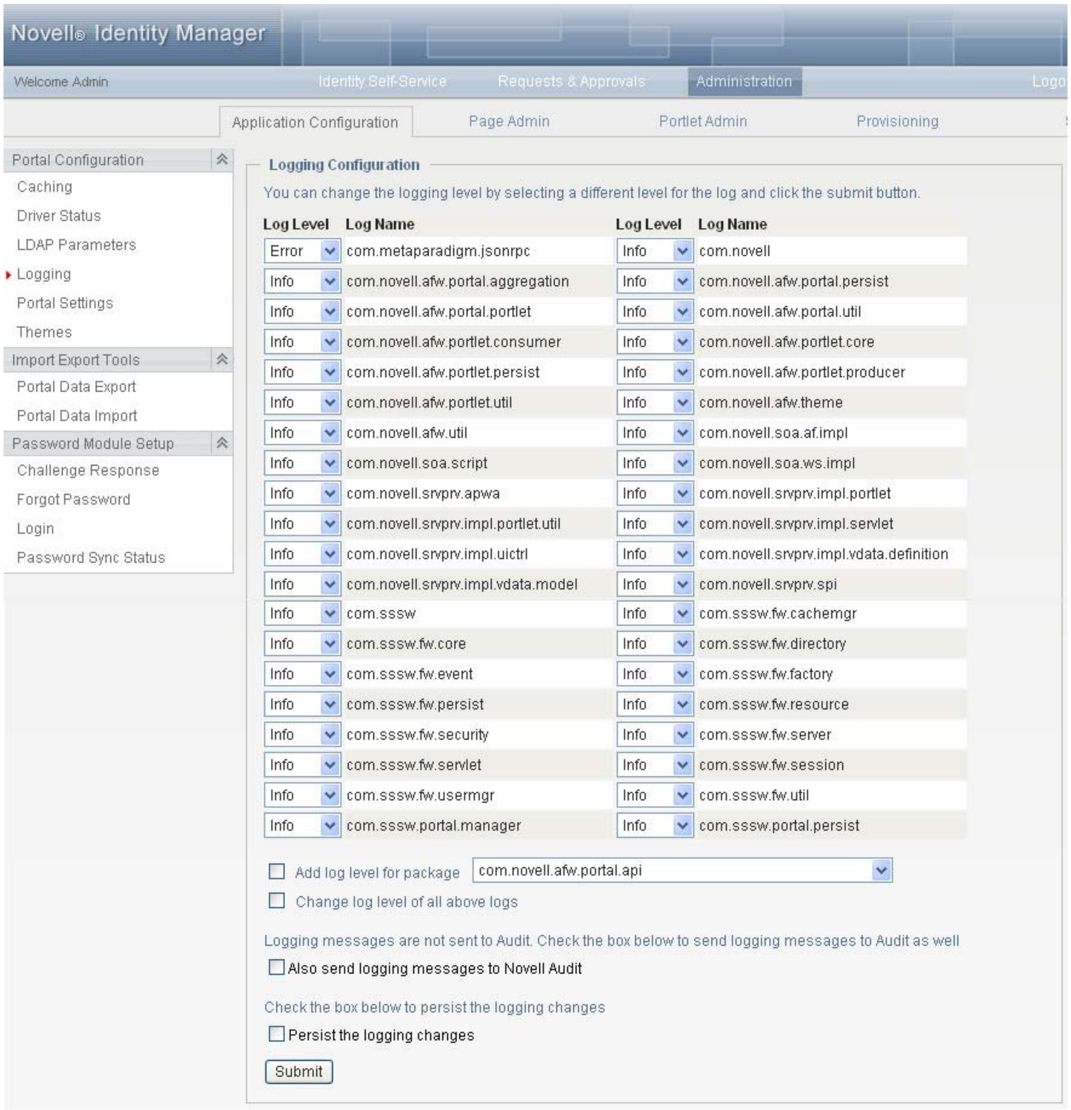
- “Selecting Events for the Driver Set” on page 23
- “Selecting Events for a Specific Driver” on page 24
- “Identity Manager Log Levels” on page 25

4.1.1 Selecting Events for a Workflow

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.



Logging Configuration

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

Log Level	Log Name	Log Level	Log Name
Error	com.metaparadigm.jsonrpc	Info	com.novell
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.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.definition
Info	com.novell.srvprv.impl.vdata.model	Info	com.novell.srvprv.spi
Info	com.sssw	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

☐ Add log level for package com.novell.afw.portal.api

☐ Change log level of all above logs

Logging messages are not sent to Audit. Check the box below to send logging messages to Audit as well

☐ Also send logging messages to Novell Audit

Check the box below to persist the logging changes

☐ Persist the logging changes

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 NovellAudit* check box to send the events to the Platform Agent..

6 To save the changes for any subsequent application server restarts, select *Persist the logging changes*.

7 Click *Submit*.

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

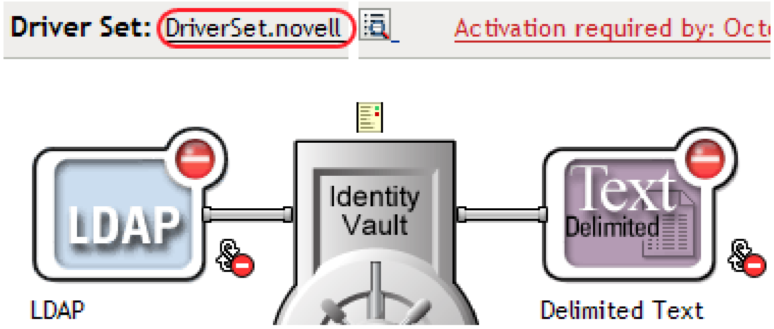
4.1.2 Selecting Events for the Driver Set

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

2 Browse to and select the Driver Set object, then click *Search*.

3 Click the driver set name.

The Modify Object page appears.



4 Select *Log Level* on the Identity Manager page, then select a log level for the driver set.

For an explanation of each log level, see "Identity Manager Log Levels" on page 25.

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

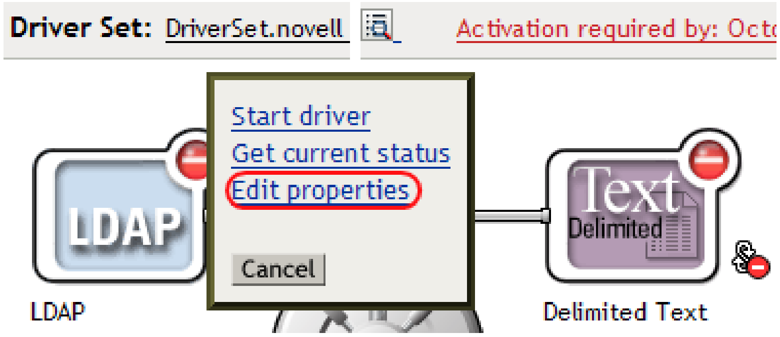
NOTE: Changes to configuration settings are logged by default.

4.1.3 Selecting Events for a Specific Driver

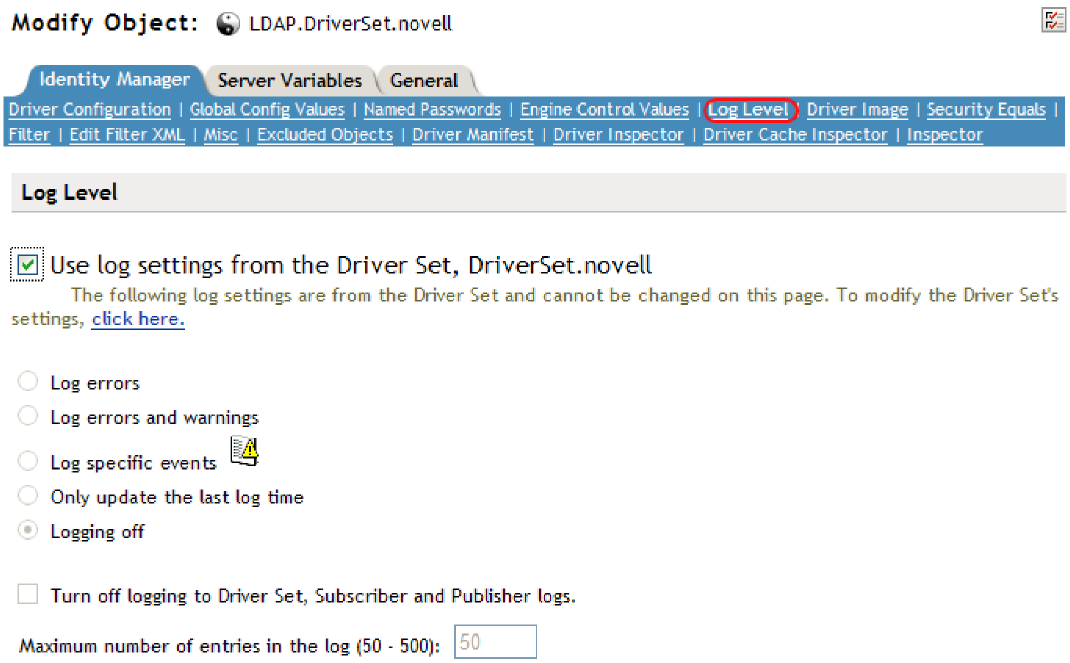
1 In iManager select *Identity Manager* > *Identity Manager Overview*.

2 Browse to and select the Driver Set object, then click *Search*.

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



4 Select *Log Level* on the Identity Manager page.


Modify Object: LDAP.DriverSet.novell
Identity Manager
Server Variables
General
Driver Configuration | Global Config Values | Named Passwords | Engine Control Values | Log Level | Driver Image | Security Equals | Filter | Edit Filter XML | Misc | Excluded Objects | Driver Manifest | Driver Inspector | Driver Cache Inspector | Inspector

Log Level

☑ Use log settings from the Driver Set, DriverSet.novell

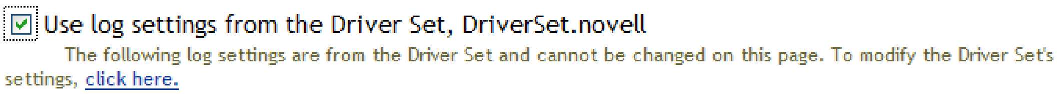
The following log settings are from the Driver Set and cannot be changed on this page. To modify the Driver Set's settings, click here.

○ Log errors
○ Log errors and warnings
○ Log specific events
○ Only update the last log time
● Logging off

□ Turn off logging to Driver Set, Subscriber and Publisher logs.

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

5 (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 DriverSet*.



☑ 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.

6 Select a log level for the current driver.

For an explanation of each log level, see "Identity Manager Log Levels" on page 25.

7 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:

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.
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 45.
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 7.2, "Viewing Status Logs," on page 43 for details.

4.2 User-Defined Events

Identity Manager enables you to configure your own events to log to Novell Audit or Novell Sentinel. Events can be logged by using an action in 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.

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.

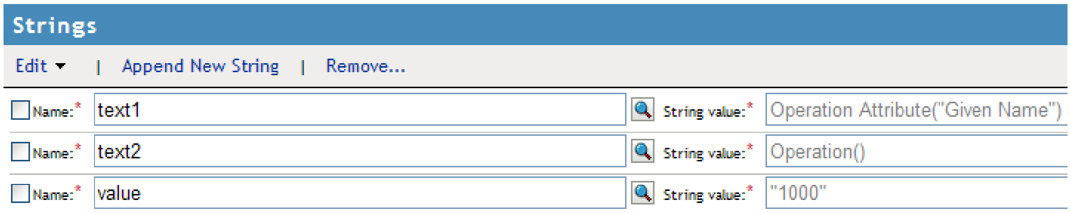
Log levels enable you to group events based on the type of event being logged. The following predefined log levels are available:

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.



□ Name:* text1 String value:* Operation Attribute("Given Name")

□ Name:* text2 String value:* Operation()

□ Name:* value String value:* "1000"

NOTE: 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.

Field	Description
value3	The value of this field depends upon the event. It can contain any numeric value up to 32 bits.
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 17. 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” (http://www.novell.com/documentation/idm35/policy_designer/data/dogenerateevent.html#dogenerateevent) in the *Policies in Designer 2.1* 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 or Novell 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 4-1 *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 an 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 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 contents of the DirXML-LogEvent attribute to determine whether the event should be logged.

Previous versions of Identity Manager used the DirXML-DriverTraceLevel attribute to set up logging levels. The logging level was specified on each Driver object and did not support inheritance. In versions after Identity Manager 2.x, Driver objects can inherit log settings from the Driver Set object. 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 object.

Securing the Logging System 5

The following sections review how to secure the connection between Identity Manager and your logging system:

- Section 5.1, "Securing the Connection with Novell Audit," on page 31
- Section 5.2, "Securing the Connection with Novell Sentinel," on page 38

5.1 Securing the Connection with Novell Audit

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). Likewise, 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 5.1.1, "Updating the Novell Audit Certificate Infrastructure," on page 31
- Section 5.1.2, "The Novell Audit AudCGen Utility," on page 32
- Section 5.1.3, "Creating a Root Certificate for the Secure Logging Server," on page 34
- Section 5.1.4, "Creating Logging Application Certificates," on page 36
- Section 5.1.5, "Validating Certificates," on page 36
- Section 5.1.6, "Securing Custom Certificates," on page 37

5.1.1 Updating the Novell Audit Certificate Infrastructure

You can substitute the internal Novell Audit CA and embedded product certificates with 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 will not be 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. 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.

5.1.2 The Novell Audit AudCGen Utility

IMPORTANT: There are many versions of the AudCGen utility. This section documents the most recent version of AudCGen 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 5-1 *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 using the `-base` parameter.
–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 using the `-base` parameter.

Parameter	Description
–base	The base path used when reading from or writing to files. The default path is platform-specific.
–bits:*RSA_key_siz*e	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 using the –base parameter.
–capkey:*filename*	The path and filename to the private key used by the Novell Audit Secure Logging Server (SLS). The SLS 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 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 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.
–h|?	Provides the AudCGen help screen.

Parameter	Description
–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	Verify 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 36.

5.1.3 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.

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

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

To generate a self-signed root certificate for the Secure Logging Server 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 this procedure, see "Creating Logging Application Certificates" on page 36.

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
   ```

2. Take the `slscsr.pem` file and submit it to a third-party CA for signature or sign it 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 will no longer be able to communicate with the Secure Logging Server using their default certificates. You must create a new certificate key pair for each logging application using AudCGen and the new root certificate key pair.

5.1.4 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 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 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
```

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 5-2 *Identity Manager Certificate and Key Paths and Filenames*

Platform	Certificate Path and Filename	PrivateKey Path and Filename
NetWare®	`sys:\system\dxicert.pem`	`sys:\system\dxipkey.pem`
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 noted locations will 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>
```

5.1.5 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 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
```

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 will still trust the Secure Logging Server root certificate and its associated logging application certificates.

5.1.6 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.

NetWare

On NetWare, the custom certificates and private key files can be protected with file system trustees and inherited rights filters. The Identity Manager instrumentation uses `sys:\system\dxipkey.pem` as the private key.

To limit access to the private key files:

1 Grant the auditor user Object rights to the key files.

2 Using iManager, or any other management tool, implement an inherited rights filter on the key file.

It is not possible to filter the Supervisor inheritance on files in a file system. Users with Supervisor rights to `sys:/system` can still access the key files. Therefore, grant Supervisor access to objects and volumes sparingly.

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.

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.

5.2 Securing the Connection with Novell Sentinel

The Audit Server and Identity Manager Instrumentation utilize embedded certificates generated by an internal Certificate Authority (CA). These SSL certificates ensure that communications between the Identity Manager instrumentation and the Audit Server are secure.

Querying and Reporting

6

After you integrate Identity Manager with Novell® Audit or Novell® Sentinel™, you can log system information to a central data store. However, logging information is only half the battle. Obviously, you have to be able to access and understand your log data for the information to be useful. Queries and reports allow you to view and interpret the information in your data store.

This section reviews how you can run reports in Novell Audit and Novell Sentinel.

- Section 6.1, “Querying Data and Generating Reports in Novell Audit,” on page 39
- Section 6.2, “Novell Sentinel Reports,” on page 40

6.1 Querying Data and Generating Reports in Novell Audit

Novell Audit provides two tools to query events and generate reports: the Novell Audit iManager plug-in and Novell Audit Report (`LReport`).

The following sections provide more information on these tools:

- Section 6.1.1, “The Novell Audit iManager Plug-in,” on page 39
- Section 6.1.2, “Novell Audit Report,” on page 39

6.1.1 The Novell Audit iManager Plug-in

The Novell Audit iManager plug-in is a Web-based JDBC* application that enables you to query MySQL* and Oracle* databases. All queries are defined in SQL.

iManager includes several predefined queries and it includes a Query Builder to help you define basic query statements. Of course, you can also build your own SQL query statements.

For complete information on defining and running queries in iManager, see the following sections in the *Novell Audit 2.0 Administration Guide*.

- “Defining Your Query Databases in iManager”
- “Defining Queries in iManager”
- “Running Queries in iManager”
- “Verifying Event Authenticity in iManager”
- “Exporting Query Results in iManager”
- “Printing Query Results in iManager”

6.1.2 Novell Audit Report

Novell Audit Report is a Windows-based, ODBC-compliant application that can use SQL query statements or Crystal Decisions* Reports to query Oracle and MySQL data stores (or any other database that has ODBC driver support). You can define your own SQL query statements or import existing query statements and reports. Query results are returned in simple data tables; rows represent individual records and columns represent fields within those records.

For complete information on defining and running queries in Novell Audit Report, see the following sections in the *Novell Audit 2.0 Administration Guide*.

- “Novell Audit Report Interface”
- “Defining Your Databases in Novell Audit Report”
- “Verifying Event Authenticity in Novell Audit Report”
- “Working with Reports in Novell Audit Report”
- “Working with Queries in Novell Audit Report”

Identity Manager Reports

In Novell Audit Report, the term “reports” refers specifically to Crystal Decisions Report Template Files (`*.rpt`). Crystal Decisions Reports graphically summarize specific sets of log data in pie charts, bar charts, and so forth.

Identity Manager provides a number of Crystal Decisions Reports (`*.rpt`) that simplify gathering information on common operations performed in Identity Manager. These reports are included on the Identity Manager installation CD. For examples of these reports, see Appendix B, “Identity Manager Reports,” on page 49.

6.2 Novell Sentinel Reports

Novell Sentinel is integrated with Crystal Reports* to generate and display reports. To run the report templates, you must first configure the location of the Crystal Enterprise Server that publishes reports in the General Options window of the Admin page.

After Novell Sentinel is configured to access the Crystal Enterprise Server, the Analysis page allows administrators to run historical reports. Vulnerability reports are available from the Advisor page. These reports are published on a Web server, they run directly against the database, and they then appear on the Analysis and Advisor pages on the Navigator bar.

For more information on running reports in Novell Sentinel, see the “Analysis Tab” and “Advisor Tab” sections in the *Novell Sentinel User’s Guide* (http://www.novell.com/documentation/sentinel5/pdfdoc/sentinel_scc_guide/NOV_vol_II_Sentinel_SCC_Guide.pdf). For examples of Novell Sentinel provisioning reports, see Section B.2, “Novell Sentinel Reports,” on page 64.

Using Status Logs

7

In addition to the functionality provided by Novell® Audit, Identity Manager logs a specified number of events on the Driver Set object and Driver object. 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 or Novell® Sentinel™.

7.1 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 on the Driver Set object to be inherited by all drivers in the set, or configured for each driver in the 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 on 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 7.1.1, "Setting the Log Level and Log Size on the Driver Set," on page 41
- Section 7.1.2, "Setting the Log Level and Log Size on the Driver," on page 42

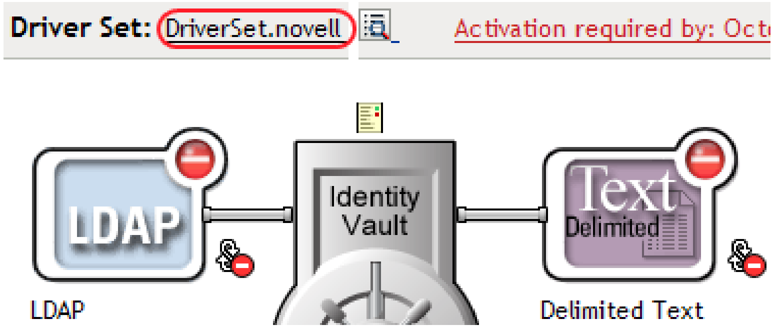
7.1.1 Setting the Log Level and Log Size on the Driver Set

1 In iManager, select *Identity Manager* > *Identity Manager Overview*, then click *Next*.

2 Browse to and select the Driver Set object, then click *Search*.

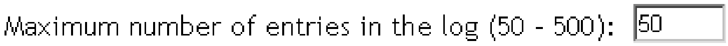
3 Click the driver set name.

The Modify Object window appears.



4 Select *Log Level* on the Identity Manager page.

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



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

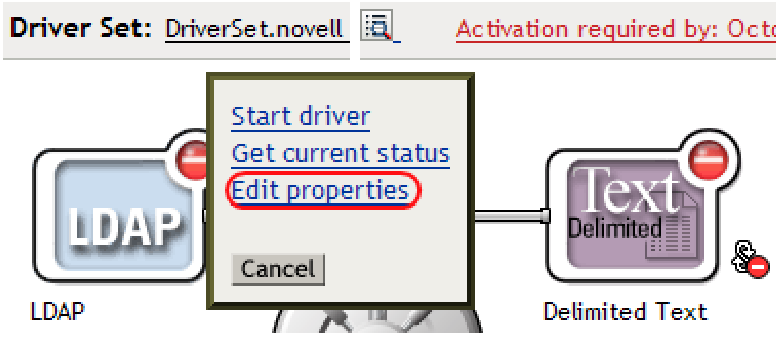
6 After you have specified the maximum number, click *OK*.

7.1.2 Setting the Log Level and Log Size on the Driver

1 In iManager select *Identity Manager* > *Identity Manager Overview*, then click *Next*.

2 Browse to and select the Driver Set object, then click *Search*.

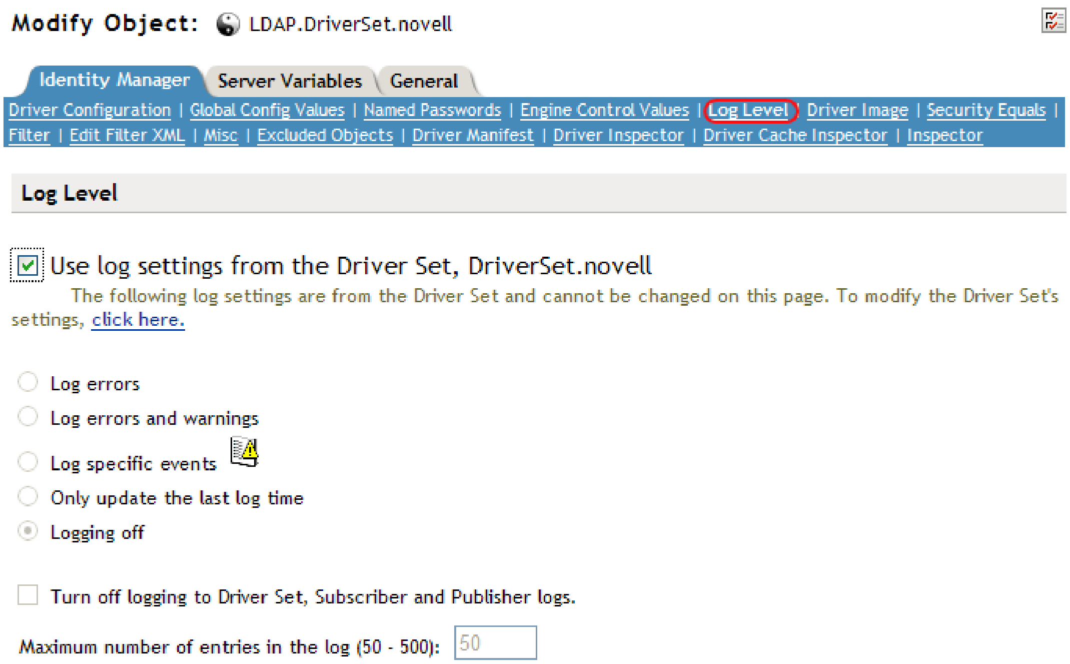
3 Click the upper right corner of the driver icon, then select *Edit properties*.



Driver Set: DriverSet.novell

Activation required by: Octo

4 Select *Log Level* on the Identity Manager page.


Modify Object: LDAP.DriverSet.novell
Identity Manager
Server Variables
General
Driver Configuration | Global Config Values | Named Passwords | Engine Control Values | Log Level | Driver Image | Security Equals | Filter | Edit Filter XML | Misc | Excluded Objects | Driver Manifest | Driver Inspector | Driver Cache Inspector | Inspector

Log Level

☑ 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.

○ Log errors

○ Log errors and warnings

○ Log specific events

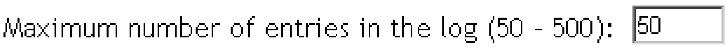
○ Only update the last log time

● Logging off

□ Turn off logging to Driver Set, Subscriber and Publisher logs.

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

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



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

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

7.2 Viewing Status Logs

Status log entries are represented in iManager with a status log icon . Anywhere you see this icon in iManager, you can view a short-term log. The following status logs are available:

- On the driver set.
- On the Publisher channel for each driver in the set.
- On the Subscriber channel for each driver in the set.

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.

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.

Identity Manager Events

A

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

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 event structure, see "Event Structure " in the *Novell Audit 2.0 Administration Guide*

The following sections list the Identity Manager events and their associated field information and triggers.

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 7.1, "Setting the Log Level and Maximum Log Size," on page 41.
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 7.1, "Setting the Log Level and Maximum Log Size," on page 41.

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 7.1, "Setting the Log Level and Maximum Log Size," on page 41.

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 provides the list of 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 provides the list of 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 provides the list of 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, you must select the *Log Specific Events* log level and specify this event. For more information, see Section 7.1, “Setting the Log Level and Maximum Log Size,” on page 41
EV_LOG_DRIVER_STOP	LOG_WARNING	To log driver stops, select *Log Errors and Warnings* log level, or select the *Log Specific Events* log level and specify this event. For more information, see Section 7.1, “Setting the Log Level and Maximum Log Size,” on page 41.

Identity Manager Reports

B

This section provides examples of reports that can be generated in Novell® Audit and Novell® Sentinel™:

- Section B.1, “Novell Audit Reports,” on page 49
- Section B.2, “Novell Sentinel Reports,” on page 64

B.1 Novell Audit Reports

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

- “Administrative Action Report” on page 49
- “Historical Approval Flow Report” on page 50
- “Resource Provisioning Report” on page 52
- “Specific User Audit Trail Report I” on page 54
- “Specific User Audit Trail Report II” on page 56
- “Specific User Audit Trail III” on page 58
- “Specific User Provisioning Report” on page 60
- “User Provisioning Report” on page 62

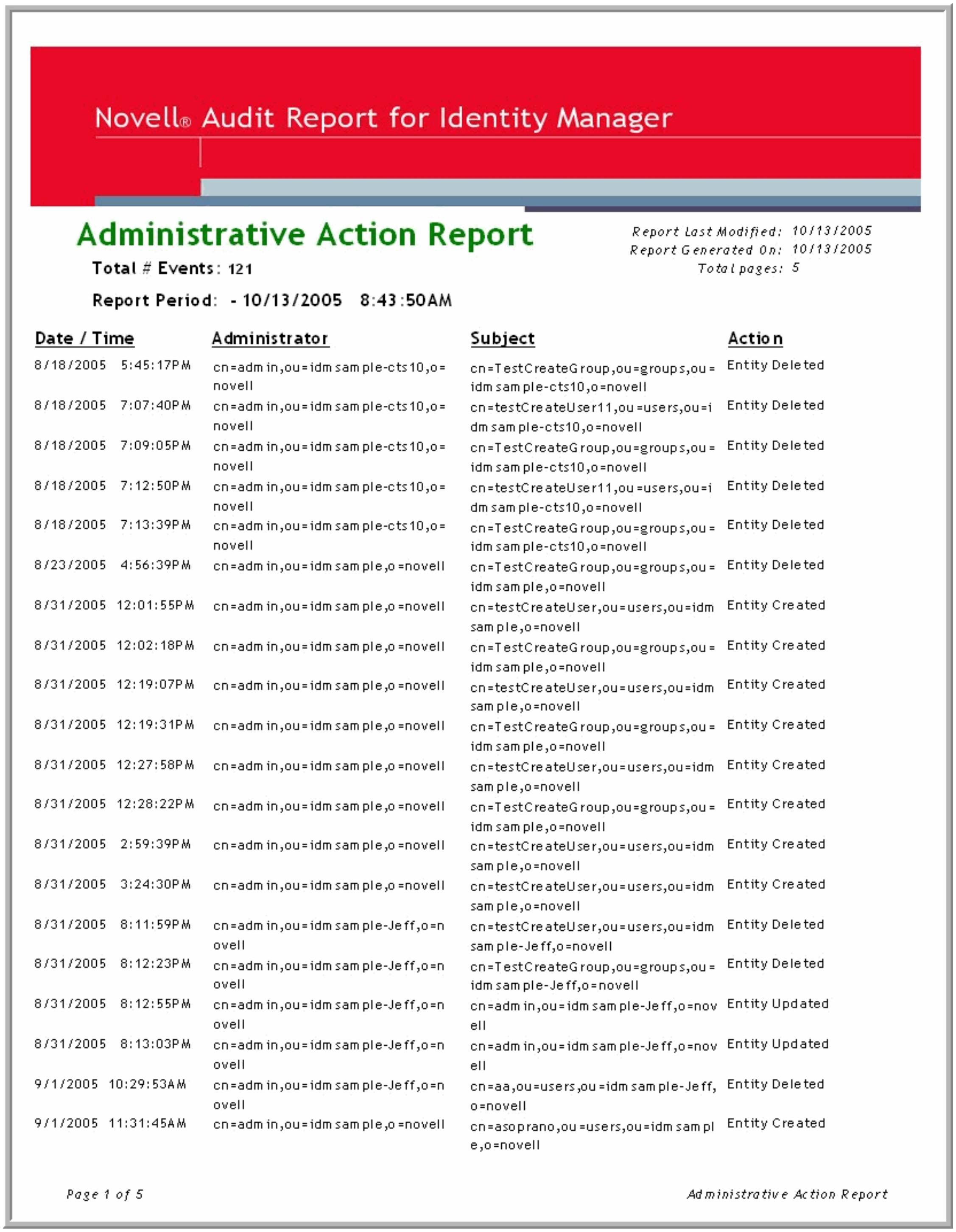
B.1.1 Administrative Action Report

The Administrative Action Report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

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

Total # Events: 121

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

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

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*

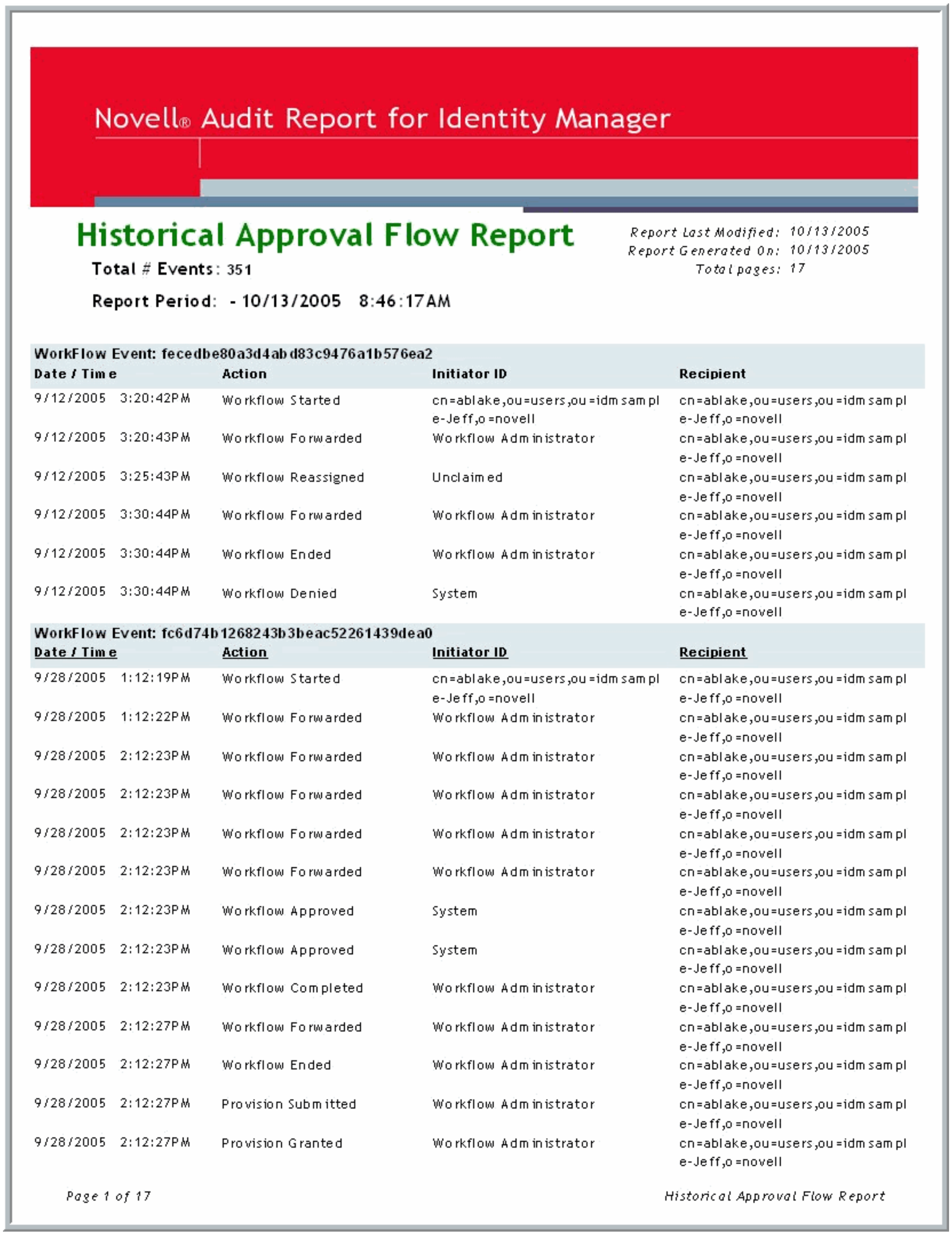
B.1.2 Historical Approval Flow Report

The Historical Approval Report is generated from the events listed in the following table. For more information on each event, see Appendix A, "Identity Manager Events," on page 45.

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

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

Total # Events: 351

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

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

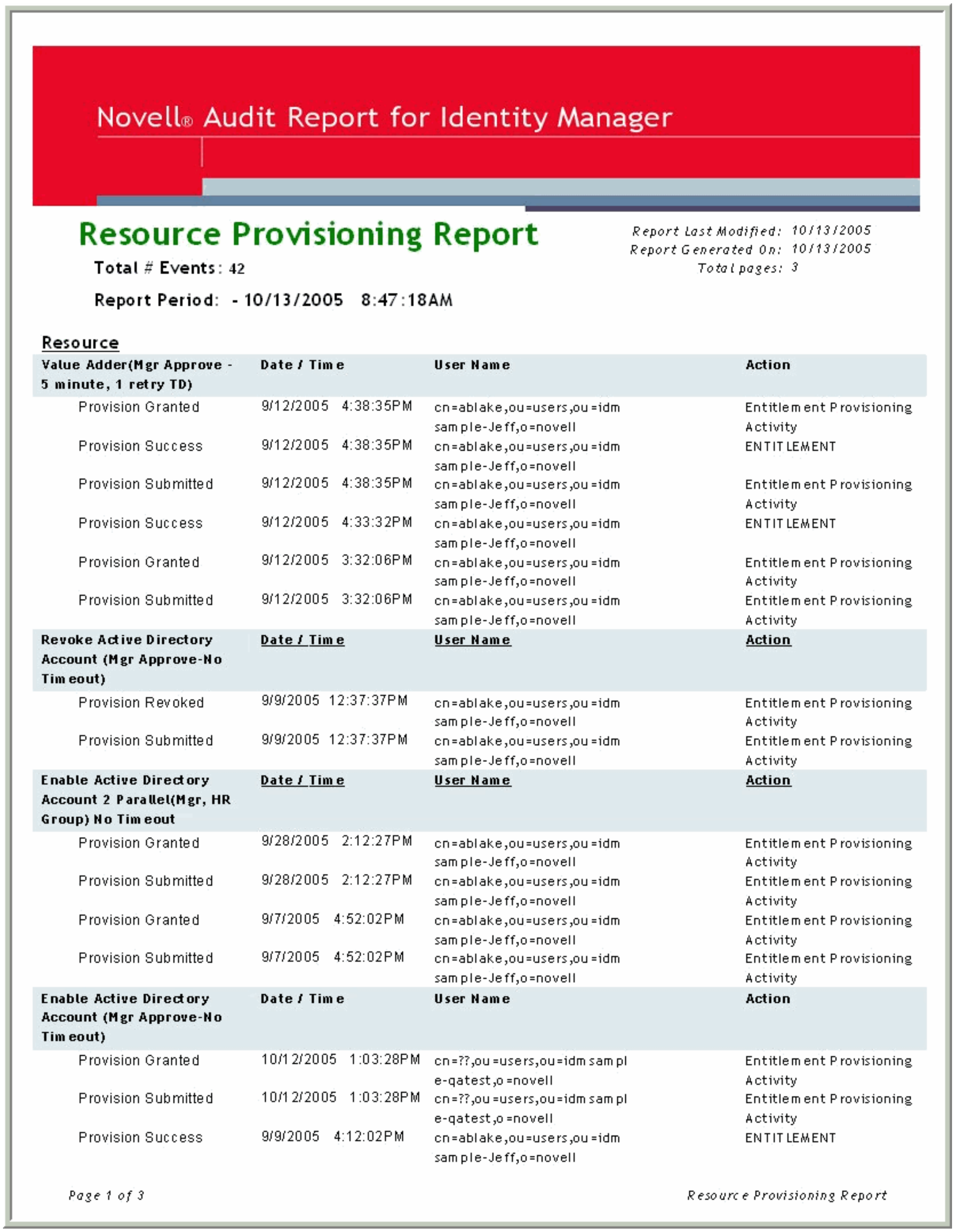
B.1.3 Resource Provisioning Report

The Resource Provisioning Report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

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 during the provisioning step on submission of entitlements.
3152F	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.

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=idmsample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idmsample-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=idmsample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idmsample-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=idmsample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Granted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idmsample-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=idmsample-qatest,o=novell	Entitlement Provisioning Activity
Provision Submitted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idmsample-qatest,o=novell	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	ENTITLEMENT

Page 1 of 3

Resource Provisioning Report

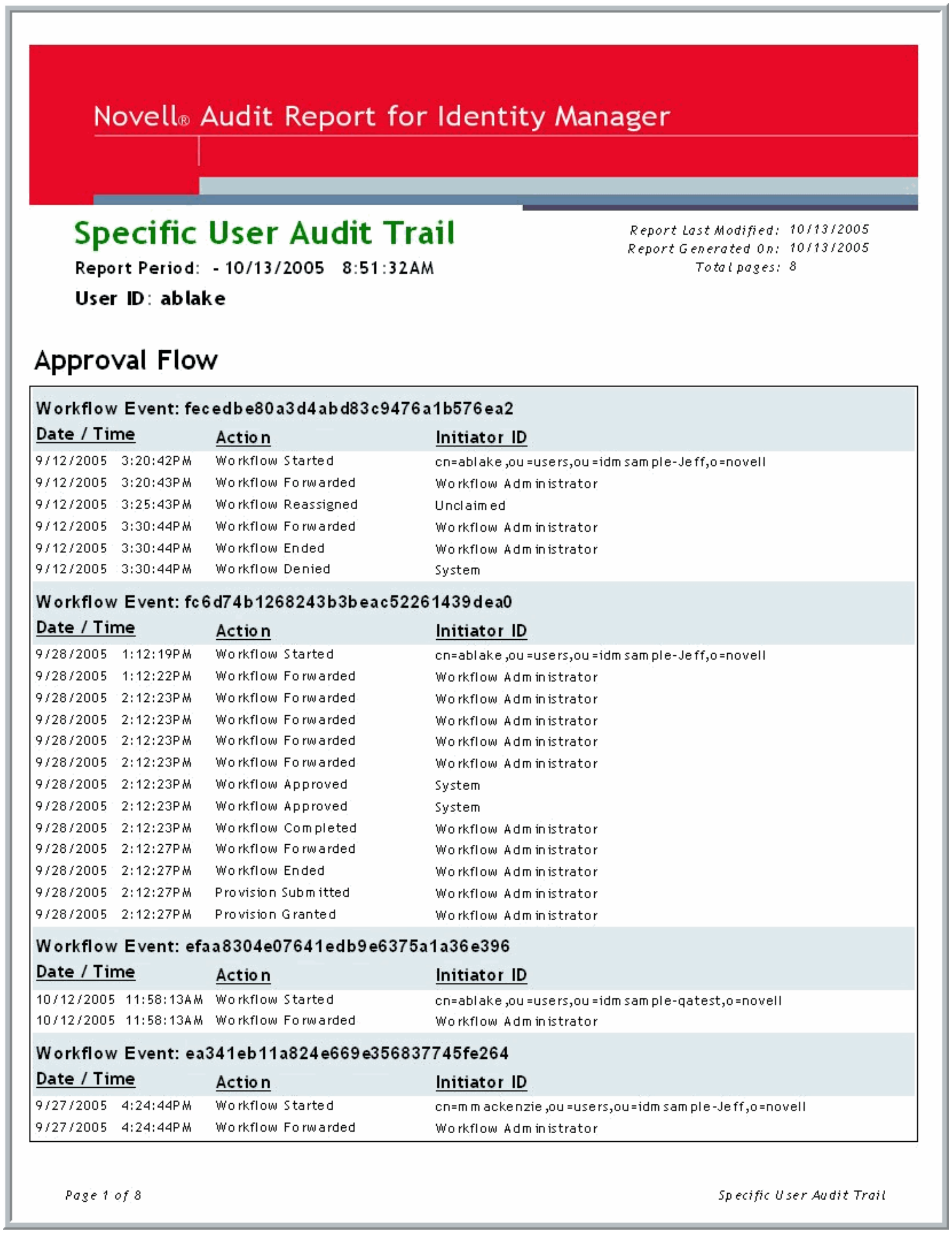
B.1.4 Specific User Audit Trail Report I

The Specific User Audit Trail Report I is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

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

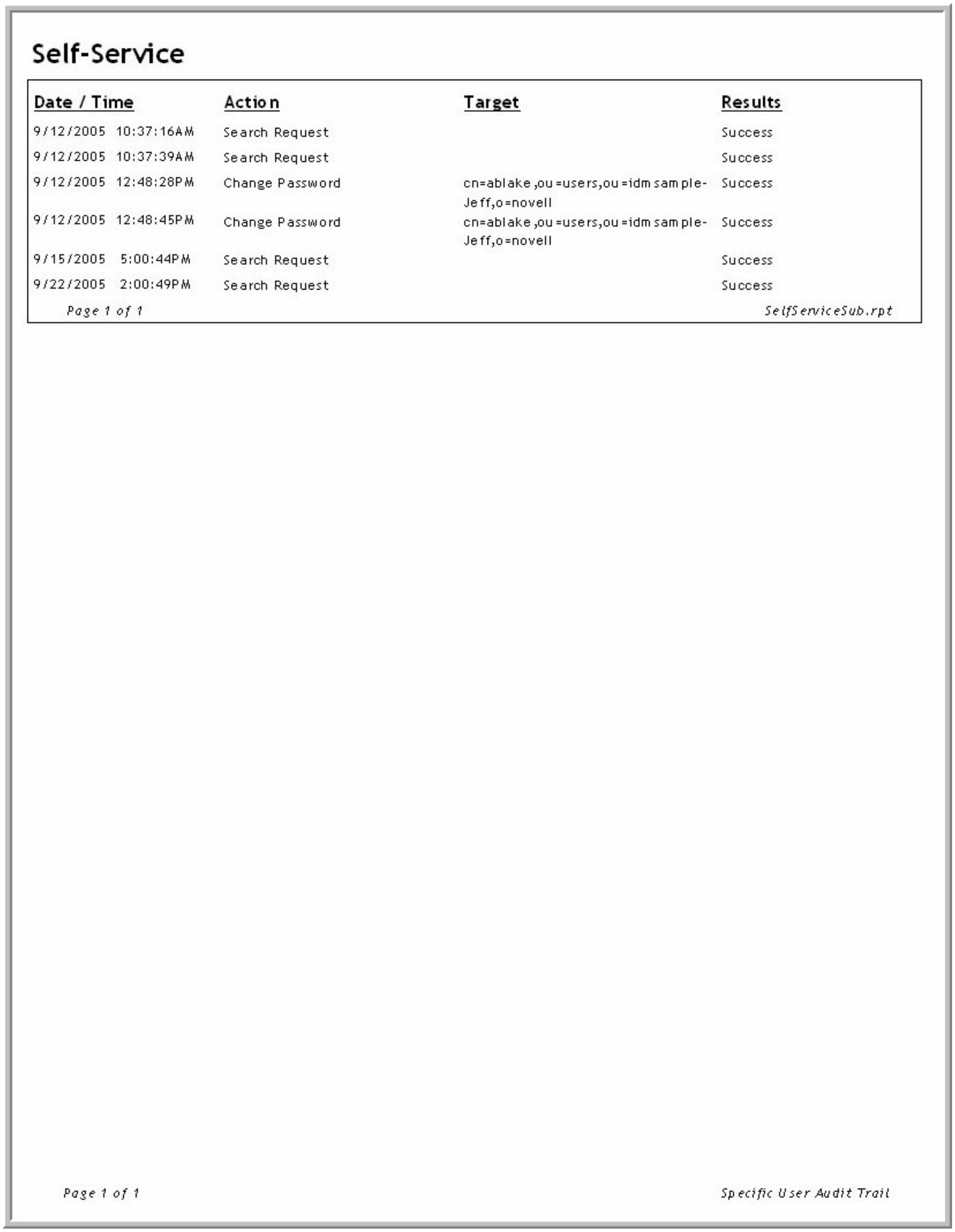
B.1.5 Specific User Audit Trail Report II

The Specific User Audit Trail Report II is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

Table B-5 User Audit Trail Events

Event ID	Description	Trigger
30007	Search	Occurs when a query document is sent to the IDM 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

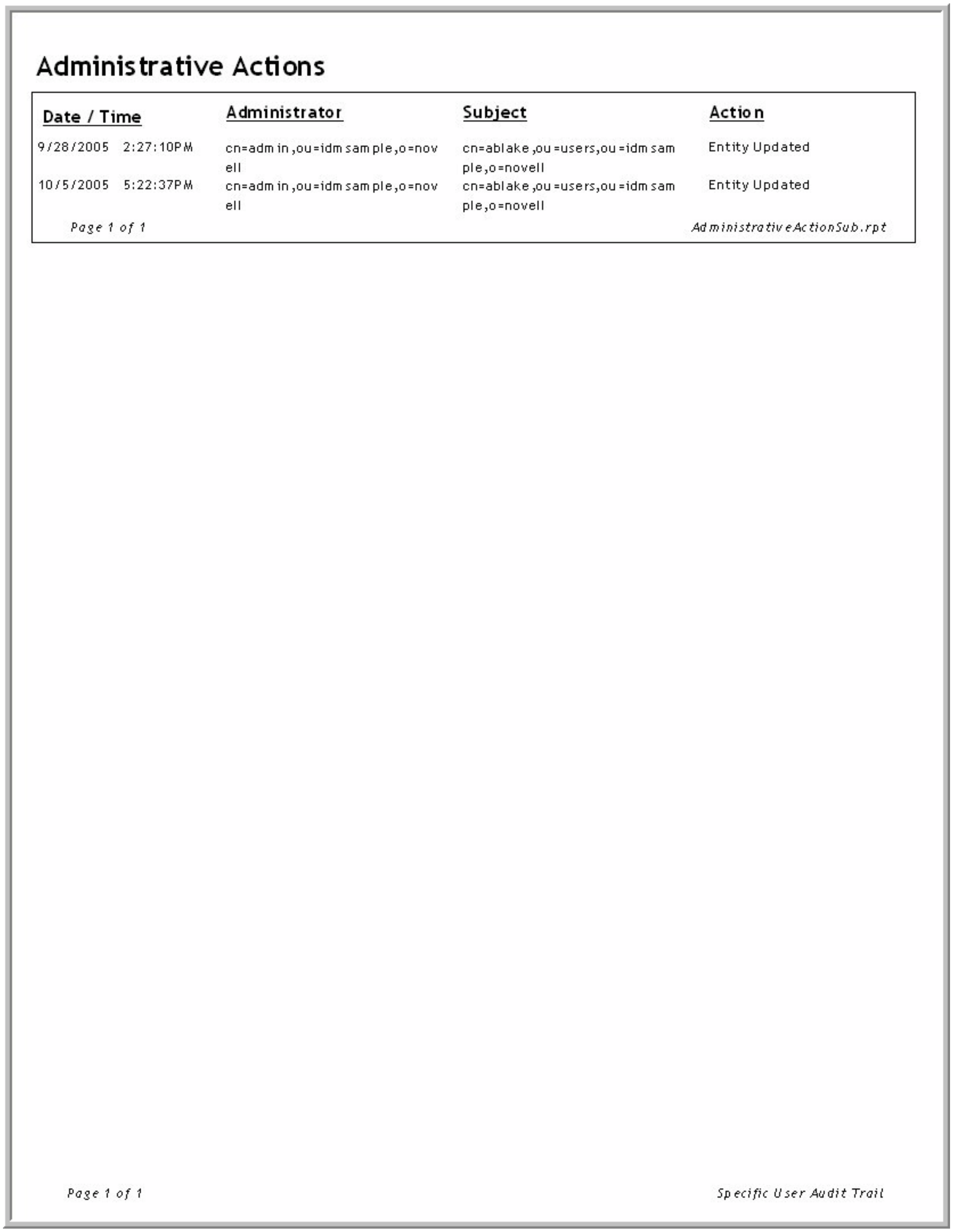
B.1.6 Specific User Audit Trail III

The Specific User Audit Trail III Report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

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

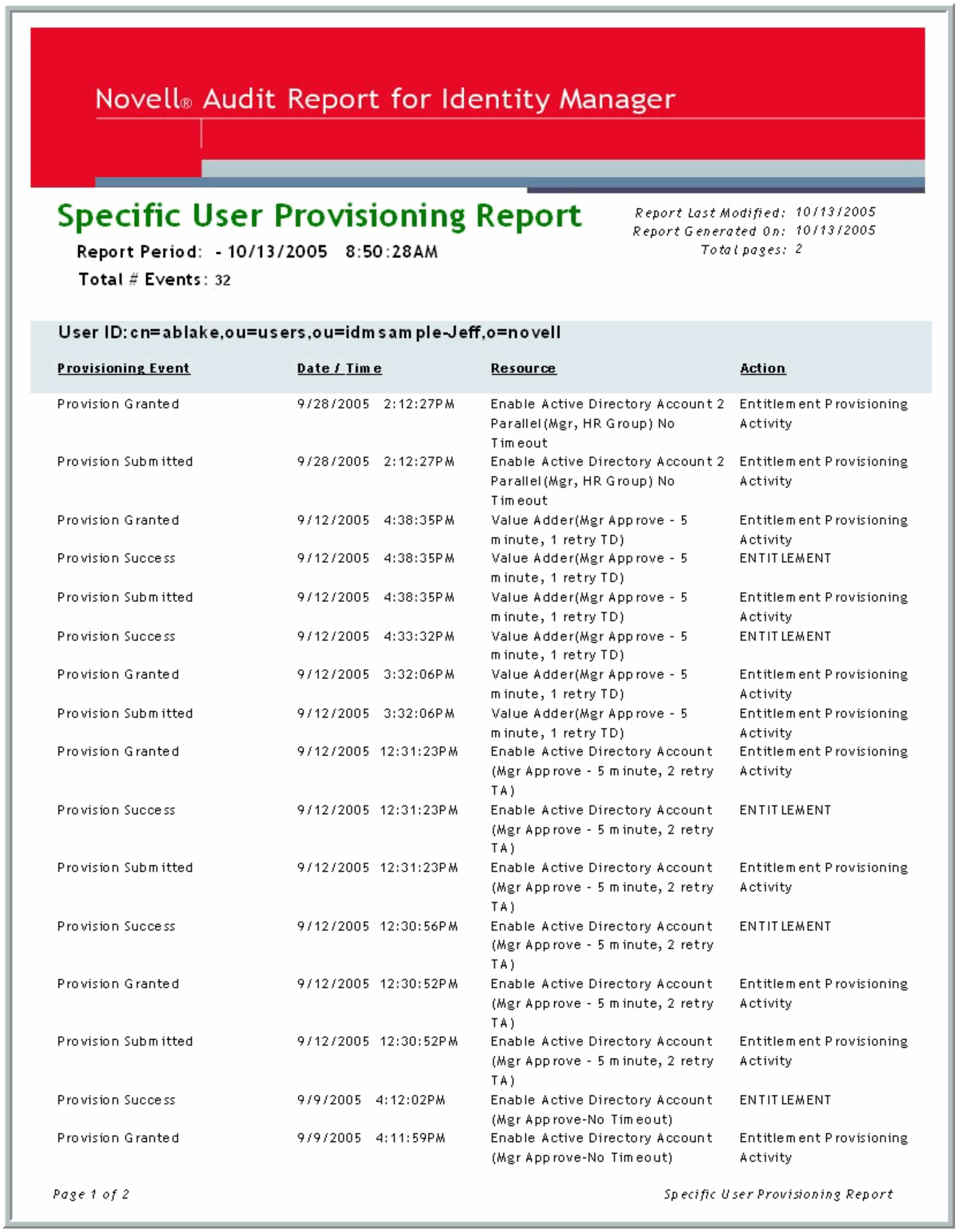
B.1.7 Specific User Provisioning Report

The Specific User Provisioning Report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

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 during the provisioning step on submission of entitlements.
3152F	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.

Figure B-7 Specific User Provisioning Report



Novell® Audit Report for Identity Manager

Specific User Provisioning Report

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

Total # Events: 32

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

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

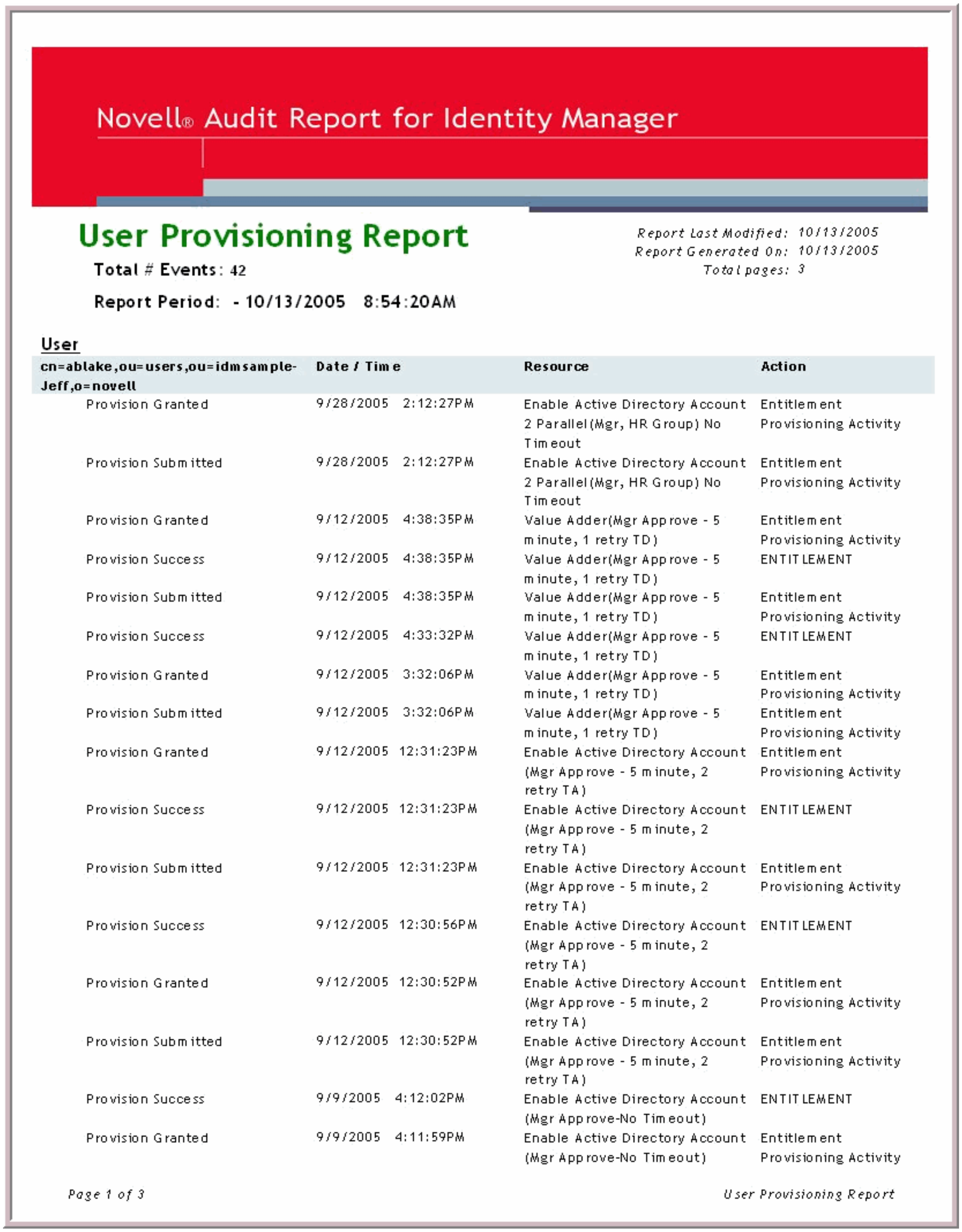
B.1.8 User Provisioning Report

The User Provisioning Report is generated from the events listed in the following table. For more information on each event, see Appendix A, "Identity Manager Events," on page 45.

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 during the provisioning step on submission of entitlements.
3152F	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.

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*

B.2 Novell Sentinel Reports

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

- "Administrative Action Report" on page 65

- "Historical Approval Flow Report" on page 66
- "Password Management Report" on page 68
- "Provisioning Report by Top 10 DIPs" on page 70
- "Provisioning Report by Top 10 Target Systems" on page 73
- "Resource Provisioning Report" on page 75
- "Specific User Audit Trail Report" on page 76
- "Specific User Provisioning Report" on page 78
- "Sync vs. Reset Report" on page 80
- "User Provisioning Report" on page 82
- "Workflow Status by Top Ten DIPs Report" on page 84
- "Workflow Status by Top Ten Target Systems Report" on page 87

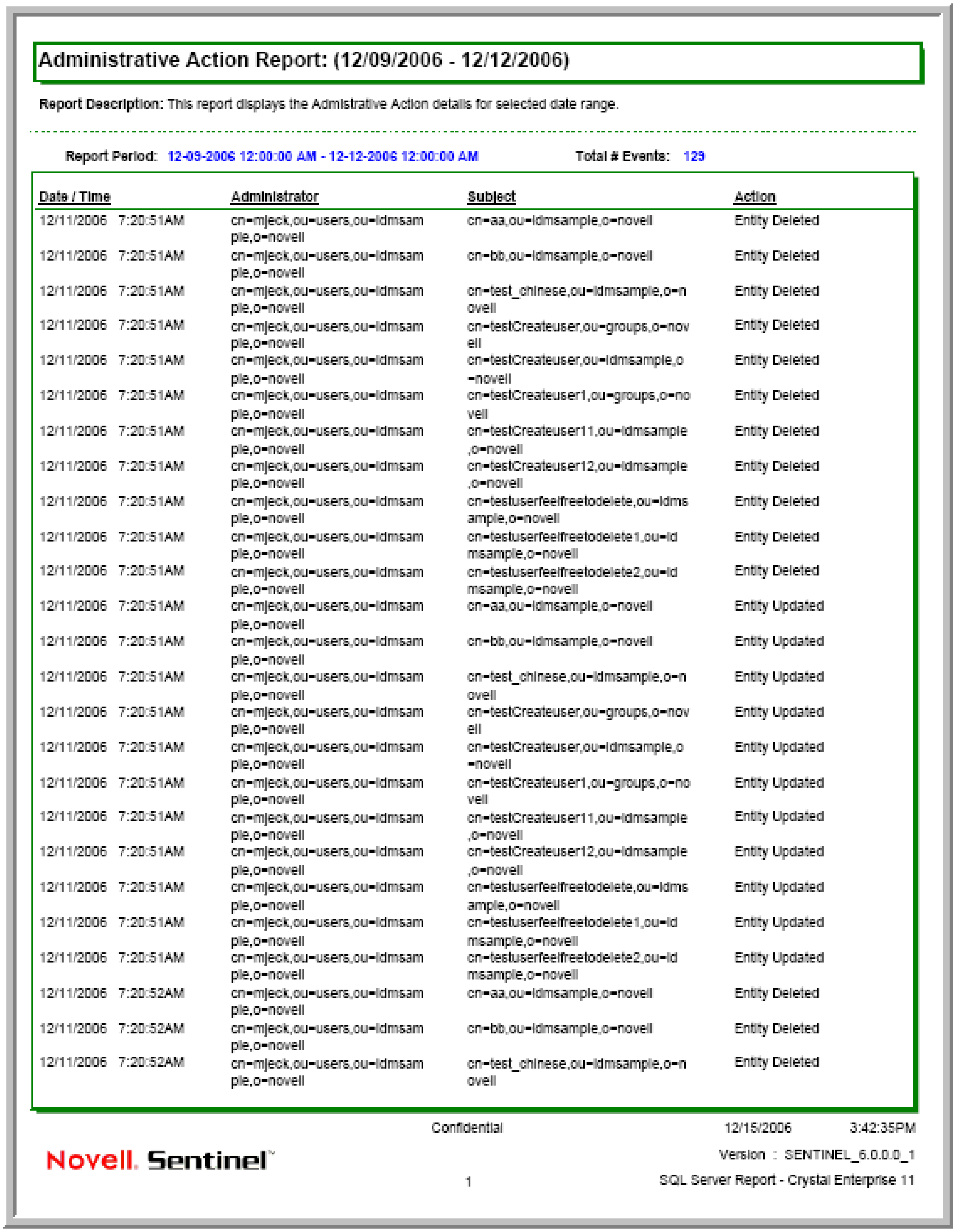
B.2.1 Administrative Action Report

The Administrative Action Report is generated from the events listed in the following table. For more information on each event, see Appendix A, "Identity Manager Events," on page 45.

***Table B-9** 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-9 Administrative Action Report



Administrative Action Report: (12/09/2006 - 12/12/2006)

Report Description: This report displays the Admistrative Action details for selected date range.

Report Period: 12-09-2006 12:00:00 AM - 12-12-2006 12:00:00 AM Total # Events: 129

Date / Time	Administrator	Subject	Action
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=aa,ou=idmsample,o=novell	Entity Deleted
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=bb,ou=idmsample,o=novell	Entity Deleted
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=test_chinese,ou=idmsample,o=novell	Entity Deleted
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testCreateuser,ou=groups,o=novell	Entity Deleted
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testCreateuser,ou=idmsample,o=novell	Entity Deleted
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testCreateuser1,ou=groups,o=novell	Entity Deleted
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testCreateuser11,ou=idmsample,o=novell	Entity Deleted
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testCreateuser12,ou=idmsample,o=novell	Entity Deleted
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testuserfeelfreetodelete,ou=idmsample,o=novell	Entity Deleted
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testuserfeelfreetodelete1,ou=idmsample,o=novell	Entity Deleted
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testuserfeelfreetodelete2,ou=idmsample,o=novell	Entity Deleted
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=aa,ou=idmsample,o=novell	Entity Updated
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=bb,ou=idmsample,o=novell	Entity Updated
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=test_chinese,ou=idmsample,o=novell	Entity Updated
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testCreateuser,ou=groups,o=novell	Entity Updated
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testCreateuser,ou=idmsample,o=novell	Entity Updated
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testCreateuser1,ou=groups,o=novell	Entity Updated
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testCreateuser11,ou=idmsample,o=novell	Entity Updated
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testCreateuser12,ou=idmsample,o=novell	Entity Updated
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testuserfeelfreetodelete,ou=idmsample,o=novell	Entity Updated
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testuserfeelfreetodelete1,ou=idmsample,o=novell	Entity Updated
12/11/2006 7:20:51AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=testuserfeelfreetodelete2,ou=idmsample,o=novell	Entity Updated
12/11/2006 7:20:52AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=aa,ou=idmsample,o=novell	Entity Deleted
12/11/2006 7:20:52AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=bb,ou=idmsample,o=novell	Entity Deleted
12/11/2006 7:20:52AM	cn=mjeck,ou=users,ou=idmsample,o=novell	cn=test_chinese,ou=idmsample,o=novell	Entity Deleted

Confidential 12/15/2006 3:42:35PM

Novell. Sentinel

Version : SENTINEL_6.0.0.0_1

1

SQL Server Report - Crystal Enterprise 11

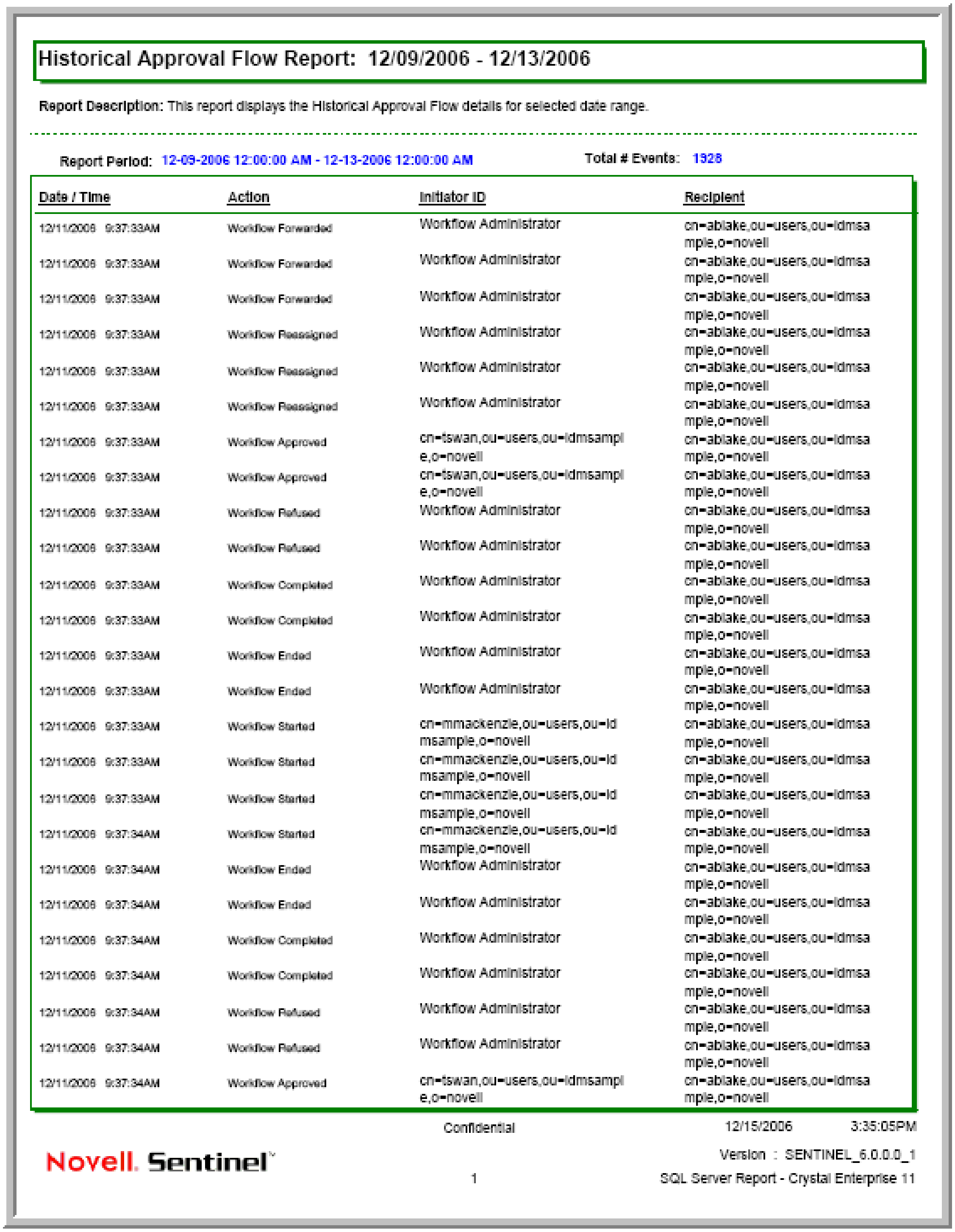
B.2.2 Historical Approval Flow Report

The Historical Approval Report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

Table B-10 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-10** Historical Approval Flow Report*



Historical Approval Flow Report: 12/09/2006 - 12/13/2006

Report Description: This report displays the Historical Approval Flow details for selected date range.

Report Period: 12-09-2006 12:00:00 AM - 12-13-2006 12:00:00 AM **Total # Events:** 1928

Date / Time	Action	Initiator ID	Recipient
12/11/2006 9:37:33AM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Reassigned	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Reassigned	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Reassigned	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Refused	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Refused	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Completed	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Completed	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:33AM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:34AM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:34AM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:34AM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:34AM	Workflow Completed	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:34AM	Workflow Completed	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:34AM	Workflow Refused	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:34AM	Workflow Refused	Workflow Administrator	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:34AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell

Confidential 12/15/2006 3:35:05PM

Novell. Sentinel

Version : SENTINEL_6.0.0.0_1

1 SQL Server Report - Crystal Enterprise 11

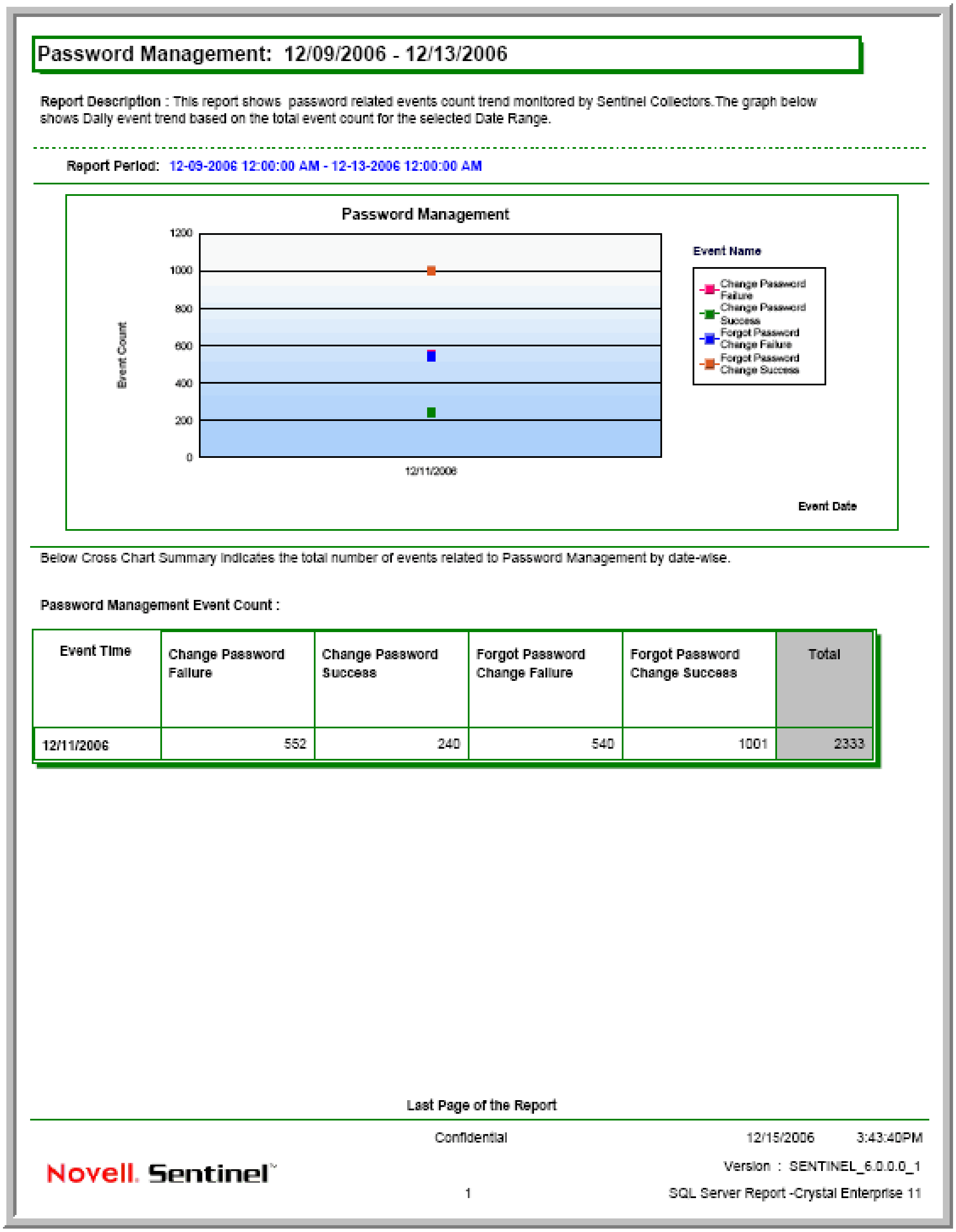
B.2.3 Password Management Report

The Password Management Report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

Table B-11 Password Management Events

Event ID	Description	Trigger
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-11 Password Management Report



Password Management: 12/09/2006 - 12/13/2006

Report Description : This report shows password related events count trend monitored by Sentinel Collectors.The graph below shows Daily event trend based on the total event count for the selected Date Range.

Report Period: 12-09-2006 12:00:00 AM - 12-13-2006 12:00:00 AM

Below Cross Chart Summary indicates the total number of events related to Password Management by date-wise.

Password Management Event Count :

Event Time	Change Password Failure	Change Password Success	Forgot Password Change Failure	Forgot Password Change Success	Total
12/11/2006	552	240	540	1001	2333

Last Page of the Report

Confidential 12/15/2006 3:43:40PM

Novell. Sentinel™ Version : SENTINEL_6.0.0.0_1

1 SQL Server Report -Crystal Enterprise 11

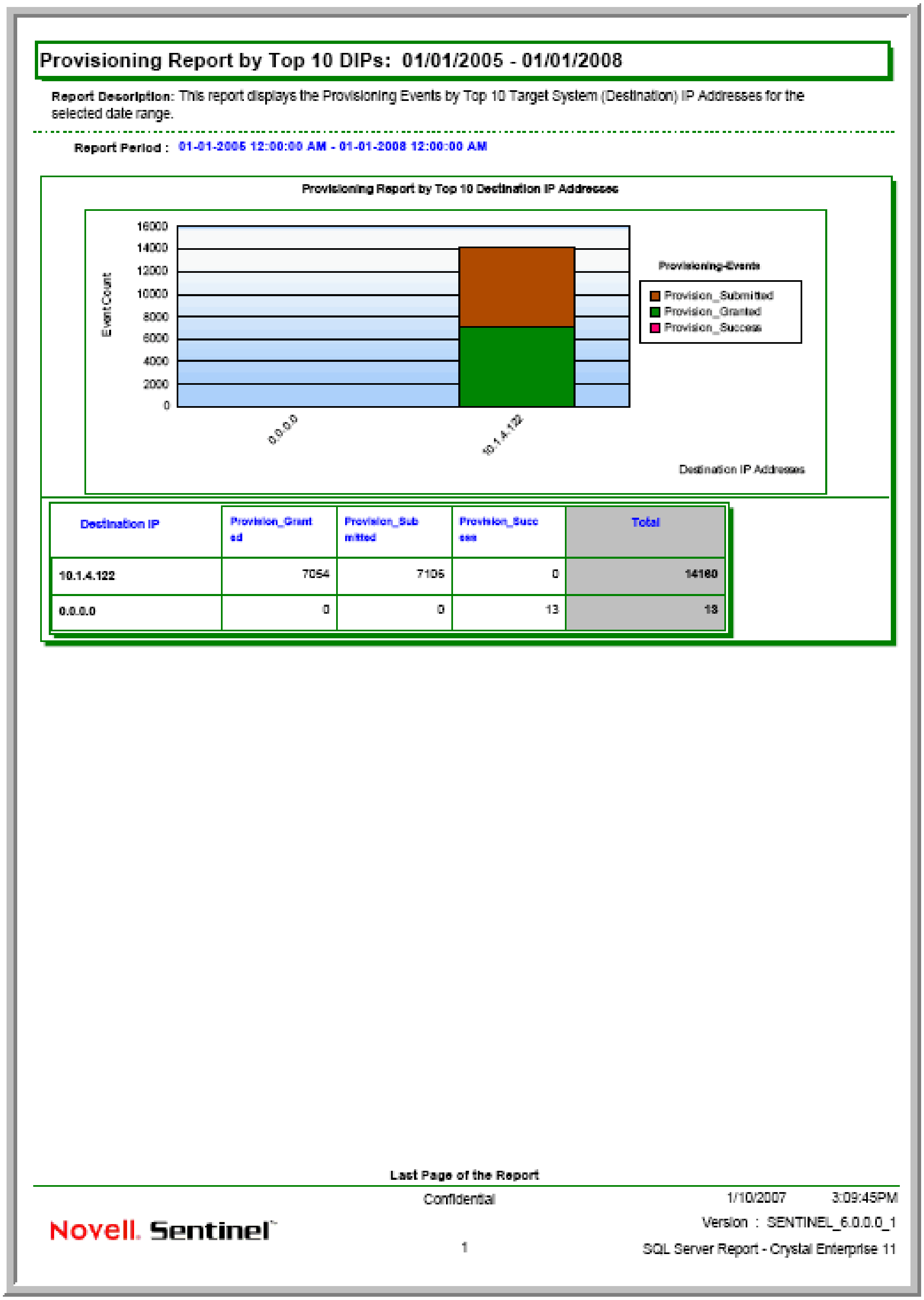
B.2.4 Provisioning Report by Top 10 DIPs

The Provisioning Report by Top 10 DIPs is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

Table B-12 Provisioning Events

Event ID	Description	Trigger
3152D	Provision_Error	Occurs when there is an error in the provisioning step.
3152E	Provision_Submitted	Occurs during the provisioning step on submission of entitlements.
3152F	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.

Figure B-12 *Provisioning Report by Top 10 DIPs*



Provisioning Report by Top 10 DIPs: 01/01/2005 - 01/01/2008

Report Description: This report displays the Provisioning Events by Top 10 Target System (Destination) IP Addresses for the selected date range.

Report Period : 01-01-2005 12:00:00 AM - 01-01-2008 12:00:00 AM

Provisioning Report by Top 10 Destination IP Addresses

Destination IP	Provision_Grant ed	Provision_Sub mitted	Provision_Succ ess	Total
10.1.4.122	7054	7106	0	14160
0.0.0.0	0	0	13	13

Last Page of the Report

Confidential 1/10/2007 3:09:45PM

Novell. Sentinel Version : SENTINEL_6.0.0.0_1

1 SQL Server Report - Crystal Enterprise 11

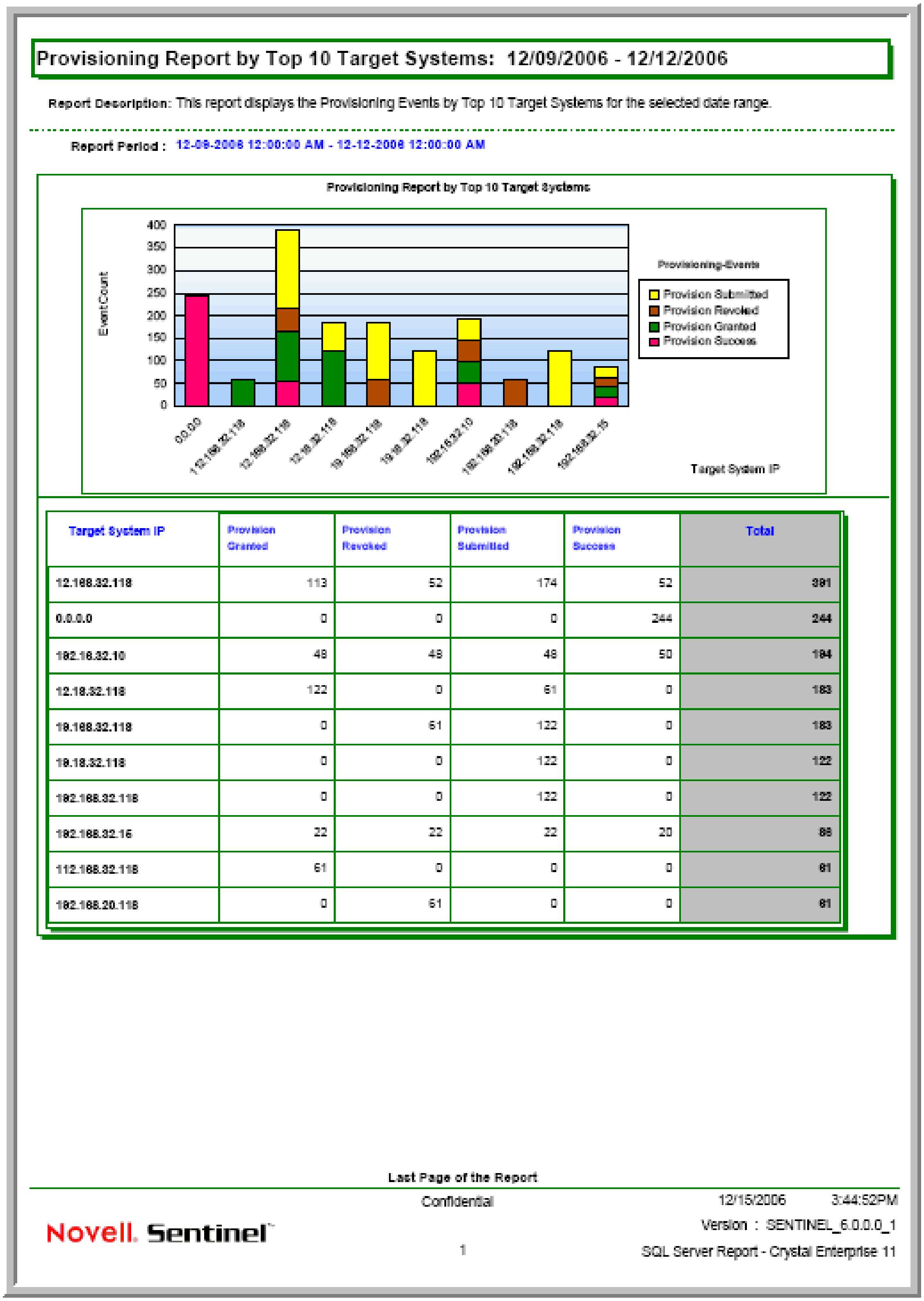
B.2.5 Provisioning Report by Top 10 Target Systems

The Provisioning Report by Top 10 Target Systems is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

Table B-13 *Provisioning Events*

Event ID	Description	Trigger
3152D	Provision_Error	Occurs when there is an error in the provisioning step.
3152E	Provision_Submitted	Occurs during the provisioning step on submission of entitlements.
3152F	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.

Figure B-13 Provisioning Report by Top 10 Target Systems



Provisioning Report by Top 10 Target Systems: 12/09/2006 - 12/12/2006

Report Description: This report displays the Provisioning Events by Top 10 Target Systems for the selected date range.

Report Period : 12-09-2006 12:00:00 AM - 12-12-2006 12:00:00 AM

Provisioning Report by Top 10 Target Systems

Target System IP	Provision Granted	Provision Revoked	Provision Submitted	Provision Success	Total
12.168.32.118	113	52	174	52	391
0.0.0.0	0	0	0	244	244
192.16.32.10	48	48	48	50	194
12.16.32.118	122	0	61	0	183
19.168.32.118	0	61	122	0	183
19.16.32.118	0	0	122	0	122
192.168.32.118	0	0	122	0	122
192.168.32.16	22	22	22	20	86
112.168.32.118	61	0	0	0	61
192.168.20.118	0	61	0	0	61

Last Page of the Report

Confidential

12/15/2006 3:44:52PM

Version : SENTINEL_6.0.0.0_1

Novell. Sentinel™

1

SQL Server Report - Crystal Enterprise 11

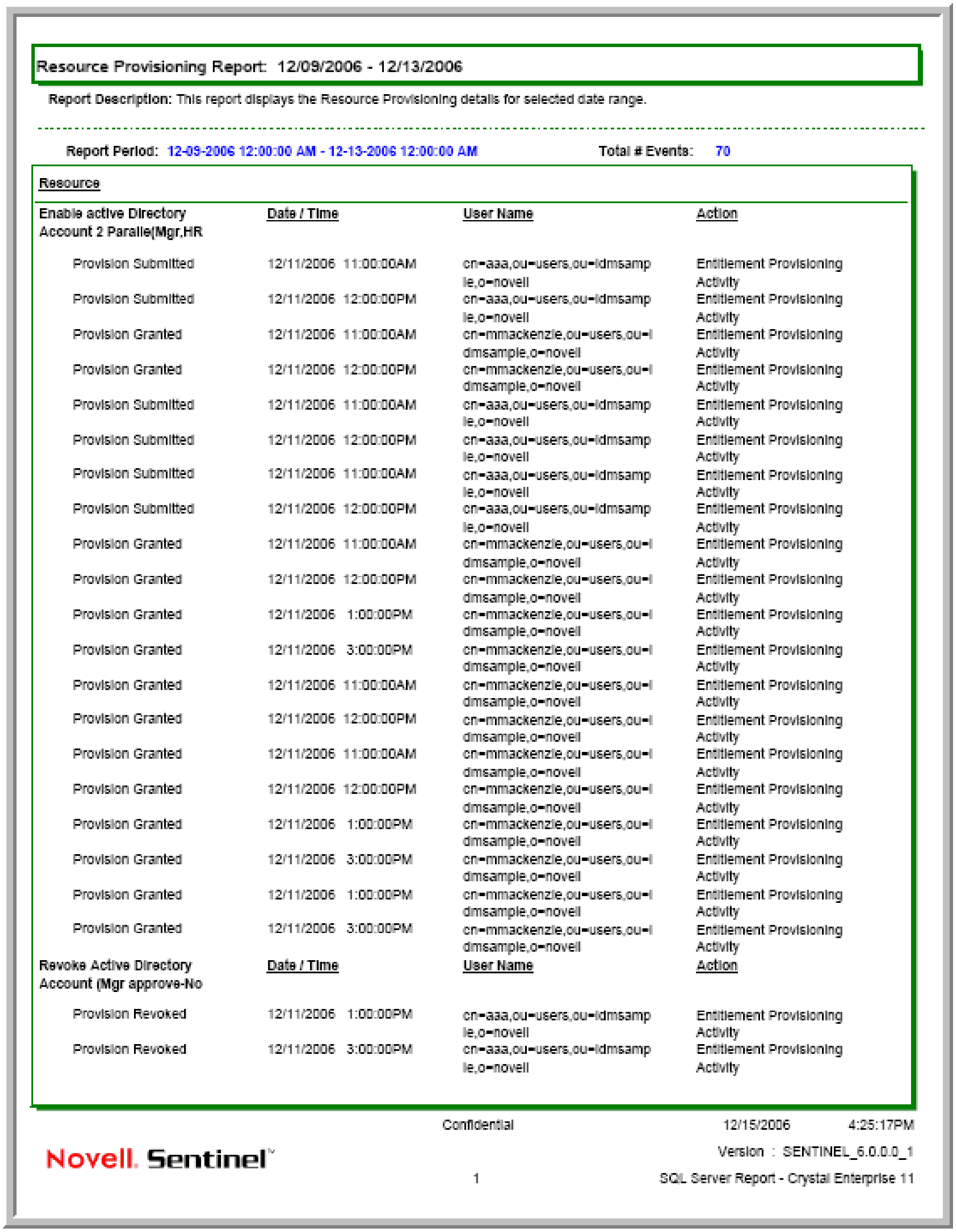
B.2.6 Resource Provisioning Report

The Resource Provisioning Report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

Table B-14 *Provisioning Events*

Event ID	Description	Trigger
3152D	Provision_Error	Occurs when there is an error in the provisioning step.
3152E	Provision_Submitted	Occurs during the provisioning step on submission of entitlements.
3152F	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.

Figure B-14 Resource Provisioning Report



Resource Provisioning Report: 12/09/2006 - 12/13/2006

Report Description: This report displays the Resource Provisioning details for selected date range.

Report Period: 12-09-2006 12:00:00 AM - 12-13-2006 12:00:00 AM **Total # Events:** 70

Resource

Enable active Directory Account 2 Paralle(Mgr,HR	Date / Time	User Name	Action
Provision Submitted	12/11/2006 11:00:00AM	cn=aaa,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 12:00:00PM	cn=aaa,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 11:00:00AM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 12:00:00PM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 11:00:00AM	cn=aaa,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 12:00:00PM	cn=aaa,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 11:00:00AM	cn=aaa,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 12:00:00PM	cn=aaa,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 11:00:00AM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 12:00:00PM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 1:00:00PM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 3:00:00PM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 11:00:00AM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 12:00:00PM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 11:00:00AM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 12:00:00PM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 1:00:00PM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 3:00:00PM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 1:00:00PM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Granted	12/11/2006 3:00:00PM	cn=mmackenzie,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Revoke Active Directory Account (Mgr approve-No	**Date / Time**	**User Name**	**Action**
Provision Revoked	12/11/2006 1:00:00PM	cn=aaa,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity
Provision Revoked	12/11/2006 3:00:00PM	cn=aaa,ou=users,ou=idmsample,o=novell	Entitlement Provisioning Activity

Confidential 12/15/2006 4:25:17PM

Novell. Sentinel™ Version : SENTINEL_6.0.0.0_1

1 SQL Server Report - Crystal Enterprise 11

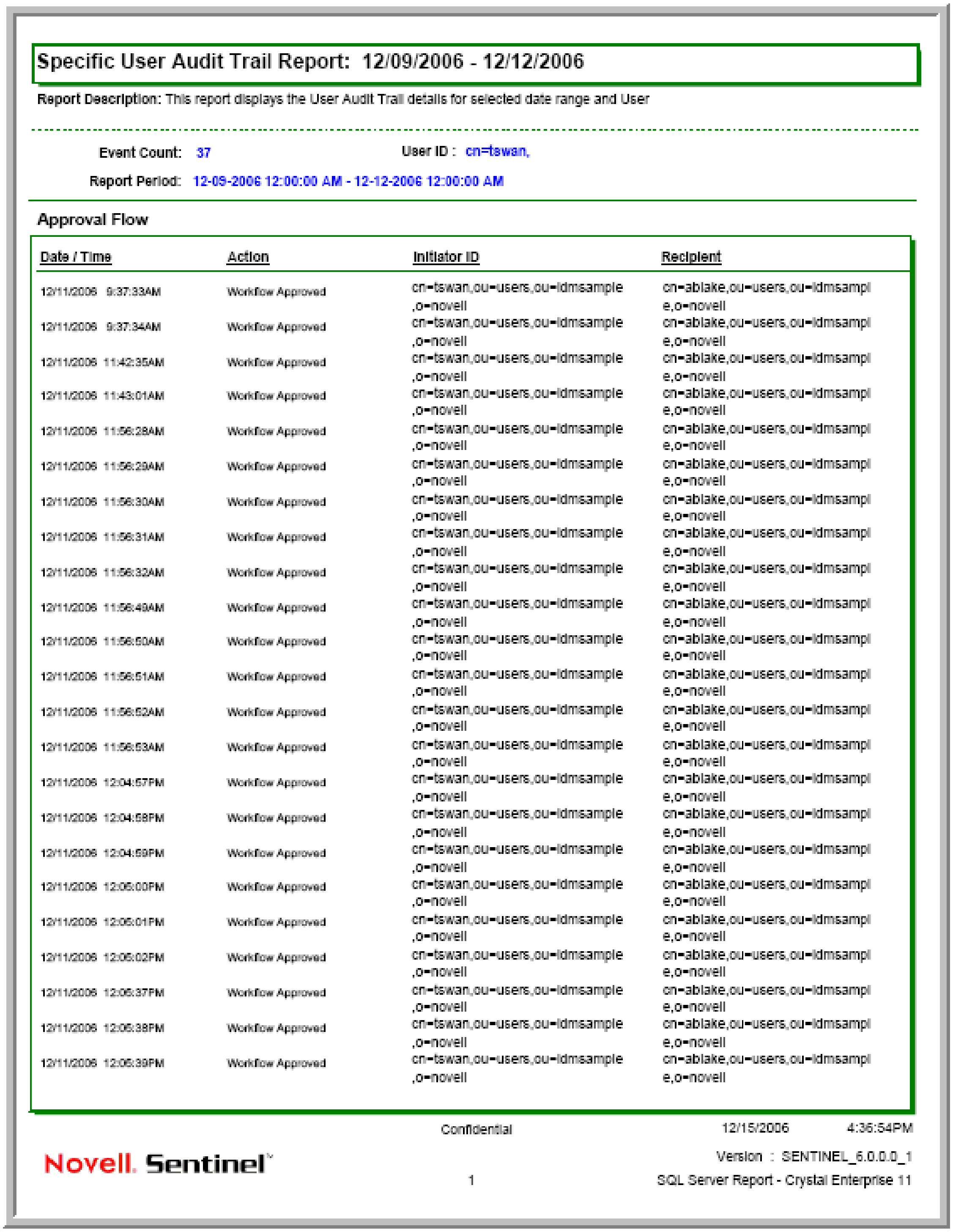
B.2.7 Specific User Audit Trail Report

The Specific User Audit Trail Report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

Table B-15 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-15 *Specific User Audit Trail Report*



Specific User Audit Trail Report: 12/09/2006 - 12/12/2006

Report Description: This report displays the User Audit Trail details for selected date range and User

Event Count: 37

User ID : cn=tswan,

Report Period: 12-09-2006 12:00:00 AM - 12-12-2006 12:00:00 AM

Approval Flow

Date / Time	Action	Initiator ID	Recipient
12/11/2006 9:37:33AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 9:37:34AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:42:35AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:43:01AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:56:28AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:56:29AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:56:30AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:56:31AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:56:32AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:56:49AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:56:50AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:56:51AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:56:52AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 11:56:53AM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 12:04:57PM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 12:04:58PM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 12:04:59PM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 12:06:00PM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 12:06:01PM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 12:06:02PM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 12:06:37PM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 12:06:38PM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell
12/11/2006 12:06:39PM	Workflow Approved	cn=tswan,ou=users,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell

Confidential 12/15/2006 4:36:54PM

Novell. Sentinel™

Version : SENTINEL_6.0.0.0_1

1

SQL Server Report - Crystal Enterprise 11

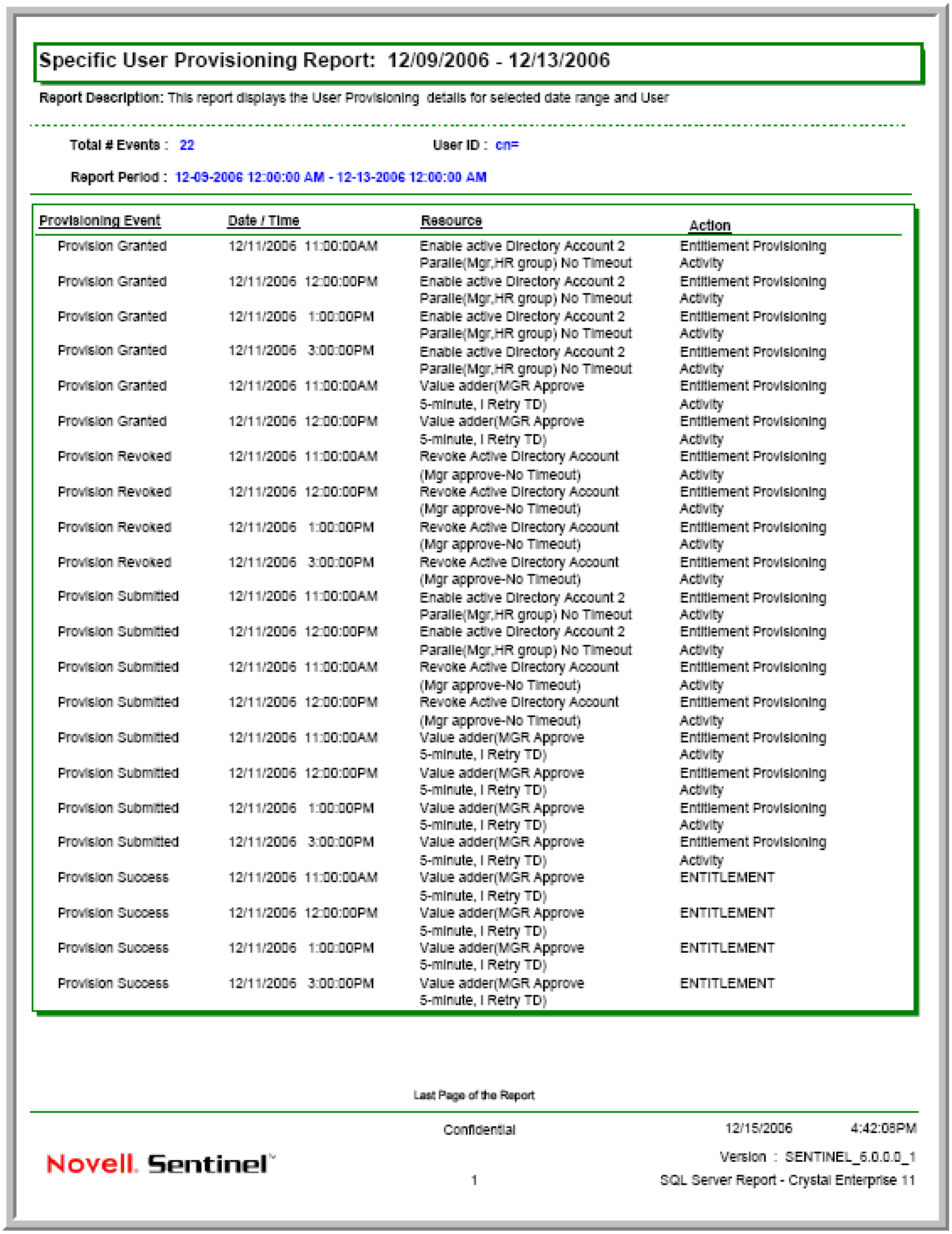
B.2.8 Specific User Provisioning Report

The Specific User Provisioning Report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

Table B-16 *Provisioning Events*

Event ID	Description	Trigger
3152D	Provision_Error	Occurs when there is an error in the provisioning step.
3152E	Provision_Submitted	Occurs during the provisioning step on submission of entitlements.
3152F	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.

Figure B-16 Specific User Provisioning Report



Specific User Provisioning Report: 12/09/2006 - 12/13/2006

Report Description: This report displays the User Provisioning details for selected date range and User

Total # Events : 22 User ID : cn=

Report Period : 12-09-2006 12:00:00 AM - 12-13-2006 12:00:00 AM

Provisioning Event	Date / Time	Resource	Action
Provision Granted	12/11/2006 11:00:00AM	Enable active Directory Account 2 Paralle(Mgr,HR group) No Timeout	Entitlement Provisioning Activity
Provision Granted	12/11/2006 12:00:00PM	Enable active Directory Account 2 Paralle(Mgr,HR group) No Timeout	Entitlement Provisioning Activity
Provision Granted	12/11/2006 1:00:00PM	Enable active Directory Account 2 Paralle(Mgr,HR group) No Timeout	Entitlement Provisioning Activity
Provision Granted	12/11/2006 3:00:00PM	Enable active Directory Account 2 Paralle(Mgr,HR group) No Timeout	Entitlement Provisioning Activity
Provision Granted	12/11/2006 11:00:00AM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
Provision Granted	12/11/2006 12:00:00PM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
Provision Revoked	12/11/2006 11:00:00AM	Revoke Active Directory Account (Mgr approve-No Timeout)	Entitlement Provisioning Activity
Provision Revoked	12/11/2006 12:00:00PM	Revoke Active Directory Account (Mgr approve-No Timeout)	Entitlement Provisioning Activity
Provision Revoked	12/11/2006 1:00:00PM	Revoke Active Directory Account (Mgr approve-No Timeout)	Entitlement Provisioning Activity
Provision Revoked	12/11/2006 3:00:00PM	Revoke Active Directory Account (Mgr approve-No Timeout)	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 11:00:00AM	Enable active Directory Account 2 Paralle(Mgr,HR group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 12:00:00PM	Enable active Directory Account 2 Paralle(Mgr,HR group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 11:00:00AM	Revoke Active Directory Account (Mgr approve-No Timeout)	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 12:00:00PM	Revoke Active Directory Account (Mgr approve-No Timeout)	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 11:00:00AM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 12:00:00PM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 1:00:00PM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 3:00:00PM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
Provision Success	12/11/2006 11:00:00AM	Value adder(MGR Approve 5-minute, I Retry TD)	ENTITLEMENT
Provision Success	12/11/2006 12:00:00PM	Value adder(MGR Approve 5-minute, I Retry TD)	ENTITLEMENT
Provision Success	12/11/2006 1:00:00PM	Value adder(MGR Approve 5-minute, I Retry TD)	ENTITLEMENT
Provision Success	12/11/2006 3:00:00PM	Value adder(MGR Approve 5-minute, I Retry TD)	ENTITLEMENT

Last Page of the Report

Confidential 12/15/2006 4:42:08PM

Novell. Sentinel™ Version : SENTINEL_6.0.0.0_1

1 SQL Server Report - Crystal Enterprise 11

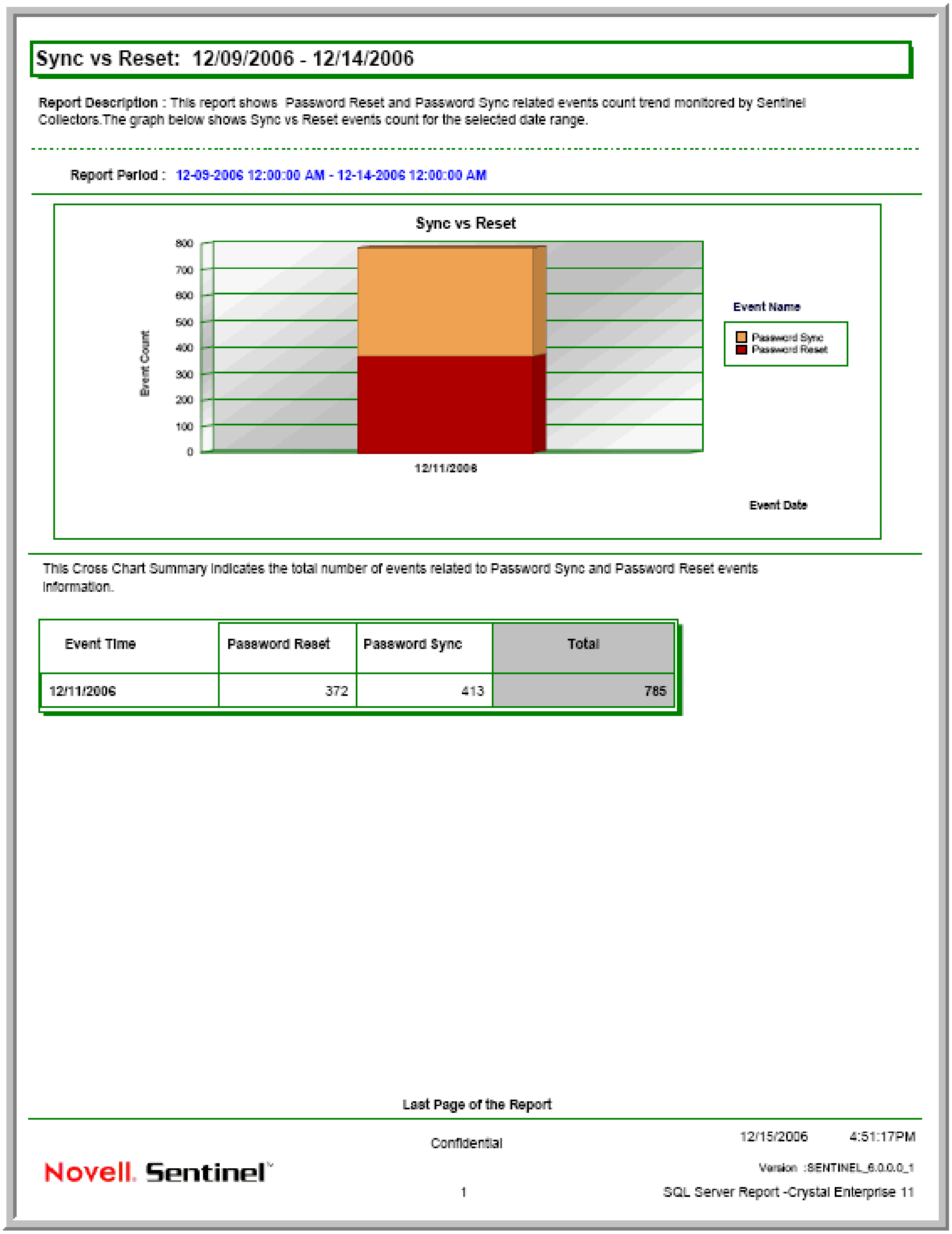
B.2.9 Sync vs. Reset Report

The Sync vs. Reset Report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

Table B-17 Provisioning Events

Event ID	Description	Trigger
30024	Password Sync	Generated when setting the distribution or simple password on an object.
30025	Password Reset	Generated when resetting the connected application password after a failed password sync operation.

Figure B-17 Sync vs. Reset Report



Sync vs Reset: 12/09/2006 - 12/14/2006

Report Description : This report shows Password Reset and Password Sync related events count trend monitored by Sentinel Collectors.The graph below shows Sync vs Reset events count for the selected date range.

Report Period : 12-09-2006 12:00:00 AM - 12-14-2006 12:00:00 AM

This Cross Chart Summary indicates the total number of events related to Password Sync and Password Reset events information.

Event Time	Password Reset	Password Sync	Total
12/11/2006	372	413	785

Last Page of the Report

Novell. Sentinel

Confidential

1

12/15/2006 4:51:17PM

Version :SENTINEL_6.0.0.0_1

SQL Server Report -Crystal Enterprise 11

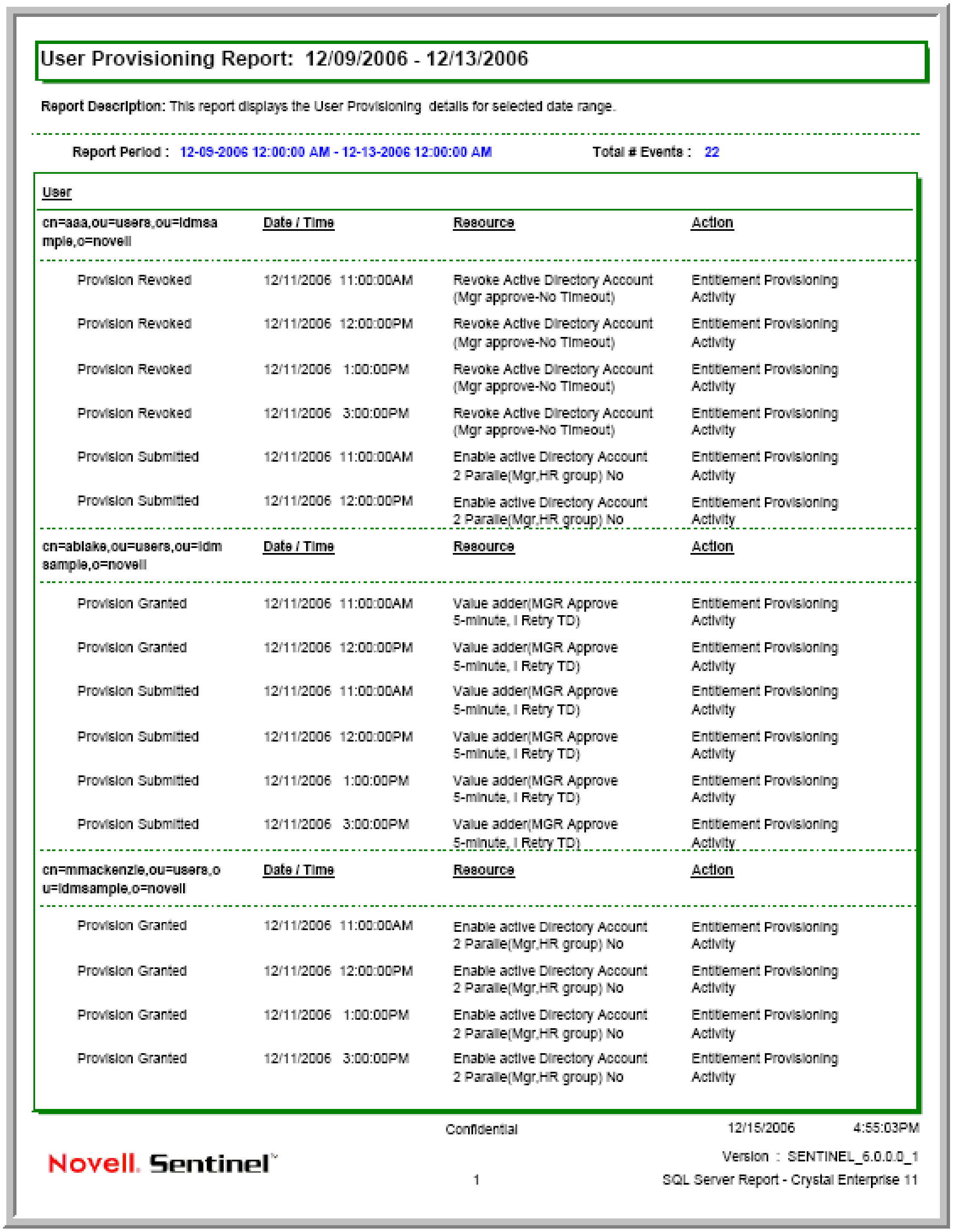
B.2.10 User Provisioning Report

The User Provisioning Report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

Table B-18 *Provisioning Events*

Event ID	Description	Trigger
3152D	Provision_Error	Occurs when there is an error in the provisioning step.
3152E	Provision_Submitted	Occurs during the provisioning step on submission of entitlements.
3152F	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.

Figure B-18 *User Provisioning Report*



User Provisioning Report: 12/09/2006 - 12/13/2006

Report Description: This report displays the User Provisioning details for selected date range.

Report Period : 12-09-2006 12:00:00 AM - 12-13-2006 12:00:00 AM   **Total # Events :** 22

User			
cn=aaa,ou=users,ou=idmsample,o=novell	Date / Time	Resource	Action
Provision Revoked	12/11/2006 11:00:00AM	Revoke Active Directory Account (Mgr approve-No Timeout)	Entitlement Provisioning Activity
Provision Revoked	12/11/2006 12:00:00PM	Revoke Active Directory Account (Mgr approve-No Timeout)	Entitlement Provisioning Activity
Provision Revoked	12/11/2006 1:00:00PM	Revoke Active Directory Account (Mgr approve-No Timeout)	Entitlement Provisioning Activity
Provision Revoked	12/11/2006 3:00:00PM	Revoke Active Directory Account (Mgr approve-No Timeout)	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 11:00:00AM	Enable active Directory Account 2 Paralle(Mgr,HR group) No	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 12:00:00PM	Enable active Directory Account 2 Paralle(Mgr,HR group) No	Entitlement Provisioning Activity
cn=ablake,ou=users,ou=idmsample,o=novell	Date / Time	Resource	Action
Provision Granted	12/11/2006 11:00:00AM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
Provision Granted	12/11/2006 12:00:00PM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 11:00:00AM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 12:00:00PM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 1:00:00PM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
Provision Submitted	12/11/2006 3:00:00PM	Value adder(MGR Approve 5-minute, I Retry TD)	Entitlement Provisioning Activity
cn=mmackenzie,ou=users,ou=idmsample,o=novell	Date / Time	Resource	Action
Provision Granted	12/11/2006 11:00:00AM	Enable active Directory Account 2 Paralle(Mgr,HR group) No	Entitlement Provisioning Activity
Provision Granted	12/11/2006 12:00:00PM	Enable active Directory Account 2 Paralle(Mgr,HR group) No	Entitlement Provisioning Activity
Provision Granted	12/11/2006 1:00:00PM	Enable active Directory Account 2 Paralle(Mgr,HR group) No	Entitlement Provisioning Activity
Provision Granted	12/11/2006 3:00:00PM	Enable active Directory Account 2 Paralle(Mgr,HR group) No	Entitlement Provisioning Activity

Confidential   12/15/2006   4:55:03PM

Novell. Sentinel   Version : SENTINEL_6.0.0.0_1

1   SQL Server Report - Crystal Enterprise 11

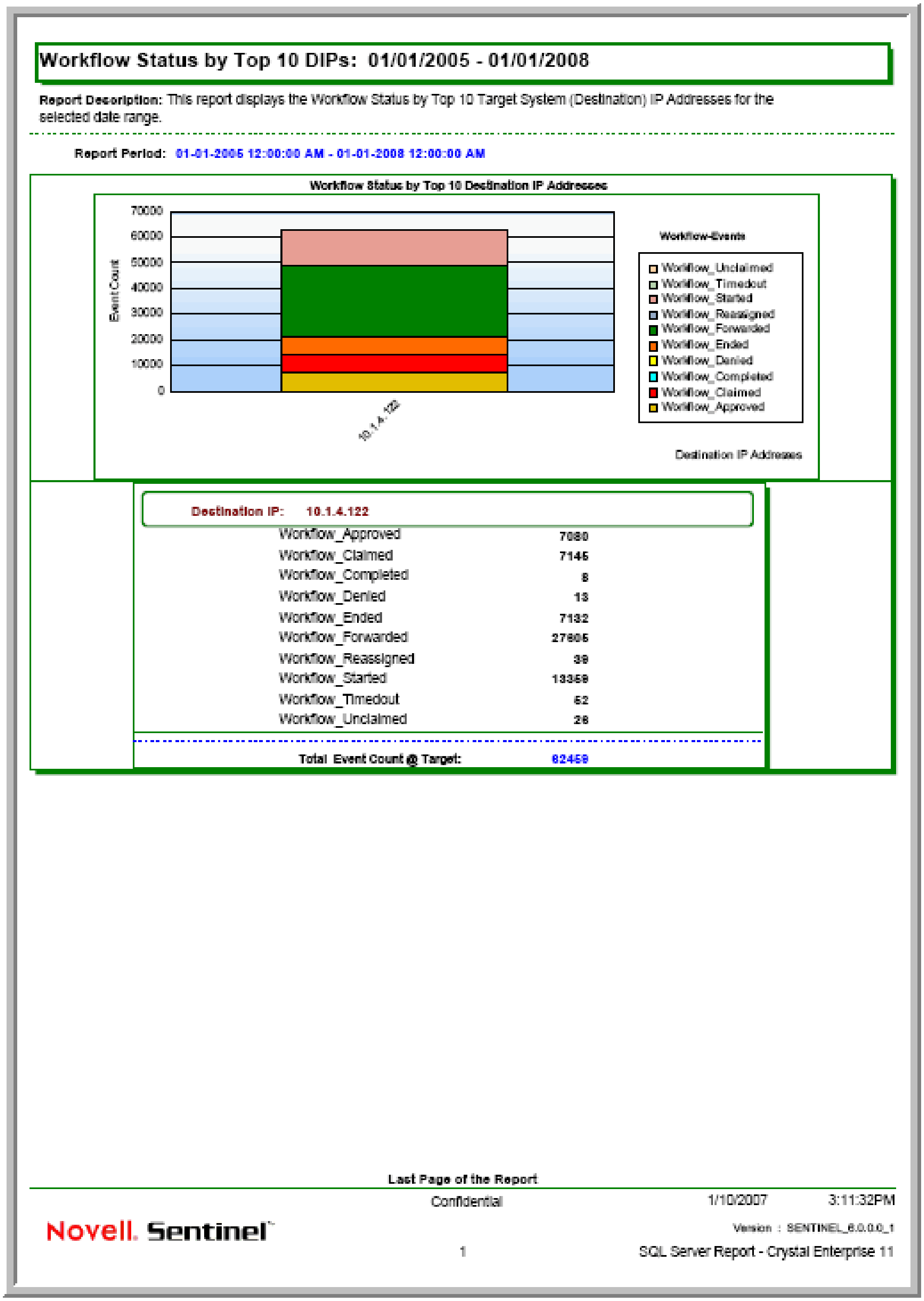
B.2.11 Workflow Status by Top Ten DIPs Report

The Workflow Status by Top Ten DIPs report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

Table B-19 Workflow Status 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-19 *Workflow Status by Top Ten DIPs Report*



Workflow Status by Top 10 DIPs: 01/01/2005 - 01/01/2008

Report Description: This report displays the Workflow Status by Top 10 Target System (Destination) IP Addresses for the selected date range.

Report Period: **01-01-2005 12:00:00 AM - 01-01-2008 12:00:00 AM**

Destination IP: **10.1.4.122**

Workflow_Approved	7080
Workflow_Claimed	7145
Workflow_Completed	8
Workflow_Denied	13
Workflow_Ended	7132
Workflow_Forwarded	27605
Workflow_Reassigned	39
Workflow_Started	13359
Workflow_Timedout	52
Workflow_Unclaimed	26
Total Event Count @ Target:	**62459**

Last Page of the Report

Confidential 1/10/2007 3:11:32PM

Novell. Sentinel

Version : SENTINEL_6.0.0.0_1

1

SQL Server Report - Crystal Enterprise 11

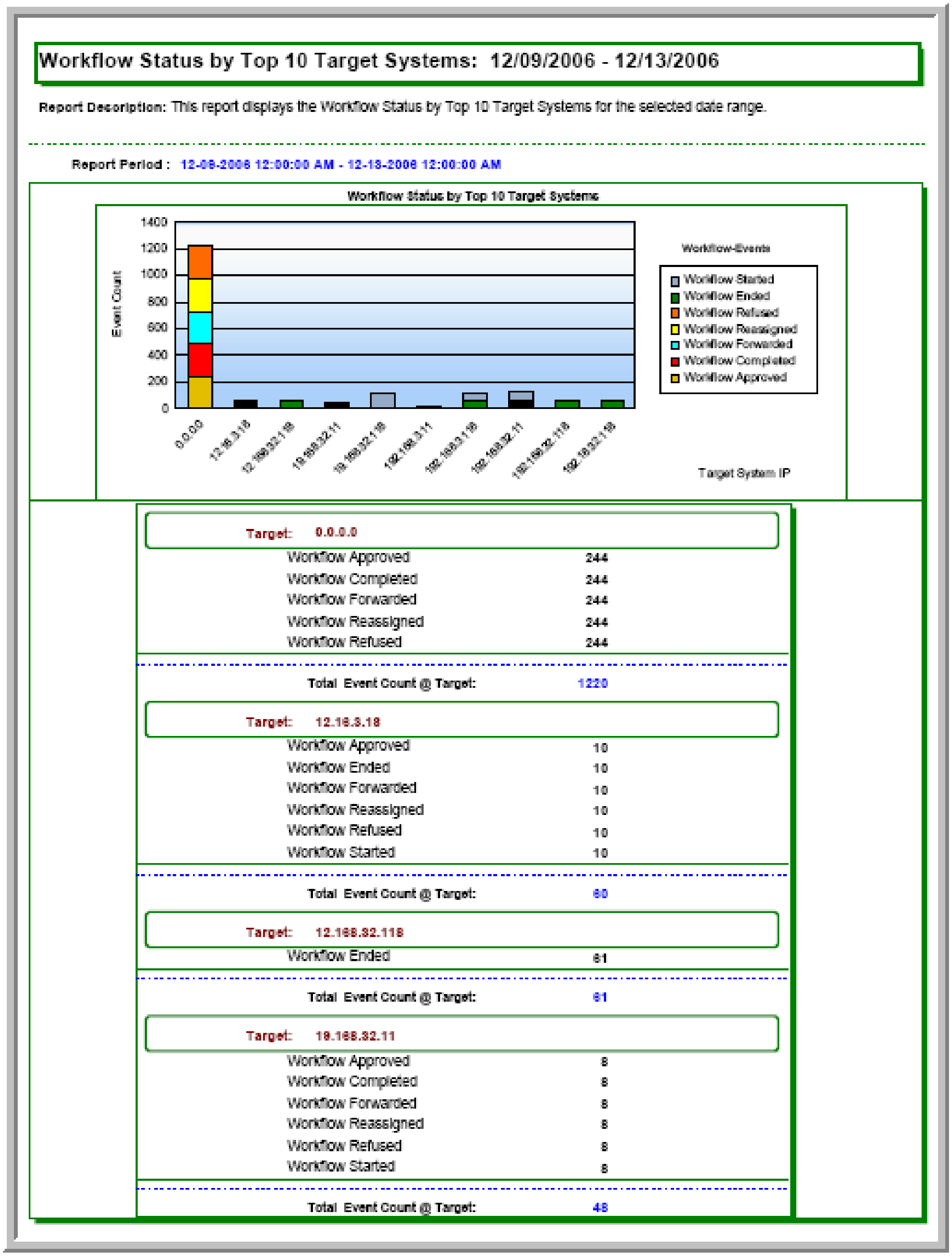
B.2.12 Workflow Status by Top Ten Target Systems Report

The Workflow Status by Top Ten Target Systems report is generated from the events listed in the following table. For more information on each event, see Appendix A, “Identity Manager Events,” on page 45.

***Table B-20** Workflow Status 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-20 *Workflow Status by Top Ten Target Systems Report*



Workflow Status by Top 10 Target Systems: 12/09/2006 - 12/13/2006

Report Description: This report displays the Workflow Status by Top 10 Target Systems for the selected date range.

Report Period : 12-09-2006 12:00:00 AM - 12-13-2006 12:00:00 AM

Target:	**0.0.0.0**
Workflow Approved	244
Workflow Completed	244
Workflow Forwarded	244
Workflow Reassigned	244
Workflow Refused	244
Total Event Count @ Target:	1220

Target:	**12.16.3.18**
Workflow Approved	10
Workflow Ended	10
Workflow Forwarded	10
Workflow Reassigned	10
Workflow Refused	10
Workflow Started	10
Total Event Count @ Target:	60

Target:	**12.168.32.118**
Workflow Ended	61
Total Event Count @ Target:	61

Target:	**19.168.32.11**
Workflow Approved	8
Workflow Completed	8
Workflow Forwarded	8
Workflow Reassigned	8
Workflow Refused	8
Workflow Started	8
Total Event Count @ Target:	48