

# Novell Nsure™ Audit

1.0.3

July 18, 2006

INSTALLATION GUIDE

[www.novell.com](http://www.novell.com)



**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.

You may not use, export, or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2002-2005 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. 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 at <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](http://www.novell.com)

*Online Documentation:* To access the online documentation for this and other Novell products, and to get updates, see [www.novell.com/documentation](http://www.novell.com/documentation).

## **Novell Trademarks**

Novell is a registered trademark of Novell, Inc. in the United States and other countries.  
SUSE is a registered trademark of SUSE AG, a Novell business.

## **Third-Party Materials**

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



# Contents

<b>About This Guide</b>	<b>7</b>
<b>1 Preparing for Installation</b>	<b>9</b>
<b>2 System Requirements and Prerequisites</b>	<b>11</b>
2.1 System Requirements	11
2.1.1 Secure Logging Server	11
2.1.2 Platform Agent	12
2.1.3 eDirectory Instrumentation	12
2.1.4 NetWare Instrumentation	13
2.2 Prerequisites	13
2.2.1 NICI	13
2.2.2 eDirectory	13
2.2.3 iManager	13
<b>3 Configuring the Data Store</b>	<b>15</b>
3.1 File Data Store	16
3.2 MySQL Data Store	17
3.3 Microsoft SQL Server Data Store	18
3.4 Oracle Data Store	19
3.5 Syslog Data Store	20
3.6 JDBC Data Store	20
<b>4 Upgrading Novell Nsure Audit</b>	<b>21</b>
<b>5 Installing and Activating Novell Nsure Audit</b>	<b>23</b>
5.1 Installing Nsure Audit with Open Enterprise Server	23
5.2 Installing Nsure Audit with NetWare 6.5	25
5.3 Installing Nsure Audit on NetWare	26
5.4 Installing Nsure Audit on Linux	28
5.5 Installing Nsure Audit on Solaris	30
5.6 Installing Nsure Audit on Windows	31
5.7 Activating Nsure Audit	32
5.8 Activating Nsure Audit Report	33
<b>6 Installing the Nsure Audit iManager Plug-in</b>	<b>35</b>
6.1 Install or Upgrade the iManager Plug-in	35
6.2 Install or Upgrade the iManager Plug-In in Assigned Mode with Role-Based Services	36
<b>7 Configuring the Secure Logging Server</b>	<b>37</b>
7.1 Configuring the Secure Logging Server	37
7.2 Configuring Multiple Secure Logging Servers	39
7.3 Configuring a Secure Logging Server with More Than One IP Address	39

<b>8</b>	<b>Configuring the Platform Agent and Logging Instrumentations</b>	<b>41</b>
8.1	Installing the Logging Components . . . . .	41
8.2	Configuring the Platform Agent . . . . .	42
8.3	Configuring eDirectory, File System, and NetWare Events . . . . .	43
<b>9</b>	<b>Verifying the Installation</b>	<b>45</b>
9.1	eDirectory Objects . . . . .	45
9.2	Data Store . . . . .	46
9.3	Secure Logging Server . . . . .	46
9.4	Platform Agent and Logging Instrumentations . . . . .	48
9.4.1	Platform Agent . . . . .	48
9.4.2	NetWare and eDirectory Instrumentations . . . . .	49
9.4.3	Nsure Audit Instrumentation . . . . .	51
9.5	Verifying Event Logging . . . . .	52

# About This Guide

Welcome to Novell® Nsure™ Audit. This guide provides the information required to install Nsure Audit.

## Audience

This guide is intended for network administrators.

## Feedback

We want to hear your comments and suggestions about this manual. Please use the Feedback option at the bottom of each page of the Nsure Audit online documentation.

## Documentation Updates

For the most recent version of the Novell Nsure Audit 1.0.3 Installation Guide, see the [Novell Documentation Web site](http://www.novell.com/documentation/lg/nsureaudit/index.html), (<http://www.novell.com/documentation/lg/nsureaudit/index.html>).

## Additional Documentation

For information on installing Novell Nsure Audit, see the *Novell Nsure Audit 1.0.3 Administration Guide*.

## Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items within 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 UNIX\*, should use forward slashes as required by your software.





# Preparing for Installation

# 1

Installing and configuring Novell® Nsure™ Audit is an eight-step process:

- 1 Meet the Nsure Audit prerequisites and requirements. For more information, see [Chapter 2, “System Requirements and Prerequisites,”](#) on page 11.
- 2 Configure MySQL\* or another supported application as the data store. For more information, see [“Configuring the Data Store”](#) on page 15
- 3 Install or update the Secure Logging Server component of Nsure Audit on a single server in your tree. Depending on whether this is a first-time install or an upgrade, see the following:
  - [“Installing and Activating Novell Nsure Audit”](#) on page 23
  - [“Upgrading Novell Nsure Audit”](#) on page 21

If you want to configure multiple Secure Logging Server in the tree, see [Section 7.2, “Configuring Multiple Secure Logging Servers,”](#) on page 39.

- 4 Install or update the Nsure Audit iManager plug-in on your iManager server. For more information, see [“Installing the Nsure Audit iManager Plug-in”](#) on page 35.
- 5 Use the Nsure Audit iManager plug-in to configure your Secure Logging Server. This includes creating the Channel object required to connect to the data store you created in [Step 2](#) as well as any other logging channels or notifications you want to activate on your logging system. For more information, see [“Configuring the Secure Logging Server”](#) on page 37.
- 6 Install and configure the Platform Agent on every server that you want to report events. You must also install the Instrumentation for each logging application that you want to report events. For example, if you have NetWare® and eDirectory™ running on a server, you must install the Platform Agent, the NetWare Instrumentation, and the eDirectory Instrumentation for that server to report NetWare and eDirectory events. For more information, see [Chapter 8, “Configuring the Platform Agent and Logging Instrumentations,”](#) on page 41.
- 7 (Optional) If you are running NetWare or eDirectory, select which events you want to report. For more information, see [“Logging eDirectory, NetWare, and File System Events”](#) in the *Novell Nsure Audit 1.0.3 Administration Guide*.
- 8 Test your installation to ensure that your Nsure Audit environment is set up and functioning correctly. For more information, see [“Verifying the Installation”](#) on page 45.



# System Requirements and Prerequisites

# 2

This section reviews the system requirements and installation procedures for each platform.

- [Section 2.1, “System Requirements,” on page 11](#)
- [Section 2.2, “Prerequisites,” on page 13](#)

For a listing of all the program files, see “[File Descriptions and Locations](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

## 2.1 System Requirements

The following sections outline the system requirements for the Secure Logging Server, Platform Agent, and Novell eDirectory™ and NetWare® Instrumentations.

### 2.1.1 Secure Logging Server

The Secure Logging Server is the server component in the Nsure™ auditing system. It is installed on the server you want to manage the flow of information to and from the auditing system.

The server where you install the Secure Logging Server must meet the following requirements:

Requirement	Description
Operating System	NetWare 6.5 NetWare 6.0 SP3 or later NetWare 5.1 SP6 or later Windows* 2003 Server Windows 2000 SP3 Solaris* 8 and 9 SUSE® Linux* Enterprise Server 8 and 9 RedHat* Linux AS and ES 2.1
eDirectory	Novell eDirectory version 8.5 or higher
Processor	A single processor, server-class PC with a Pentium* II 400 Mhz
Disk Space	At least 40 MB  The space you need for your data store depends on a number of factors which include, but are not limited to, how many events per second you are storing and how long you want to keep the data. For MySQL, a system that generates around 80 events per second with an average event size of 80 bytes consumes approximately 500 MB of disk space for the database table and 150 MB for the index in a 24 hour period.

Requirement	Description
RAM	512 MB

## 2.1.2 Platform Agent

The Platform Agent is the client portion of the Nsure auditing system. It is a shared library that is used by instrumented applications to log events to Novell Nsure Audit. It does not have any system requirements other than disk space for the Disconnected Mode Cache. (eDirectory is not required.)

The Platform Agent must be installed on every server or workstation running applications that log events to Nsure Audit. The Platform Agent supports the following platforms:

- NetWare 4.2 or later
- Windows NT, Windows 2000 and Windows 2000 Server, Window XP, Windows 2003 Server.
- SUSE Linux Enterprise Server 8 and 9
- Solaris 8 and 9
- RedHat Linux 7.3, 8, AS, and ES 2.1

## 2.1.3 eDirectory Instrumentation

The eDirectory Instrumentation enables Nsure Audit to log eDirectory events. To avoid receiving duplicate entries for eDirectory events, enable the do not sent replicated events option. To enable this, open the Nsure Audit tab of your NCP Server object and check the “Do not send replicated events” checkbox. To log non-replicated events (such as logins), it must be installed on each individual server for which you want to log non-replicated events.

eDirectory Instrumentation also requires that the Platform Agent be installed on the same machine.

The eDirectory Instrumentation supports the following versions of the Directory:

- NDS<sup>®</sup> 6.x
- NDS 7.x
- NDS 8.x
- eDirectory 8.6 (NetWare, Windows, Linux, and Solaris)
- eDirectory 8.7 (NetWare, Windows, Linux, and Solaris)

## 2.1.4 NetWare Instrumentation

The NetWare Instrumentation allows Nsure Audit to log NetWare and file system events. It must be loaded on every server for which you want to log NetWare and file system events. It also requires that the Platform Agent be installed on the same machine.

The NetWare Instrumentation supports the following versions of NetWare:

- NetWare 4.2 SP9 or later
- NetWare 5.1 SP6 or later
- NetWare 6.0 SP3 or later
- NetWare 6.5

## 2.2 Prerequisites

The following must be set up to use Novell Nsure Audit:

- [Section 2.2.1, “NICI,” on page 13](#)
- [Section 2.2.2, “eDirectory,” on page 13](#)
- [Section 2.2.3, “iManager,” on page 13](#)

### 2.2.1 NICI

Any NetWare server that reports eDirectory events must be updated with the NICI 2.6.5 or later. This update is available at [download.novell.com](http://download.novell.com).

### 2.2.2 eDirectory

eDirectory 8.7 must be installed and configured in your environment. Nsure Audit uses eDirectory to store product configuration, and requires eDirectory schema extensions specific to Nsure Audit.

Make sure the tree is synchronized and error free. For detailed information on eDirectory Health Check procedures, see [“Keeping eDirectory Healthy” in the \*eDirectory 8.7 Administration Guide\* \(<http://www.novell.com/documentation/lg/edir87/edir87/data/a5ziqam.html>\)](#).

To extend the schema and create the necessary objects, you must have Admin rights to the root of the tree where you plan to install Nsure Audit. You must provide the administrator username and password during installation so the installation program can extend the schema.

### 2.2.3 iManager

Nsure Audit is configured using the Nsure Audit iManager plug-in, which requires iManager 2.5.



# Configuring the Data Store

# 3

Using its available channel drivers, Novell® Nsure™ Audit can log events to the following applications and interfaces:

- Flat file in the file system
- MySQL database
- Oracle\* database
- Microsoft\* SQL Server database
- Java\*
- JDBC\*
- JMS
- SNMP
- SMTP
- Syslog database

Before selecting a storage device for your data store, you need to consider your system's logging traffic. On the high end, the File driver can process over 30,000 events per second on a P4 Xeon\* class server. Databases, on the other hand, are, much slower (the MySQL driver can handle about 5,000 events per second on a P4 Xeon class server); however, they provide advanced querying and reporting.

Nsure Audit is designed to handle occasional peaks that exceed a given database's limitations; however, if you expect to consistently exceed the database driver's capacity, you must plan your setup accordingly, either by using multiple Secure Logging Servers or by using the File driver. For information on configuring multiple logging servers, see [Section 7.2, "Configuring Multiple Secure Logging Servers," on page 39](#).

---

**IMPORTANT:** In planning your system setup, you should perform your own throughput test in your environment and not rely solely on the numbers provided in this document.

---

After configuring a Nsure Audit data store, you must create a Channel object. Each Channel object defines the parameters associated with its corresponding storage device. For example, MySQL Channel objects include the IP address or host name of the MySQL database server, a username and password for connecting with the server, the database and table names, and fields for SQL table create and expiration commands. For more information on creating and configuring Channel objects, see ["Configuring System Channels"](#) in the *Novell Nsure Audit 1.0.3 Administration Guide*.

After creating the Channel object, you must configure the logging server to log events to that channel. The Log Driver property in the Logging Server object determines which Channel object the server uses to create the data store. For more information on the Log Driver property, see ["Configuring the Secure Logging Server"](#) in the *Novell Nsure Audit 1.0.3 Administration Guide*.

After the Channel and Logging Server objects are configured, you must restart the logging server to load the Channel object configuration and the channel driver. In most cases, the channel driver automatically creates the necessary file or database table for the data store.

---

**IMPORTANT:** Nsure Audit does not secure the data store. Therefore, you must manage data store security at the database for MySQL and Oracle data stores, or through the file system for file data stores.

---

The data store structure for common storage devices is discussed in the following sections:

- [Section 3.1, “File Data Store,” on page 16](#)
- [Section 3.2, “MySQL Data Store,” on page 17](#)
- [Section 3.3, “Microsoft SQL Server Data Store,” on page 18](#)
- [Section 3.4, “Oracle Data Store,” on page 19](#)
- [Section 3.5, “Syslog Data Store,” on page 20](#)
- [Section 3.6, “JDBC Data Store,” on page 20](#)

## 3.1 File Data Store

Depending on the File Channel object configuration, the File channel driver (`lgdfile`) can log events in raw format, or it can translate the event data into a human-readable log. By default, file data stores are named `auditlog; however;` however, you can specify the log filename in the File Channel object configuration.

Raw files simply contain the event data; consequently, they are not in a human-readable format. However, because they maintain a consistent field structure across events, they can be imported into spreadsheet programs like Microsoft Excel.

The following is a sample from a raw log file:

```
16777343,1051924636,1051924647,eDirInst\Object,721699,7,0,.OntarioTest
Data.Channels.Logging
Services,,0,0,0,LlNhdHVybiBMb2dnaW5nIFNlcnZlci5Mb2dnaW5nIFNlcnZpY2Vz
16777343,1051924636,1051924647,eDirInst\Object,721690,7,0,.eDirectoryI
nstrumentation.Applications.Logging
Services,,0,0,0,LlNhdHVybiBMb2dnaW5nIFNlcnZlci5Mb2dnaW5nIFNlcnZpY2Vz
16777343,1051926065,1051926065,eDirInst\Object,720897,7,0,.BillBob.SIM
,,0,0,1,LmFkbWluLlNJTQ=
```

---

**NOTE:** Nsure Audit includes a utility, called `LETrans`, that can translate raw log files into human-readable format. See “[LETrans](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

---

Translated log files, on the other hand, can be visually scanned for content; however, it is difficult to generate reports from these files because there is no consistent field structure—they contain only the event descriptions.

The following is a sample from a translated log file:

```
[Sat, 03 May 2003 01:25:10 +0000] eDirInst\Object: A read operation was
performed on object .OntarioTestData.Channels.Logging Services by
.Saturn Logging Server.Logging Services
[Sat, 03 May 2003 01:25:10 +0000] eDirInst\Object: A list Subordinate
Entires operation has been performed on container .eDirectory
Instrumentation.Applications.Logging Services by .Saturn Logging
Server.Logging Services
```



[Sat, 03 May 2003 01:39:41 +0000] eDirInst\Object: A new eDirectory object called .BillBob.SIM (Class:User) was created by .admin.SIM

In addition to providing different log formats, the File channel is capable of creating localized logs. If the logging applications have localized Log Schema (LSC) files, the File channel can write translated log files in the language designated in the File Channel object.

---

**NOTE:** LSC files catalog the events that can be logged for a given application. They can also indicate what kind of data is stored in the event fields and provide descriptive information on the event itself. For more information, see “[Log Schema Files](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

---

For more information on the File channel, see “[File](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

## 3.2 MySQL Data Store

When the logging server loads the MySQL Channel object configuration, the MySQL channel driver, `lgdmsql`, automatically creates the data store’s table using the following table structure:

Field	Type	Null	Key	Default	Extra
SourceIP	int(11)	YES			
ClientTimestamp	int(11)	YES	MUL		
ClientMS	int(11)	YES			
ServerTimestamp	int(11)	YES			
SessionID	int(11)	YES			
Component	varchar(255)	YES			
EventID	int(11)	YES	MUL		
Severity	int(11)	YES			
Grouping	int(11)	YES			
Originator	varchar(255)	YES			
OriginatorType	int(11)	YES			
Target	varchar(255)	YES			
TargetType	int(11)	YES			
SubTarget	varchar(255)	YES			
Text1	varchar(255)	YES			
Text2	varchar(255)	YES			
Text3	varchar(255)	YES			
Value1	int(11)	YES			
Value2	int(11)	YES			
Value3	int(11)	YES			
MIMEType	int(11)	YES			
DataSize	int(11)	YES			
Data	mediumblob	YES			
Signature	varchar(255)	YES			

The table name is defined in the MySQL Channel object configuration page. The default table name is NAUDITLOG.

The MySQL Channel uses MyIsam as its database engine; therefore, the default maximum table size using MySQL 4.1 is 4 GB. MySQL 5.0 limits table sizes to 65,536 TB. Table size may be further constrained by the maximum file size your operating system can manage.

---

**IMPORTANT:** If the SQL server data volume runs out of disk space, any clients logging events will freeze and need to be restarted.

---

If you need larger tables, use the `max_rows` and `avg_row_length` commands in the MySQL Channel object's Create Table Options property.

For more information on the MySQL channel, see “[MySQL](#)” and “[Using MySQL with Nsure Audit](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

### 3.3 Microsoft SQL Server Data Store

When the SQL Server Channel object configuration is loaded in the logging server's memory, the SQL Server channel driver, `lgdmsql`, automatically creates the following table structure for the SQL Server data store:

Column Name	Data Type	Length	Allow Nulls
SourceIP	int	4	✓
ClientTimeStamp	int	4	✓
ClientMS	int	4	✓
ServerTimeStamp	int	4	✓
SessionID	int	4	✓
Component	varchar	255	✓
EventID	int	4	✓
Severity	int	4	✓
Grouping	int	4	✓
Originator	varchar	255	✓
OriginatorType	int	4	✓
Target	varchar	255	✓
TargetType	int	4	✓
SubTarget	varchar	255	✓
Text1	varchar	255	✓
Text2	varchar	255	✓
Text3	varchar	255	✓
Value1	int	4	✓
Value2	int	4	✓
Value3	int	4	✓
MIMEType	int	4	✓
DataSize	int	4	✓
Data	image	16	✓
Signature	varchar	255	✓

The table name is defined in the Microsoft SQL Channel object configuration page. The default table name is `NAUDITLOG`.

For more information on the Microsoft SQL Server channel, see “[Microsoft SQL Server](#)” and “[Using Microsoft SQL Server with Nsure Audit](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

## 3.4 Oracle Data Store

When the Oracle Channel object configuration is loaded in the logging server's memory, the Oracle channel driver, `lgdora`, automatically creates the following table structure for the Oracle data store:

Name	Datatype	Size	Scale	Nulls?
SOURCEIP	NUMBER		0	
CLIENTTIMESTAMP	NUMBER		0	
CLIENTMS	NUMBER		0	
SERVERTIMESTAMP	NUMBER		0	
SESSIONID	NUMBER		0	
COMPONENT	VARCHAR2	255		
EVENTID	NUMBER		0	
SEVERITY	NUMBER		0	
GROUPING	NUMBER		0	
ORIGINATOR	VARCHAR2	255		✓
ORIGINORTYPE	NUMBER		0	
TARGET	VARCHAR2	255		✓
TARGETTYPE	NUMBER		0	
SUBTARGET	VARCHAR2	255		✓
TEXT1	VARCHAR2	255		✓
TEXT2	VARCHAR2	255		✓
TEXT3	VARCHAR2	255		✓
VALUE1	NUMBER		0	
VALUE2	NUMBER		0	
VALUE3	NUMBER		0	
MIMETYPE	NUMBER		0	
DATASIZE	NUMBER		0	
DATA	LONG RAW			✓
SIGNATURE	VARCHAR2	255		✓

The table name is defined in the Oracle Channel object configuration page. The default table name is `NAUDITLOG`.

For more information on the Oracle channel, see “[Oracle](#)” and “[Using Oracle with Nsure Audit](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

This channel driver is used only on platforms where Oracle can run natively; when running the Secure Logging Server on NetWare, create a JDBC channel to connect to the Oracle server.

## 3.5 Syslog Data Store

The Syslog channel driver, `lgdsyslg`, allows the logging server to log events to a specific syslog facility on any syslog host.

It is also capable of creating localized logs. If the logging applications have localized LSC files, the Syslog channel can write the log files in the language designated in the Syslog Channel object.

For more information on the Syslog channel, see “[Syslog](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

## 3.6 JDBC Data Store

The JDBC channel allows the logging server to output filtered events to any JDBC-enabled data store. For performance reasons, we recommend using only the File or database channels discussed in this section as the primary log channel. You should use JDBC data stores only for notifications.

---

**WARNING:** The JDBC channel does not work on NetWare 5.x. The JDBC channel requires JVM\* 1.4.2, which is not compatible with NetWare 5.x. Attempting to run the JDBC channel on NetWare 5.x abends the server.

---

For more information on the JDBC channel, see “[JDBC](#)” and “[Using JDBC Data Stores with Nsure Audit](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

# Upgrading Novell Nsure Audit

# 4

When upgrading from a previous version of Novell® Nsure™ Audit, please consider the following:

- You do not need to uninstall the previous version of Nsure™ Audit. To upgrade, simply follow the 2.0 product installation instructions for your respective platform.
- If an existing Platform Agent configuration file (`logevent.cfg` or `logevent.conf`) is found during the upgrade, the installation asks if you want to overwrite the Platform Agent configuration file. Do not overwrite the existing file unless you want your Platform Agent to revert to the default configuration settings.
- During an upgrade or install, if iManager 2.0 or newer is found on the system, the Nsure Audit plug-in is copied to the appropriate iManager directory. To complete the upgrade of the iManager plug-in, please follow the instructions detailed in [Chapter 6, “Installing the Nsure Audit iManager Plug-in,”](#) on page 35.
- If you upgrade an existing eDirectory™ Instrumentation, it could take up to five minutes before the updated Instrumentation reloads. To expedite the loading of the eDirectory Instrumentation Agent, you can manually stop and restart it using the following commands:

**Table 4-1** eDirectory Instrumentation Commands

Operating System	command
NetWare®	<code>unload auditds</code> <code>load auditds</code>
Windows	<p>To manually load or unload the eDirectory instrumentation:</p> <ol style="list-style-type: none"><li>1. Load <code>ndscons.exe</code>.</li></ol> <hr/> <p><b>NOTE:</b> <code>ndscons.exe</code> is usually in the <code>\novell\nds</code> directory.</p> <ol style="list-style-type: none"><li>2. In the list of installed services, select <i>Nsure Audit Component</i>.</li><li>3. Click <i>Start</i> or <i>Stop</i>.</li></ol> <p>To configure the eDirectory instrumentation to load each time the server restarts:</p> <ol style="list-style-type: none"><li>1. Load <code>ndscons.exe</code>.</li><li>2. In the list of installed services, select <i>Nsure Audit Component</i>.</li><li>3. Click <i>Startup</i>.</li><li>4. Select the <i>Automatic</i> startup type and click <i>OK</i>.</li></ol>
Linux	<code>ndstrace -c "unload auditDS"</code> <code>ndstrace -c "load auditDS"</code>
Solaris	<code>ndstrace -c "unload auditDS"</code> <code>ndstrace -c "load auditDS"</code>

- On NetWare, if you upgrade an existing NetWare Instrumentation, it could take up to five minutes before the updated Instrumentation reloads. To expedite the loading of the NetWare Instrumentation, you can manually stop and restart it using the following commands:

```
unload auditnw
```

```
load auditnw
```

- On NetWare, if any applications that log events to Nsure Audit are executing during the upgrade, the new Platform Agent cannot be updated until your server restarts. To avoid restarting your server after the upgrade completes, shut down any applications dependent on `logevent.nlm` (such as NetMail<sup>®</sup> or BorderManager<sup>®</sup>) before you attempt the Nsure Audit upgrade.

# Installing and Activating Novell Nsure Audit

# 5

This section contains instructions for installing Novell® Nsure™ Audit on each supported platform. To install, complete the instructions for your Secure Logging Server platform:

- [Section 5.1, “Installing Nsure Audit with Open Enterprise Server,” on page 23](#)
- [Section 5.2, “Installing Nsure Audit with NetWare 6.5,” on page 25](#)
- [Section 5.3, “Installing Nsure Audit on NetWare,” on page 26](#)
- [Section 5.4, “Installing Nsure Audit on Linux,” on page 28](#)
- [Section 5.5, “Installing Nsure Audit on Solaris,” on page 30](#)
- [Section 5.6, “Installing Nsure Audit on Windows,” on page 31](#)
- [Section 5.7, “Activating Nsure Audit,” on page 32](#)
- [Section 5.8, “Activating Nsure Audit Report,” on page 33](#)

## 5.1 Installing Nsure Audit with Open Enterprise Server

- 1 Start the Open Enterprise Server (OES) installation.
- 2 In the Choose a Pattern window, select the Novell Nsure Audit Starter Pack.
  - Select Pre-Configured Server > Novell Nsure Audit Starter Pack.
  - or
  - Select Customized NetWare Server and mark the following components:
    - Apache Web Server and Tomcat Servlet Container
    - MySQL (if you want to configure the MySQL data store during installation)
    - Novell Nsure Audit Starter Pack
    - iManager
- 3 In the Summary window, review the products to be installed, then click Copy Files.
- 4 When the installation program displays the Component Selection window for the Novell Nsure Audit Starter Pack, select the program components you want to install.
  - **Install Secure Logging Server:** Installs the Secure Logging Server (lengine.nlm), the Multiple Directory Database (mdb.nlm), and the channel drivers (lgd\*.nlm) to the current server. It also creates a Logging Server object in the Logging Services container.

You need at least one Secure Logging Server in your network.

    - **Autoconfigure MySQL:** creates the MySQL Channel object in the Logging Services' Channel container and configures the Secure Logging Server to log events to the MySQL database. If you select this option, you must install MySQL with the OES install. (See [Step 2.](#))

---

**WARNING:** The MySQL Channel object is created with a default Expiration script that runs every night at midnight and automatically deletes every record older than 12 hours. This was done because the default events logged by the NetWare and eDirectory instrumentations quickly fill the database. To remove this setting, simply delete the script from the SQL Expiration Commands property in the MySQL Channel object and restart the Secure Logging Server. For more information, see [MySQL Channel Object](#) in the *Novell Nsure Audit 1.0.3 Administration Guide*.

---

- Install Platform Agent installs and configures the Platform Agent (logevent.nlm), the Caching Module (lcache.nlm), and the NetWare and eDirectory instrumentations (auditNW.nlm and auditDS.nlm respectively).

You must install the Platform Agent on every workstation or server that is running an application that logs events to Novell Nsure Audit. To enable NetWare and file system logging, the NetWare instrumentation must be installed and loaded on every server on which you want to log NetWare and file system events. To log eDirectory events, auditDS must be installed and loaded on one server per DS Replica.

- `Secure Logging Server Address` is the IP address or host name of the Secure Logging Server that the Platform Agent connects to.

**5** If you selected the Autoconfigure MySQL option, the installation program displays the Database Options window so you can define your MySQL data store.

- `MySQL Database Host`: The IP Address or host name of the MySQL database server.
- `Port`: Defines the port at which the Secure Logging Server connects to the database server. If this field is left blank, the Secure Logging Server uses the default MySQL port assignment, 3306.
- `DB Username`: User account the Secure Logging Server uses to log in to the database. This account has all privileges to the default database and can log in from any IP address. The default username for the OES data store is “auditusr.”
- `DB User Password`: Password the logging server uses to authenticate with the database. You must confirm this password. The default password for the OES data store is “auditpwd.”
- `Database Name`: Name of the database to which the logging server writes events. The default database name is “naudit.”
- `Table Name`: Database table to which the logging server writes events. The default table is “log.”

**6** Follow the prompts to complete the rest of the OES install.

Upon completing the installation, you must restart the server or manually launch the installed components. For the program startup commands, see [Commands and Utilities](#) in the *Novell Nsure Audit 1.0.3 Administration Guide*.



## 5.2 Installing Nsure Audit with NetWare 6.5

When installing Novell Nsure Audit on NetWare 6.5, we recommended that you follow these instructions to first install Nsure Audit 1.0 from your NetWare 6.5 Installation CD, then run the Nsure Audit 1.0.3 installation to upgrade to version 1.0.3 using the instructions in [Section 5.3](#), “Installing Nsure Audit on NetWare,” on page 26.

- 1 Start the NetWare 6.5 installation.
- 2 In the Choose a Pattern window, select the Novell Nsure Audit Starter Pack.
  - Select Pre-Configured Server > Novell Nsure Audit Starter Pack.or
  - Select Customized NetWare Server and mark the following components:
    - Apache2 Web Server and Tomcat4 Servlet Container
    - MySQL (if you want to configure the MySQL data store during installation)
    - Novell Nsure Audit Starter Pack
    - iManager 2.0
- 3 In the Summary window, review the products to be installed, then click Copy Files.
- 4 When the installation program displays the Component Selection window for the Novell Nsure Audit Starter Pack, select the program components you want to install.
  - **Install Secure Logging Server:** Installs the Secure Logging Server (`lengine.nlm`), the Multiple Directory Database (`mdb.nlm`), and the channel drivers (`lgd*.nlm`) to the current server. It also creates a Logging Server object in the Logging Services container.You need at least one Secure Logging Server in your network.
  - **Autoconfigure MySQL:** creates the MySQL Channel object in the Logging Services' Channel container and configures the Secure Logging Server to log events to the MySQL database. If you select this option, you must install MySQL with the NetWare 6.5 install. (See [Step 2](#).)

---

**WARNING:** The MySQL Channel object is created with a default Expiration script that runs every night at midnight and automatically deletes every record older than 12 hours. This was done because the default events logged by the NetWare and eDirectory instrumentations quickly fill the database. To remove this setting, simply delete the script from the SQL Expiration Commands property in the MySQL Channel object and restart the Secure Logging Server. For more information, see [MySQL Channel Object](#) in the *Novell Nsure Audit 1.0.3 Administration Guide*.

---

- **Install Platform Agent** installs and configures the Platform Agent (`logevent.nlm`), the Caching Module (`lcache.nlm`), and the NetWare and eDirectory instrumentations (`auditNW.nlm` and `auditDS.nlm` respectively).

You must install the Platform Agent on every workstation or server that is running an application that logs events to Novell Nsure Audit. To enable NetWare and file system logging, the NetWare instrumentation must be installed and loaded on every server on which you want to log NetWare and file system events. To log eDirectory events, `auditDS` must be installed and loaded on one server per DS Replica.

- **Secure Logging Server Address** is the IP address or host name of the Secure Logging Server that the Platform Agent connects to.

- 5 If you selected the Autoconfigure MySQL option, the installation program displays the Database Options window so you can define your MySQL data store.
  - **MySQL Database Host:** The IP Address or host name of the MySQL database server.
  - **Port:** Defines the port at which the Secure Logging Server connects to the database server. If this field is left blank, the Secure Logging Server uses the default MySQL port assignment, 3306.
  - **DB Username:** User account the Secure Logging Server uses to log in to the database. This account has all privileges to the default database and can log in from any IP address. The default username for the NetWare 6.5 data store is “auditusr.”
  - **DB User Password:** Password the logging server uses to authenticate with the database. You must confirm this password. The default password for the NetWare 6.5 data store is “auditpwd.”
  - **Database Name:** Name of the database to which the logging server writes events. The default database name is “naudit.”
  - **Table Name:** Database table to which the logging server writes events. The default table is “log.”
- 6 Follow the prompts to complete the rest of the NetWare 6.5 install. For more information, see the [NetWare 6.5 Overview and Installation Guide \(http://www.novell.com/documentation/lg/nw65/install/data/hz8pck9v.html\)](http://www.novell.com/documentation/lg/nw65/install/data/hz8pck9v.html).

Upon completing the installation, you must restart the server or manually launch the installed components. For the program startup commands, see **Commands and Utilities** in the *Novell Nsure Audit 1.0.3 Administration Guide*.

## 5.3 Installing Nsure Audit on NetWare

- 1 On the NetWare server, insert, and if necessary, mount the Nsure Audit 1.0.3 installation CD, then launch NWConfig.
  - On NetWare 5.x or later, load `nwconfig.nlm` at the server console.
  - On NetWare 4.2, enter `load install` at the server console. Only the instrumentation and Platform Agent can be installed on NetWare 4.2.
- 2 In NWConfig, Select Product Options > Install a Product Not Listed.
- 3 Press F3 (F4 if you’re using RCONSOLE) and specify the path to the directory where the installation program can find the `base.ips` file, which is located in the NetWare directory on the installation CD.
- 4 Select your install options. Each option is outlined in the following table. The third and fourth columns contain the recommended settings for a new installation and upgrade.

Option	Description	New Install	Upgrade
First-time Directory Install	Extends the Directory schema for Novell Nsure Audit version 1.0.3.	Yes	No

Option	Description	New Install	Upgrade
Configure Server for Nsure Audit	Creates the Secure Logging Server object in Logging Services. It also creates a File Channel object in the Logging Services Channel container, and configures the Secure Logging Server to log events to the File channel.	Yes	No
Nsure Audit Log Server Files	Installs the Novell Nsure Audit Secure Logging Server (lengine.nlm). The Secure Logging Server securely receives reported events, and is installed on only one server in your tree.	Yes	Yes
Nsure Audit Instrumentation Files	Installs the NetWare Instrumentation (auditNW.nlm) and the eDirectory Instrumentation (auditDS.nlm). This instrumentation must be installed on any NetWare server that will report events.	Yes	Yes
Nsure Audit Platform Agent Files	Installs the Novell Nsure Audit Platform Agent (logevent.nlm). The Platform Agent must be present on any NetWare server that will report events. If you are certain another instrumented application has previously installed the Nsure Audit 1.0.3 Platform Agent on this server, you can leave this unselected.	Yes	Yes
Backup Files from Previous Versions	Makes a backup of existing Nsure Audit files to enable rollback.	No	Yes
Directory Schema Update	Updates the Directory schema for Novell Nsure Audit version 1.0.3.	No	Yes
<hr/> <p><b>NOTE:</b> You must scroll to see this option in nwconfig.</p> <hr/>			

- 5 Press F10 to continue, then follow the on-screen instructions until you have completed the installation program.

If you selected First-time Directory Install or Directory Schema Update, enter the Directory administrator's login name and password to update the schema. This account must have admin rights to the root of the tree. If the admin object is not in the same context as the current server, you must enter the object's fully distinguished name (for example, .Admin.Accounts.Finance.YourCo).

If you selected Configure Server for Nsure Audit, you are prompted to provide a name for the Secure Logging Server object.

Upon completing the installation, you must restart the server or manually launch the installed components. For the program startup commands, see [Commands and Utilities](#) in the *Novell Nsure Audit 1.0.3 Administration Guide*.

## 5.4 Installing Nsure Audit on Linux

- 1 Log in as root on the host.
- 2 Enter the following command from the Linux console:  
On SUSE, `mount /media/cdrom`  
On RedHat, `mount /mnt/cdrom`
- 3 Enter the following command from the Linux console:  
On SUSE, `cd /media/cdrom/Linux`  
On RedHat, `cd /mnt/cdrom/Linux`
- 4 You are now in the setup directory for the Nsure Audit Linux install. Enter the following command from the Linux console to begin the installation:

```
./pinstall.lin
```

The `pinstall.lin` script performs the following actions:

- Verifies that eDirectory for Linux has been installed.
- Copies the Novell Nsure Audit files to the installation directory.
- Starts the `auditext.sh` script.

If you receive a Permission Denied error when attempting to execute the install script, you might need to grant execute rights to `pinstall.lin` by running `chmod 755 pinstall.lin`.

- 5 When prompted, accept the license agreement.
- 6 Select your install options.
  - Platform Agent: Installs the Novell Nsure Audit Platform Agent.
  - eDirectory Instrumentation Files and Platform Agent: Installs the eDirectory Instrumentation and Platform Agent.
  - Secure Logging Server and Platform Agent: Installs the Novell Nsure Audit Secure Logging Server.
  - All: Installs the Secure Logging Server, Platform Agent, and the eDirectory instrumentation.
- 7 After the Nsure Audit components are installed, the `auditext` utility is automatically launched to extend your eDirectory schema, and configure the default Nsure Audit objects.

In `auditext`, run Add Schema Extensions if you are performing a new install or an upgrade, then run Configure Server if you are performing a new install.

If prompted, enter the Directory administrator's login name and password to update the schema.

---

**IMPORTANT:** This account must have admin rights to the root of the tree.

---

If the admin object is not in the same context as the current server, you must enter the object's fully distinguished name (for example, `.Admin.Accounts.Finance.YourCo`).

- 8 If prompted, enter a name for the Secure Logging Server object.
- 9 Continue to follow the installation instructions on the screen until you have exited the Novell Nsure Audit installation program.

When the installation is complete, the Secure Logging Server automatically launches, and the following command is added to `/usr/lib/nds-modules/ndsmodules.conf` to automatically load the eDirectory instrumentation with eDirectory:

```
auditds auto #NSure Audit Platform Agent
```

Remove this command if you do not want the eDirectory instrumentation to automatically load.

To manually start the eDirectory instrumentation, enter:

```
start ndstrace -c "load auditds"
```

## 5.5 Installing Nsure Audit on Solaris

- 1 Log in as root on the host.
- 2 If necessary, mount the `Nsure Audit 1.0.3 Installation` CD, then browse to the Solaris directory from the Solaris console.
- 3 You are now in the setup directory for the Nsure Audit Solaris install. Enter the following command from the Solaris console to begin the installation:

```
./pinstall.sol
```

The `pinstall.sol` script performs the following actions:

- Verifies that eDirectory for Solaris has been installed.
- Copies the Novell Nsure Audit files to the installation directory.
- Starts the `auditext.sh` script.

If you receive a permission denied error when attempting to execute the install script, you might need to grant execute rights to `pinstall.lin` by running `chmod 755 pinstall.lin`

- 4 When prompted, accept the license agreement.
- 5 Select your install options.
  - Platform Agent: Installs the Novell Nsure Audit Platform Agent.
  - eDirectory Instrumentation Files and Platform Agent: Installs the eDirectory Instrumentation and Platform Agent.
  - Secure Logging Server and Platform Agent: Installs the Novell Nsure Audit Secure Logging Server.
  - All: Installs the Secure Logging Server, Platform Agent, and the eDirectory instrumentation.
- 6 After the Nsure Audit components are installed, the `auditext` utility is launched automatically to extend your eDirectory schema, and configure the default Nsure Audit objects.

In `auditext`, run `Add Schema Extensions` if performing a new install or an upgrade, then run `Configure Server` if you are performing a new install.

If prompted, enter the Directory administrator's login name and password to update the schema.

---

**IMPORTANT:** This account must have admin rights to the root of the tree.

---

If the admin object is not in the same context as the current server, you must enter the object's fully distinguished name (for example, `.Admin.Accounts.Finance.YourCo`).

- 7 If prompted, enter a name for the Secure Logging Server object.
- 8 Continue to follow the installation instructions on the screen until you have exited the Novell Nsure Audit installation program.

When the installation is complete, the Secure Logging Server automatically launches, and the following command is added to `/etc/init.d/naudit` to automatically load the eDirectory instrumentation with eDirectory:

```
ndstrace -c "load auditds"
```

Remove this command if you do not want the eDirectory instrumentation to automatically load.

To manually start the eDirectory instrumentation, run the following command from the Solaris console:

```
ndstrace -c "load auditds"
```

## 5.6 Installing Nsure Audit on Windows

- 1 At the Windows server, log in as Administrator or as a user with administrative privileges.
- 2 Run `naudit_win32` from the Windows setup directory on the `Nsure Audit 1.0.3` Installation CD.
- 3 Follow the on-screen instructions in the Novell Nsure Audit Installation Wizard to view and accept the license agreement.
- 4 Provide your customer information.
- 5 Specify the destination directory, then click Next.  
The default directory is `\program files\novell\nsure audit`.
- 6 Select the type of installation you want to perform on the current server, then click Next.
  - Custom: Allows you to individually select which program components to install.
  - Full installation: Installs the Secure Logging Server (`lengine.exe`), the channel drivers (`lgd*.dll`), the Platform Agent (`logevent.dll`), the eDirectory instrumentation (`auditDS.dlm`), and Nsure Audit Report (`lreport.exe`).
  - instrumentation: Installs the Platform Agent and the eDirectory instrumentation.
  - Reporting Application: Installs Nsure Audit Report.
  - Server: Installs the Secure Logging Server, and the channel drivers.The Custom, Full Installation, and Server options create the Secure Logging Server object in Logging Services. They also create a File Channel object in the Logging Services Channel container and they configure the logging server to log events to the File channel.
- 7 If you are installing the instrumentation, specify the IP address of the Secure Logging Server.
- 8 Confirm your settings, then click Next.
- 9 If you are installing the Secure Logging Server, provide the following information when prompted:
  - Specify the Directory administrator's login name and password to update the schema.

---

**IMPORTANT:** This account must have admin rights to the root of the tree.

---
  - Specify a name for the Secure Logging Server object.
- 10 Click OK to confirm the installation.
- 11 Click Finish to complete the Novell Nsure Audit installation.

When the installation is complete, the Secure Logging Server automatically launches; however, you must manually load the eDirectory instrumentation.

To manually load or unload the eDirectory instrumentation:

- 1 Load `ndscons.exe`.

---

**NOTE:** `ndscons.exe` is usually in the `\novell\nds` directory.

---

- 2 In the list of installed services, select Novell Nsure Audit Component.
- 3 Click Start or Stop.

To configure the eDirectory instrumentation to load each time the server restarts:

- 1 Load ndscons.exe.
- 2 In the list of installed services, select Novell Nsure Audit Component.
- 3 Click Startup.
- 4 Mark the Automatic startup type and click OK.

## 5.7 Activating Nsure Audit

When you install the full version of Nsure Audit, the license file is installed with the product and the product is automatically activated; that is, you can configure all the product channels and instrumentations.

If you install the Nsure Audit Starter Pack and you want to upgrade to the full version without re-installing the product, you must purchase a product license.

---

**NOTE:** The Nsure Audit Starter Pack is a scaled down version of Nsure Audit. It allows you to configure the File, SMTP and MySQL channels along with the Windows and Log File Parser instrumentations. However, if you want to use any other channel or instrumentation, you must purchase a product license.

If you configure an unlicensed channel or instrumentation without a Nsure Audit license, the Secure Logging Server (`lengine`) does not load. You must either remove or disable the channel or instrumentation to allow `lengine` to load.

---

When you purchase a license for the Nsure Audit Starter Pack, you receive a license file with an `.nlf` extension. To activate the full version of Nsure Audit, you must copy the license file to the directory that contains the Secure Logging Server program file, `lengine`.

The following table outlines the default `lengine` directory for each platform:

**Table 5-1** *Default lengine Directory*

Platform	Directory
NetWare	<code>sys:\system\naudit.nlf</code>
Windows	<code>\program files\novell\nsure audit\naudit.nlf</code>
Linux	<code>/opt/novell/naudit/naudit.nlf</code>
Solaris	<code>/opt/NOVLnaudit/naudit.nlf</code>

After you copy the license file to the `lengine` directory, you must restart the logging server. For instructions, see “[Secure Logging Server Startup Commands](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.



## 5.8 Activating Nsure Audit Report

To activate Nsure Audit Report (`lreport`):

- 1 In Nsure Audit Report, click *File > Import*, then select *Application Schemata*.
- 2 Specify the IP address of your Nsure Audit logging server, then select a language.

After you activate `lreport`, activation messages no longer appear in Nsure Audit Report.



# Installing the Nsure Audit iManager Plug-in

The Nsure™ Audit iManager plug-in package file is contained in the `add_ons\iManager_plugins` folder in the `Nsure Audit 1.0.3 Installation CD`. Additionally, if an installation of iManager is found during install, the package file was copied to the iManager packages folder on your server.

To install or upgrade the iManager plug-in, complete one of the following task:

- [Section 6.1, “Install or Upgrade the iManager Plug-in,” on page 35](#)
- [Section 6.2, “Install or Upgrade the iManager Plug-In in Assigned Mode with Role-Based Services,” on page 36](#)

## 6.1 Install or Upgrade the iManager Plug-in

- 1 Log in to iManager.
- 2 Click the Configure button .
- 3 Under Module Installation, click Available Novell Plug-in Modules.
- 4 Click New, then browse for the `naudit.npm` file.

The `naudit.npm` module package is located in the `add_ons\iManager_plugins` directory on the `Nsure Audit Installation CD`.

- 5 Click OK. You are returned to the Available Novell Plug-in Modules page.
- 6 Select the `naudit.npm` file, then click Install.

This install takes a few minutes.

- 7 Restart Tomcat.

Platform	Restart Command
NetWare 6.5 or later	Enter <code>TC4STOP</code> . Wait at least 1 minute, then enter <code>TOMCAT4</code> to start the service again.
Windows	Stop and start the Tomcat service.
Solaris	Enter <code>/etc/init.d/imgr stop</code> , then enter <code>/etc/init.d/imgr start</code> .
Linux	Enter <code>/etc/init.d/novell-tomcat4 stop</code> , then enter <code>/etc/init.d/novell-tomcat4 start</code> .

Allow adequate time for Tomcat to fully initialize before attempting to launch iManager.

- 8 Restart Apache.
- 9 Log in to iManager.
- 10 Verify that the Auditing and Logging Role appears in the Roles and Tasks page.


## 6.2 Install or Upgrade the iManager Plug-In in Assigned Mode with Role-Based Services

---

**IMPORTANT:** To reinstall the Nsure Audit plug-in (naudit.npm), you must first delete the rbsModule object for the plug-in from eDirectory using the Module Configuration > Delete RBS Module task.

---

If you are running iManager in Assigned Mode and have RBS configured, complete the following steps to install or update the Nsure Audit iManager plug-in:

- 1 Log into iManager as a Collection Owner.
- 2 Click the Configure button .
- 3 Click iManager Configuration > Modules > Install to install the naudit.npm module package.
- 4 Select the naudit.npm file to install.


The naudit.npm module package is located in the add\_ons\iManager\_plugins directory on the Nsure Audit Installation CD.

This install takes a few minutes.

- 5 Restart Tomcat.

Platform	Restart Command
NetWare 6.5 or later	Enter <code>TC4STOP</code> . Wait at least 1 minute, then enter <code>TOMCAT4</code> to start the service again.
Windows	Stop and start the Tomcat service.
Solaris	Enter <code>/etc/init.d/imgr stop</code> , then enter <code>/etc/init.d/imgr start</code> .
Linux	Enter <code>/etc/init.d/novell-tomcat4 stop</code> , then enter <code>/etc/init.d/novell-tomcat4 start</code> .

Allow adequate time for Tomcat to fully initialize before attempting to launch iManager.

- 6 Restart Apache.
- 7 Log in to iManager, then click the Configure button .
- 8 Select Role-Based Services > RBS Configuration.  
The table on the 2.x Collections tabbed page displays any out-of-date modules.
- 9 To update, select the number listed in the Out-of-Date column for the Collection that contains the Nsure Audit plug-in (naudit.npm).  
iManager displays the Collection's list of outdated modules, including naudit.npm.
- 10 Select the Nsure Audit plug-in, then click Update at the top of the table.

# Configuring the Secure Logging Server

# 7

The Secure Logging Server manages the flow of information to and from the Novell® auditing system. It receives incoming events and requests from the Platform Agents, logs information to the data store, monitors designated events, and provides filtering and notification services. It can also be configured to automatically reset critical system attributes according to a specified policy.




You configure the Secure Logging Server using the Nsure™ Audit iManager plug-in. If you are performing an upgrade, configuring the Secure Logging Server is optional because your Nsure Audit environment continues to operate with your previous configuration.

The following sections review how to configure the Secure Logging Server and how to configure a system with multiple Secure Logging Servers:

- [Section 7.1, “Configuring the Secure Logging Server,” on page 37](#)
- [Section 7.2, “Configuring Multiple Secure Logging Servers,” on page 39](#)
- [Section 7.3, “Configuring a Secure Logging Server with More Than One IP Address,” on page 39](#)

## 7.1 Configuring the Secure Logging Server

To configure the Secure Logging Server:

- 1 Log in to iManager.
- 2 Click the *Roles and Tasks* button  on the iManager toolbar.
- 3 In the Roles and Tasks view, expand the *Auditing and Logging Role*, then select *Logging Server Options*.
- 4 Select the Secure Logging Server object, then click *OK*.
  - Click the *Object History* button  to see a list of Logging Server objects that have been selected during this iManager session.
  - or
  - Click the *Object Selector* button  to locate the object in the directory tree. To move up or down in the tree, click the navigation arrows. You can also search the tree by typing the object name and context in the Search frame.

- 5 Run the configuration wizard by clicking the *Secure Logging Server Interactive Configuration Guide* link on the summary screen. This configuration guide provides on-screen information to guide you in setting up your Secure Logging Server.

## Server Configuration: Logging Server

General Channels Notifications Log Applications  
 Summary | Configuration | Memory | Status

This summary gives you an overview of how your Secure Logging Server is configured. If you wish to configure it you may select Channels, Notifications, Applications above, or you may use the [Secure Logging Server Interactive Configuration Guide](#) to be guided through the configuration process.

For detailed instructions on configuring the Secure logging Server, see “[Configuring the Secure Logging Server](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

- 6 To minimize server reaction time and ensure high system performance, we recommend that you create a local replica of the Logging Server object and its associated objects on the logging server.
- 7 After you have completed the Secure Logging Server configuration, restart your Secure Logging Server using the following commands:

Platform	Command
NetWare®	<pre>unload lengine load lengine</pre>
Windows	<ol style="list-style-type: none"> <li>1. Click <i>Start &gt; Settings &gt; Control Panel</i>.</li> <li>2. Open the Services window. <ul style="list-style-type: none"> <li>• On Windows NT*, select <i>Services</i>.</li> <li>• On Windows 2000 and XP, select <i>Administrative Tools &gt; Services</i>.</li> </ul> </li> <li>3. In the list of installed services, right-click <i>Nsure Audit Manager</i>, then select <i>Stop</i>.</li> <li>4. Right-click <i>Nsure Audit Manager</i>, then select <i>Start</i>.</li> </ol>
Linux	<pre>/etc/init.d/novell-naudit stop /etc/init.d/novell-naudit start</pre>
Solaris	<pre>/etc/init.d/naudit stop /etc/init.d/naudit start</pre>

## 7.2 Configuring Multiple Secure Logging Servers

By default, the installation program creates the Secure Logging Server in the Logging Services container. The logging server then reads its channel and notification configuration information from the Channels.Logging Services and Notifications.Logging Services containers and loads the channels and notifications located within these containers.

If you want to provide system redundancy or load balancing in your logging system, you can create multiple Secure Logging Server objects for servers on the same platform in the default Logging Services container. In this way, all the logging servers load the same channels and send data to the same database.

However, if you want to log data to different databases (such as in a WAN environment); load different channels and notifications on each logging server; if you have an extremely large eDirectory™ tree; or if you are running Nsure Audit Secure Logging servers on multiple platforms, we recommend that you create separate eDirectory organizational units as containers for each Secure Logging Server's configuration object.

If you want a combination of both configurations—for example, you want to provide system redundancy or load balancing in a WAN environment—you can create multiple eDirectory organizational units with multiple Secure Logging Server objects.

The following sections in the *Novell Nsure Audit 1.0.3 Administration Guide* review how to implement multiple Secure Logging Servers in your logging system based on whether you want to locate the Secure Logging Server objects in the same container, different containers, or a combination of both:

- “Creating Multiple Secure Logging Server Objects in a Single eDirectory Container”
- “Creating Secure Logging Server Objects in Different eDirectory Containers”
- “Creating Multiple Secure Logging Server Objects in Multiple eDirectory Containers”

## 7.3 Configuring a Secure Logging Server with More Than One IP Address

Secure Logging Servers with more than one IP address have problems running Nsure Audit because MDB does not know which IP address to use with eDirectory. You can point Nsure Audit to a specific IP address using an MDB configuration file.

The required filename and path for the MDB configuration file is as follows:

**Table 7-1** *MDB Configuration File*

Platform	Directory
NetWare	sys:\etc\mdb.cfg
Windows	\windows\mdb.cfg
Linux	/etc/mdb.conf
Solaris	/etc/mdb.conf

To point Nsure Audit to a specific IP address for eDirectory, the MDB configuration file must store the following parameter:

```
driver=mdbds referral=eDirectory_IP_Address
```

For example,

```
driver=mdbds referral=192.168.123.45
```



# Configuring the Platform Agent and Logging Instrumentations

# 8

This section contains instructions on installing and configuring the Platform Agent and Instrumentations on servers that will report events to the Secure Logging Server.

- [Section 8.1, “Installing the Logging Components,” on page 41](#)
- [Section 8.2, “Configuring the Platform Agent,” on page 42](#)
- [Section 8.3, “Configuring eDirectory, File System, and NetWare Events,” on page 43](#)

## 8.1 Installing the Logging Components

You must install the Platform Agent on every server that you want to report events to the Secure Logging Server. You must also install the Instrumentation associated with every logging application that you want to report events to Novell® Nsure™ Audit.

To install the logging components on servers that will report events to the Secure Logging Server:

- 1 Run the Nsure Audit installation.

For specific instructions, see [Chapter 5, “Installing and Activating Novell Nsure Audit,” on page 23](#).

- 2 To install only the logging components, select the following install options:

Platform	Install Option	Description
NetWare®	Install Nsure Audit Instrumentation Agents	<p>Installs the Platform Agent (<code>logevent.nlm</code>), the NetWare Instrumentation (<code>auditNW.nlm</code>), and the eDirectory Instrumentation (<code>auditDS.nlm</code>).</p> <p>These instrumentations must be installed on any NetWare server that you want to report eDirectory™, file system, or NetWare events.</p> <hr/> <p><b>IMPORTANT:</b> Before you install the eDirectory instrumentation on NetWare, your server must be updated with the latest version of NICI. See <a href="#">Section 2.2.1, “NICI,” on page 13</a> for details.</p>
Linux	eDirectory Instrumentation Files with Platform Agent	<p>Installs the Platform Agent (<code>liblogevent.so</code>), the eDirectory Instrumentation (<code>libauditDS.so</code>), the Platform Agent (<code>liblogevent.so</code>), and the Log Parser (<code>logparse</code>).</p> <p>The eDirectory instrumentation must be installed on any Linux server that you want to report eDirectory events.</p>

Platform	Install Option	Description
Solaris	eDirectory Instrumentation Files with Platform Agent	Installs the Platform Agent ( <code>liblogevent.so</code> ), the eDirectory Instrumentation ( <code>libauditDS.so</code> ), the Platform Agent ( <code>liblogevent.so</code> ), and the Log Parser ( <code>logparse</code> ).  The eDirectory instrumentation must be installed on any Solaris server that you want to report eDirectory events.
Windows	Instrumentation	Installs the Platform Agent ( <code>logevent.dll</code> ), the eDirectory instrumentation ( <code>auditDS.dlm</code> ), the Windows Instrumentation ( <code>nauditwin.exe</code> ), and the Log Parser ( <code>logparse.exe</code> ).  The eDirectory and Windows instrumentations must be installed on any Windows server that you want to report eDirectory and Windows events.

- 3** If you are installing the eDirectory Instrumentation on a server that is located in a different tree than your Secure Logging Server, you must also select one of the following install options to add the Nsure Audit schema extensions to eDirectory:

Platform	Install Option
NetWare	Add Schema Extensions
Linux, Solaris, Windows	Extend Schema

If the eDirectory Instrumentation is located in the same tree as your Secure Logging Server, the schema is extended during the Secure Logging Server installation.

- 4** If you are upgrading from a previous version of Nsure Audit and the installation finds an existing Platform Agent configuration file (`logevent.cfg` or `logevent.conf`), the installation asks if you want to overwrite the Platform Agent configuration file. Do not overwrite the existing file unless you want your Platform Agent to revert to the default configuration settings.
- 5** After the installation is complete, configure the Platform Agent on each server as explained in [Section 8.2, “Configuring the Platform Agent,” on page 42](#).

## 8.2 Configuring the Platform Agent

The Platform Agent, `logevent`, is the client portion of the Nsure auditing system. The Platform Agent is required on any server that reports events to Nsure Audit. It receives logging information and system requests from authenticated applications and transmits the information to the Secure Logging Server.

The Platform Agent’s configuration settings are stored in a simple, text-based configuration file (`logevent`). The default location of this file is as follows:

**Table 8-1** Platform Agent Configuration File

Operating System	File
NetWare	/etc/logevent.cfg
Linux	/etc/logevent.conf
Solaris	/etc/logevent.conf
Windows	/windows_directory/logevent.cfg

The *windows\_directory* is usually *drive:\windows*.

Storing the Platform Agent’s configuration in a local text file makes the Platform Agent small, unobtrusive, and self-contained—that is, it has no external dependencies, so it is always available to receive logged events. Storing the Platform Agent’s configuration in a text-based file also allows the Platform Agent to eventually run on platforms that do not have eDirectory support.

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

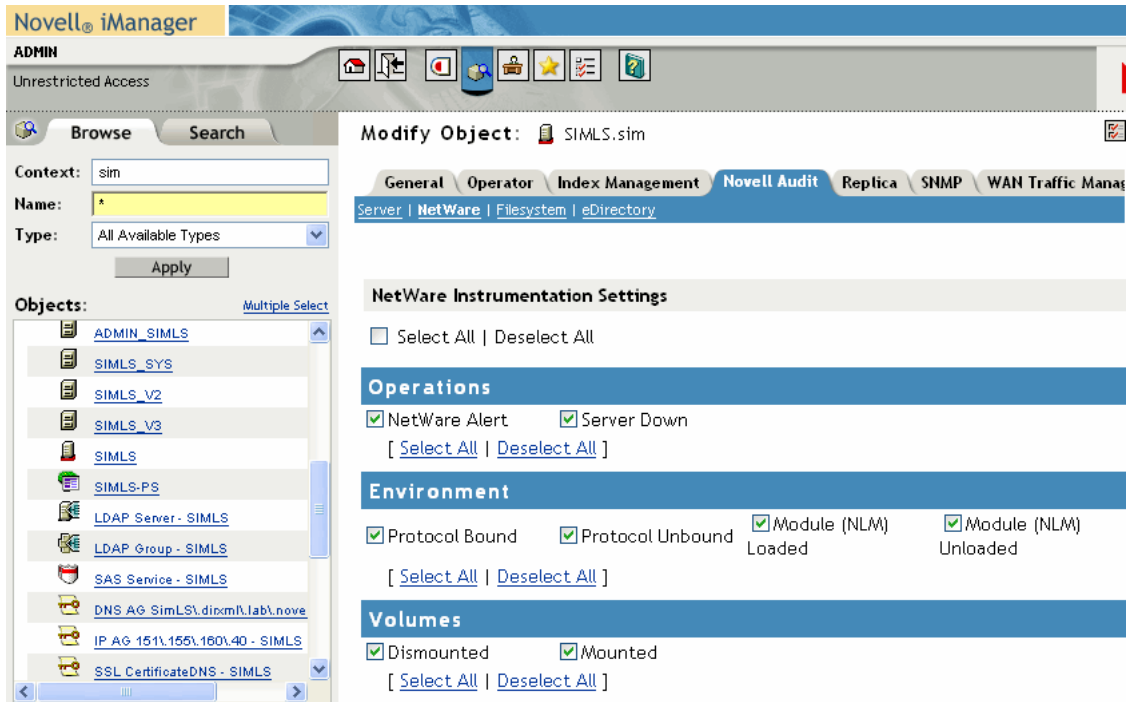
```
LogHost=127.0.0.1
LogCacheDir=c:\logcache
LogCachePort=288
LogEnginePort=289
LogCacheUnload=no
LogReconnectInterval=600
LogDebug=never
LogSigned=always
```

For detailed information on `logevent` parameters and the Platform Agent Configuration tool, see “Configuring the Platform Agent” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

## 8.3 Configuring eDirectory, File System, and NetWare Events

Novell® Nsure™ Audit provides the instrumentations necessary to log Novell eDirectory™, NetWare®, traditional file system, and NSS events. To configure which events you want to log to the data store, you must enable those events on the NCP server object.

During installation, Nsure Audit extends the definition of the NCP Server object to include log settings for eDirectory, NetWare, and file system events. These settings are found under the *Nsure Audit* tab in the NCP Server object.



The Nsure Audit screen has four different menus: *Server*, *NetWare*, *Filesystem*, and *eDirectory*.

The *Server* menu identifies the Logging Server object associated with the current NCP Server object. This menu is for informational purposes only and cannot be modified.

The *NetWare*, *Filesystem*, and *eDirectory* menus list the events that fall in their respective categories.

To select which NetWare, File system, or eDirectory events you want to log:

- 1 Click *Nsure Audit* in the NCP Server object.
- 2 Select an event menu (NetWare, Filesystem, or eDirectory).
- 3 Mark the check box next to the events you want to log.
- 4 Click *Apply*.

---

**IMPORTANT:** You must click *Apply* in each screen to save your changes.

---

- 5 When finished, click *OK*.

When you click *Apply*, the logging server automatically begins logging the marked events.

---

**NOTE:** You do not need to restart the logging server to effect changes to Nsure Audit attributes in the NCP Server object.

---

# Verifying the Installation

After you have completed the instructions in this Installation Guide, you should have the following Novell® Nsure™ Audit components in your environment:

- A Secure Logging Server that is configured to log events to your data store, and send notifications to any additional channels you have configured.
- One or more Platform Agents and the Instrumentations required for the logging applications on each server that logs events to the Secure Logging Server. The Platform Agent on each system should be configured to report events to your Secure Logging Server and each Instrumentation should be configured to report the events you want to monitor.

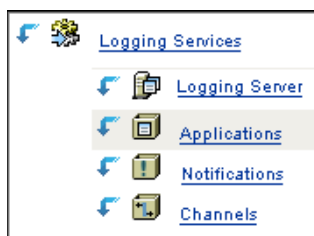
This section contains basic procedures and information to make sure these Nsure Audit components are installed and working correctly.

- [Section 9.1, “eDirectory Objects,” on page 45](#)
- [Section 9.2, “Data Store,” on page 46](#)
- [Section 9.3, “Secure Logging Server,” on page 46](#)
- [Section 9.4, “Platform Agent and Logging Instrumentations,” on page 48](#)

## 9.1 eDirectory Objects

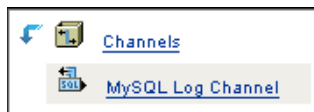
In eDirectory™, verify that you have a Logging Services container at the root of your tree with a Secure Logging Server object. The Logging Services container should also contain an Application, Notification, and Channel container.

**Figure 9-1** Logging Services Container in eDirectory



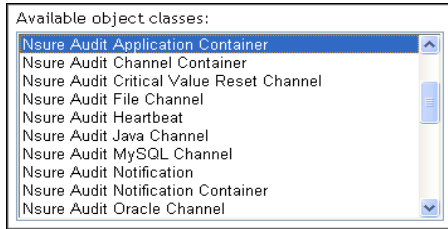
Within the Channel container, you should have a Channel object for your data store.

**Figure 9-2** Channel Container in eDirectory



If any of these objects are missing, verify that the Nsure Audit schema extensions are installed by using the *Schema > Class Information* task. In the class list, verify that the NAudit classes are present:

**Figure 9-3** Nsure Audit Schema Class Information



If these schema extensions are missing, run the AuditExt utility and select the *Add Schema Extensions* option. For a listing of the AuditExt startup commands, see “[AuditExt](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

If the schema has been extended correctly, but you do not have a Logging Services container or Secure Logging Server object, run `opt/novell/naudit/auditext` and select the *Configure Server* option.

If you have not done this, follow the instructions in [Chapter 7, “Configuring the Secure Logging Server,”](#) on page 37.

## 9.2 Data Store

Make sure that your data store is running and is accessible to the Secure Logging Server.

## 9.3 Secure Logging Server

The Nsure Audit Secure Logging Server should be running on your server. The following table outlines the startup commands for each platform:

---

**IMPORTANT:** You must individually start or stop each logging server in the tree.

---

**Table 9-1** *Secure Logging Server Startup Commands*

<b>Platform</b>	<b>Startup Command</b>
Windows	<p>To determine if the Nsure Audit Manager service is running, open the Services applet from <i>Control Panel &gt; Administrative Tools</i>.</p> <p>On Windows, the startup script for the Secure Logging Server is included in the <code>naudit.exe</code> file. <code>Naudit.exe</code> has an Automatic startup type so <code>lengine.exe</code> loads each time the server restarts.</p> <p>To manually load or unload the Secure Logging Server on Windows, you must start or stop the Nsure Audit Manager service:</p> <ol style="list-style-type: none"><li>1. Click <i>Start &gt; Settings &gt; Control Panel</i>.</li><li>2. Open the Services window.<ul style="list-style-type: none"><li>• On Window NT, select <i>Services</i>.</li><li>• On Windows 2000 and XP, select <i>Administrative Tools &gt; Services</i>.</li></ul></li><li>3. In the list of installed services, right-click <i>Nsure Audit Manager</i>, then select <i>Start</i> or <i>Stop</i>.</li></ol>
NetWare®	<p><code>Lengine.nlm</code> should be running on the server hosting the Secure Logging Server. This is configured to load automatically at startup during install.</p> <p>To determine if <code>lengine.nlm</code> is loaded, enter <code>m lengine</code> at the NetWare command prompt. If <code>lengine</code> is not loaded, reload it and check the NetWare logger screen for any messages.</p> <p>To manually load the Secure Logging Server on NetWare, enter</p> <pre>load lengine</pre> <p>or</p> <pre>load auditsvr.ncf</pre> <p>If you want to prevent the Secure Logging Server from being unloaded by users with access to the server console, you can append the <code>-n</code> switch to the server startup script. (For example, <code>load lengine -n</code>.)</p> <p>To manually unload the Secure Logging Server on NetWare, enter</p> <pre>unload lengine</pre> <hr/> <p><b>NOTE:</b> <code>Lengine.nlm</code> and <code>auditsvr.ncf</code> are located in the <code>sys:\system</code> directory.</p>

Platform	Startup Command
Linux	<p>To verify that the Secure Logging Server is running, use the following command:</p> <pre>ps -ef  grep lengine</pre> <p>The Linux startup script for the Secure Logging Server is <code>/etc/init.d/novell-naudit</code>. This startup script loads <code>lengine</code> each time the server restarts.</p> <p>To manually start the Secure Logging Server on Linux, enter</p> <pre>/etc/init.d/novell-naudit start</pre> <p>To stop the Secure Logging Server on Linux, enter</p> <pre>/etc/init.d/novell-naudit stop</pre>
Solaris	<p>To verify that the Secure Logging Server is running, use the following command:</p> <pre>ps -ef  grep lengine</pre> <p>On Solaris, the startup script for the Secure Logging Server is <code>/etc/init.d/naudit</code>. This startup script loads <code>lengine</code> each time the server restarts.</p> <p>To manually start the Secure Logging Server on Solaris, enter</p> <pre>/etc/init.d/naudit start</pre> <p>To stop the Secure Logging Server on Solaris, enter</p> <pre>/etc/init.d/naudit stop</pre>

For more information on the Secure Logging Server, see [Chapter 7, “Configuring the Secure Logging Server,” on page 37](#) and “Configuring the Secure Logging Server” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

## 9.4 Platform Agent and Logging Instrumentations

You must install the Platform Agent on every server that you want to report events to the Secure Logging Server. You must also install the Instrumentation associated with every logging application that you want to report events to Nsure Audit. This section reviews how to verify you are running the Platform Agent and Instrumentations required to log events to the Secure Logging Server:

- [Section 9.4.1, “Platform Agent,” on page 48](#)
- [Section 9.4.2, “NetWare and eDirectory Instrumentations,” on page 49](#)
- [Section 9.4.3, “Nsure Audit Instrumentation,” on page 51](#)

### 9.4.1 Platform Agent

Each logging application requires a Platform Agent to send events to the Secure Logging Server. Consequently, each logging application’s associated Instrumentation automatically loads the Platform Agent.

The following table outlines commands you can use to verify that the Platform Agent is loaded:



---

**NOTE:** In some cases, it might be possible that the Platform Agent is available when `lcache` is not running. The `lcache` process is started by the Platform Agent when an instrumentation attempts to send an event. In the unlikely event that none of the instrumentations are sending events to the Platform Agent, `lcache` will not be running; however, the Platform Agent will still be available.

---

**Table 9-2** *Commands Used to Verify the Platform Agent is Loaded*

---

Operating System	Command
NetWare	To determine if <code>logevent.nlm</code> is loaded on NetWare, enter <code>m logevent</code> at the NetWare command prompt.  If <code>logevent.nlm</code> is not loaded, reload it and check the NetWare logger screen for any messages.
Linux/Solaris	To verify that the Platform Agent is running on Linux or Solaris, use the following command:  <pre>ps -ef  grep lcache</pre>
Windows	To determine if the Platform Agent is running on Windows, open <i>Task Manager</i> and verify that <code>lcache.exe</code> is running.

---

For more information on the Platform Agent, see “[Configuring the Platform Agent](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*

## 9.4.2 NetWare and eDirectory Instrumentations

The NetWare and eDirectory Instrumentations for Nsure Audit (`auditNW` and `auditDS`, respectively) allow Nsure Audit to log NetWare, eDirectory, and file system events.

To enable NetWare and file system logging, `auditNW` must be loaded on every server where you want to log NetWare and file system events. Additionally, the Platform Agent must be installed on every server where you want to log NetWare, file system, and eDirectory events. `auditNW` and `auditDS` automatically load the Platform Agent (`logevent`) to send events to the Secure Logging Server.

---

**NOTE:** Before the Platform Agents are launched, the `LogHost` parameter in the Platform Agent configuration file on each server must be updated with the IP address or DNS name of your Secure Logging Server. For more information, see “[Configuring the Platform Agent](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

---

Typically, `auditNW` and `auditDS` are automatically loaded each time the server restarts. However, you can also manually load or unload the instrumentation files.

The following table reviews the startup commands for the eDirectory and NetWare Instrumentations.

---

**IMPORTANT:** You must individually start or stop the instrumentations on each server in the tree.

---

**Table 9-3** NetWare and eDirectory Instrumentation Startup Commands

Platform	Startup Command
NetWare	<p>On NetWare, the startup scripts for <code>auditNW</code> and <code>auditDS</code> are included in the <code>auditagt.ncf</code> file. <code>Auditagt.ncf</code> is added to the server's <code>autoexec.ncf</code> file during installation. Therefore, the NetWare and eDirectory Instrumentations automatically load each time the server restarts.</p> <p>If you want to prevent <code>auditNW</code> or <code>auditDS</code> from being unloaded by users with access to the server console, you can append the <code>-n</code> switch to the agent startup scripts. (For example, <code>load auditnw -n</code>.)</p> <p>To manually start the NetWare or eDirectory Instrumentation on NetWare, enter</p> <pre>load auditnw</pre> <p>or</p> <pre>load auditDS</pre> <p>To load both the NetWare and eDirectory Instrumentations, enter</p> <pre>load auditagt.ncf</pre> <p>To stop the NetWare and eDirectory Instrumentations on NetWare, enter</p> <pre>unload auditnw</pre> <pre>unload auditDS</pre> <hr/> <p><b>NOTE:</b> <code>Auditnw.nlm</code>, <code>audit.ds</code>, and <code>auditagt.ncf</code> are located in the <code>sys:\system</code> directory.</p>
Linux	<p>On Linux systems, the eDirectory Instrumentation must be manually loaded on one server per DS Replica.</p> <p>To manually start the eDirectory Instrumentation on Linux, enter</p> <pre>ndstrace -c "load auditDS"</pre> <p>To manually stop the eDirectory Instrumentation on Linux, enter</p> <pre>ndstrace -c "unload auditDS"</pre> <p>To automatically load the eDirectory Instrumentation each time the server restarts, add the following to the <code>ndsmodules.conf</code> file:</p> <pre>auditDS auto #NSure Audit Platform Agent</pre> <hr/> <p><b>NOTE:</b> On eDirectory 8.7, the path to the <code>ndsmodules.conf</code> file is <code>/usr/lib/nds-modules/ndsmodules.conf</code>. On eDirectory 8.8, the path is <code>/etc/opt/novell/eDirectory/nds-modules/ndsmodules.conf</code>.</p> <hr/> <p>On Linux systems, the startup script is <code>/etc/init.d/novell-naudit</code>.</p>

Platform	Startup Command
Solaris	<p>On Solaris systems, the eDirectory Instrumentation must be manually loaded on one server per DS Replica.</p> <p>To manually start the eDirectory Instrumentation on Solaris, enter</p> <pre>ndstrace -c "load auditDS"</pre> <p>To manually stop the eDirectory Instrumentation on Solaris, enter</p> <pre>ndstrace -c "unload auditDS"</pre> <p>To automatically load the eDirectory Instrumentation each time the server restarts, add the following to the <code>/usr/lib/nds-modules/ndsmodules.conf</code> file:</p> <pre>auditDS auto #NSure Audit Platform Agent</pre> <hr/> <p><b>NOTE:</b> On eDirectory 8.7, the path to the <code>ndsmodules.conf</code> file is <code>/usr/lib/nds-modules/ndsmodules.conf</code>. On eDirectory 8.8, the path is <code>/etc/opt/novell/eDirectory/nds-modules/ndsmodules.conf</code>.</p> <hr/> <p>On Solaris systems, the startup script is <code>/etc/init.d/naudit</code>.</p>
Windows	<p>On Windows, the eDirectory Instrumentation is managed through the Novell eDirectory Services utility. By default, the eDirectory Instrumentation must be manually loaded on one server per DS Replica.</p> <p>To manually load or unload the eDirectory Instrumentation on Windows:</p> <ol style="list-style-type: none"> <li>1. Load <code>ndscons.exe</code>. <code>Ndscons.exe</code> is usually in the <code>\novell\nds\</code> directory.</li> <li>2. In the list of installed services, select the <i>Nsure Audit Component</i>.</li> <li>3. Click <i>Start</i> or <i>Stop</i>.</li> </ol> <p>To configure <code>auditDS.dlm</code> to load each time the server restarts:</p> <ol style="list-style-type: none"> <li>1. Load <code>ndscons.exe</code>. <code>Ndscons.exe</code> is usually in the <code>\novell\nds\</code> directory.</li> <li>2. In the list of installed services, select the <i>Nsure Audit Component</i>.</li> <li>3. Click <i>Startup</i>.</li> <li>4. Select the <i>Automatic</i> startup type, then click <i>OK</i>.</li> </ol>

For more information on the eDirectory and NetWare Instrumentations, see “[Section 8.1, “Installing the Logging Components,” on page 41](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*. For a complete listing of logged events, see “[Application Events](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*

### 9.4.3 Nsure Audit Instrumentation

The Nsure Audit Instrumentation (`NsureAuditInst`) logs an event every time the Secure Logging Server loads a Channel, Notification, or Application object. It also logs an event each time a Channel driver fails to load or if there is a bad Heartbeat or Notification configuration. Therefore, by reviewing your system’s Audit the Auditor events, you can determine if your logging server is performing the way you expect.

The Nsure Audit Instrumentation automatically loads with the Secure Logging Server. We do not recommend that you unload the Nsure Audit Instrumentation.

For more information about the Nsure Audit instrumentation, see t“[Section 8.1, “Installing the Logging Components,” on page 41](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.

## 9.5 Verifying Event Logging

The final step in testing is verifying that your data store is receiving the events reported to the Secure Logging Server. The audit console displays the number of events that have been stored; verify that the events reported to your Secure Logging Server are in your data store by running queries in iManager or Nsure Audit Report (`lreport`). For more information, see “[Generating Queries and Reports](#)” in the *Novell Nsure Audit 1.0.3 Administration Guide*.