AUTHORIZED DOCUMENTATION

Administration Guide

Novell® SecretStore®

3.4.1

May, 2009

www.novell.com

Legal Notices

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

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

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

Copyright © 2006-2009 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 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 online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This guide provides an overview of Novell® SecretStore. It includes instructions on how to install, configure, and manage SecretStore.

Audience

This guide is written primarily 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 Comment 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 *Novell SecretStore 3.4.1 Administration Guide*, see SecretStore 3.4.1 Administration Guide Web site (http://www.novell.com/documentation/secretstore34/index.html).

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.

Novell SecretStore Overview

1

Novell® SecretStore® is a simple and secure password management solution. SecretStore enables you to use a single authentication to Novell eDirectory™ to access most UNIX*, Windows*, Web, and mainframe applications.

After you've authenticated to eDirectory, applications enabled for SecretStore store and retrieve the appropriate login credentials. When you use SecretStore, you eliminate the need to remember or synchronize all the multiple passwords required for accessing password-protected applications, Web sites, and mainframes.

NOTE: SecretStore 3.4.1 has the same functionality as earlier versions, but is built on eDirectory 8.8.*x*, rather than eDirectory 8.7.3.*x* used in earlier versions.

This section provides information on the following:

1.1 Server and Workstation Components

This topic describes SecretStore components for servers and workstations.

1.1.1 Server Components

Table 1-1 *NetWare Servers*

Filename	Description
`sssi.nlm`	The Novell SecretStore installation NetWare® Loadable Module™ (NLM). It extends: ◆ eDirectory schema ◆ Installs the Novell SecretStore server and its plug-ins (`lsss.nlm`, `sss.nlm`, `ssldp.nlm`, and `ssncp.nlm`) ◆ Configures the eDirectory LDAP server to enable SecretStore extensions ◆ Initializes or validates the Security Domain Infrastructure (SDI) on NetWare The NLM is currently a component of the eDirectory installation and is installed with the product installation. **NOTE:** On all other platforms, such as UNIX* and Windows*, the server installation and configuration is also a component of eDirectory installation.
`sss.nlm`	The Novell SecretStore service. SecretStore provides a secure infrastructure for storing and retrieving secrets and credentials in eDirectory. SecretStore uses NICI and SDI to safely and securely store a user's secrets. Novell SecureLogin, Novell Portal Services, Novell Identity Manager, Novell Access Manager, and Novell iChain® all provide single sign-on functionality to applications that use SecretStore. Upon a successful authentication of the user to an application, if the application is enabled for SecretStore, the application stores its login credential in SecretStore. From then on, when the user logs in to eDirectory and launches the application, the single sign-on client retrieves the application password from SecretStore, provides it to the application or Web site in the background, and authenticates the user.
`ssldp.nlm`	The SecretStore LDAP transport plug-in.
`sssncp.nlm`	The SecretStore NCP™ transport plug-in.
`lsss.nlm`	The LDAP SecretStore extension manager. It enables applications to use the Lightweight Directory Access Protocol (LDAP) to securely store and retrieve secrets.

Table 1-2 *SLES, Solaris, or AIX Servers*

Filename	Description
`libsss.so`	The SecretStore service.
`libssldp.so`	The SecretStore LDAP transport plug-in.
`libssncp.so`	The SecretStore NCP transport plug-in.
`liblsss.so`	The LDAP SecretStore extension manager.

Table 1-3 *Windows Servers*

Filename	Description
`sss.dlm`	The SecretStore service.
`ssldp.dlm`	The SecretStore LDAP transport plug-in for Windows.
`ssncp.dlm`	The SecretStore NCP transport plug-in for Windows.
`lsss.dll`	The LDAP SecretStore extension manager.

For more information on SecretStore, see the following:

- SecretStore information in Novell Developer Kits, available at:
  - Novell SecretStore Developer Kit for C (http://developer.novell.com/wiki/index.php/Novell_SecretStore_Developer_Kit_for_C)
  - Novell SecretStore Developer Kit for Java (http://developer.novell.com/wiki/index.php/Novell_SecretStore_Developer_Kit_for_Java)
- Novell AppNotes, May, 2003, A Technical Overview of Novell SecretStore 3.2 (http://support.novell.com/techcenter/articles/dnd20030503.html)
- Novell AppNotes, June, 2003, Understanding the Novell SecretStore 3.2 APIs (http://support.novell.com/techcenter/articles/dnd20030603.html)

1.1.2 Workstation Components

For the SecretStore 3.4.1 service release, the SecretStore client requires the following components:

NICI client: Enables the SecretStore client to provide all the encrypted traffic between SecretStore, the SecretStore client, the Novell Modular Authentication Services (NMAS™) client, and application connectors over NCP.

NMAS client: Enables single sign-on users to authenticate to eDirectory.

SecretStore client: Provides the mechanism to access the SecretStore service and ensure secure transmission, storage, and retrieval of secrets to and from eDirectory.

The SecretStore client collects secrets (for example, usernames and passwords), recognizes an application credential or password field, and helps to authenticate users by passing the credentials to the application.

The SecureLogin client enables anyone to use applications without repeatedly entering passwords. A user can be logged in to or disconnected from a network.

NOTE: The NCP protocol is supported only on the Windows client platform. Other platforms must use LDAP protocol.

SecretStore iManager plug-in: Enables administrators or users to create, configure, and administer SecretStore components and data through iManager. It is available on the supported server and client platforms.

1.2 SecretStore Service Objects

The SecretStore server components and workstation components work with eDirectory objects to provide SecretStore services.

1.2.1 SecretStore

The SecretStore object is a Container object, located within the eDirectory security container, that can hold default SecretStore service settings.

This object is automatically named SecretStore and placed in the Security container when the SecretStore service is installed on the server.

The SecretStore system requires at least one SecretStore Container object. The SecretStore object can contain sssServerPolicyOverride objects.

For more information on SecretStore objects, see Section 4.1.1, “SecretStore Objects,” on page 39.

1.2.2 sssServerPolicyOverride Object

sssServerPolicyOveride objects enable you to customize access to applications, depending on group or user needs for different parts of the tree.

sssServerPolicyOverride objects reside in the SecretStore Container object. Each sssServerPolicyOverride object must take the name of the context that the Group or User objects are in.

The server servicing the replicas of that container should be configured to load with `/o=` option on the command line to use the override.object DN for the users in that container, as shown in the following example:

```
load sss /o=RSDev.digitalairlines.SecretStore.Security
```

This configuration permits the server to advertise itself to the root of the partition with the specified override.object DN. To minimize the amount of tree walking by the SecretStore client, you can define the sssServerPolicyOverrideDN attribute for individual users, organizational units, organizations, etc. This allows the SecretStore client to read this attribute, search the root of the partition for the server that supports that override configuration, then connect the user to the read/write replica for SecretStore access.

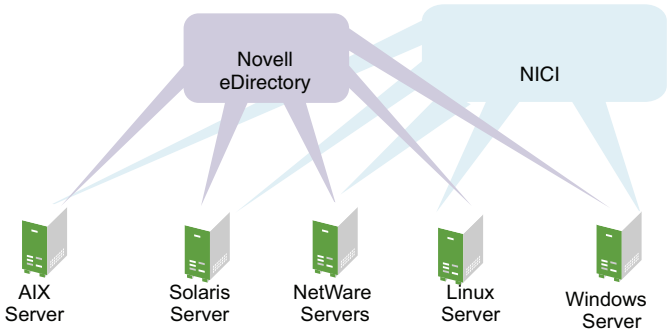
For more information on sssServerPolicyOverride objects, including how to create one, see “Creating an Override Object” on page 40.

1.3 How SecretStore Works

SecretStore 3.4.1 is supported eDirectory 8.8.4 and 8.8.5 running on AIX*, SUSE® Linux Enterprise Server (SLES) 32-bit and 64-bit, Solaris* 32-bit and 64-bit, and Windows Server* 32-bit and 64-bit.

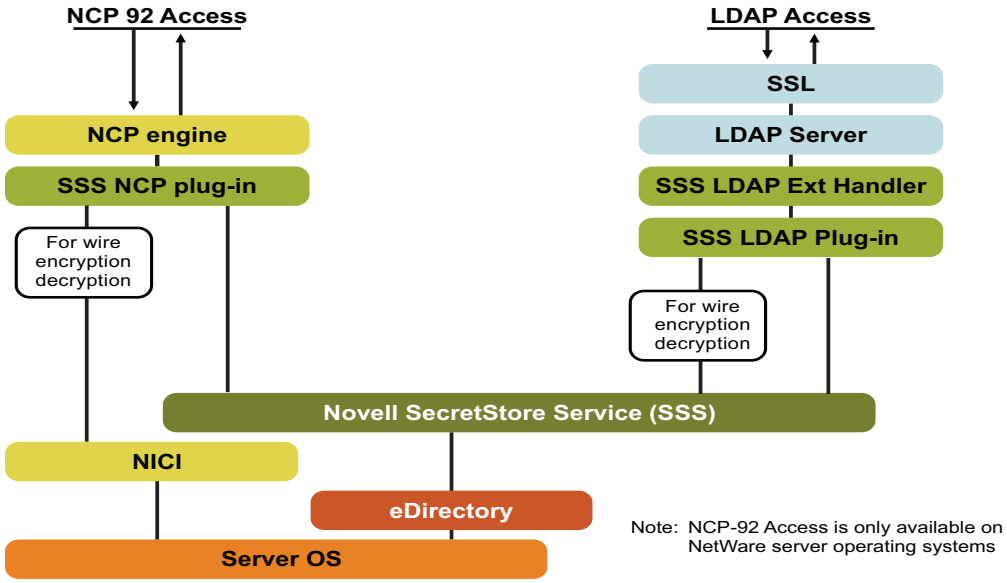
The SecretStore service is installed on the servers as a component of eDirectory. SecretStore runs on eDirectory and NICI, and the SecretStore Transport plug-ins run on SecretStore.

Figure 1-1 *Platforms that Support SecretStore*



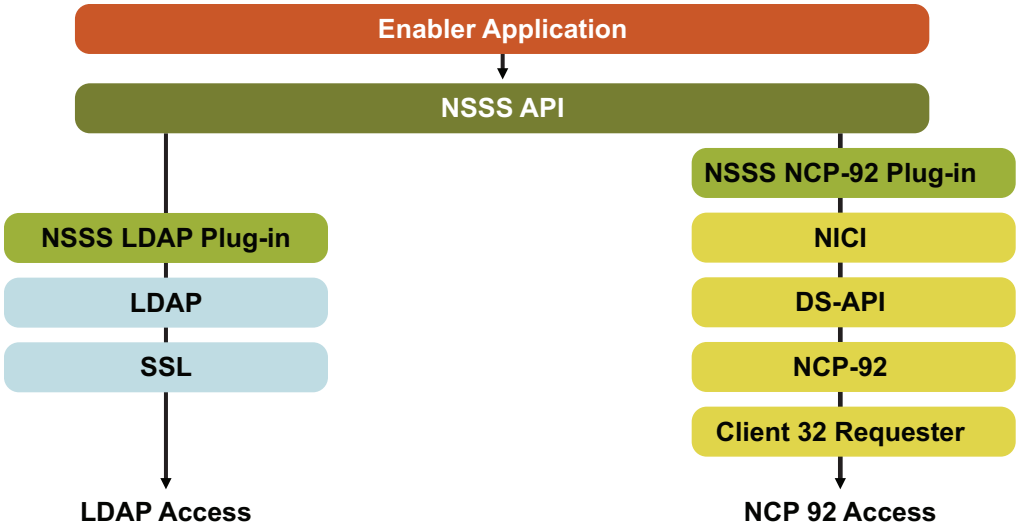
The following figure illustrates the server NCP and LDAP protocol stacks on a server platform:

Figure 1-2 *SecretStore, eDirectory and NICI, and Plug-ins*



The following figure illustrates the client NCP and LDAP protocol stacks on a client workstation:

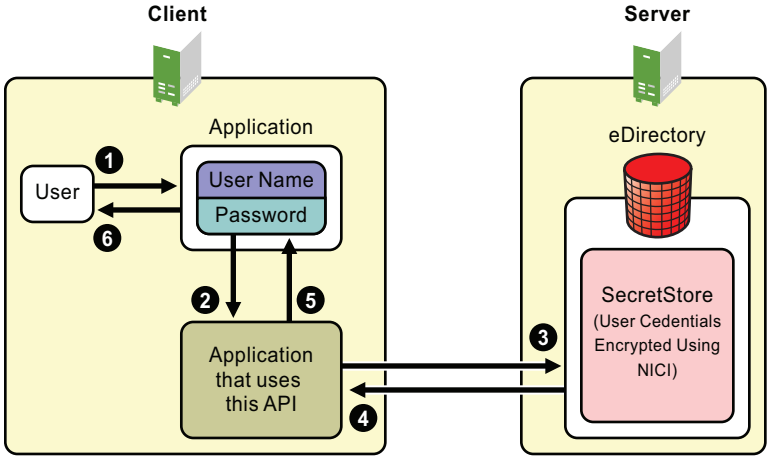
Figure 1-3 *Client NCP and LDAP Protocol Stacks*



NOTE: SecretStore plug-ins include client APIs, NCP, and an LDAP extension.

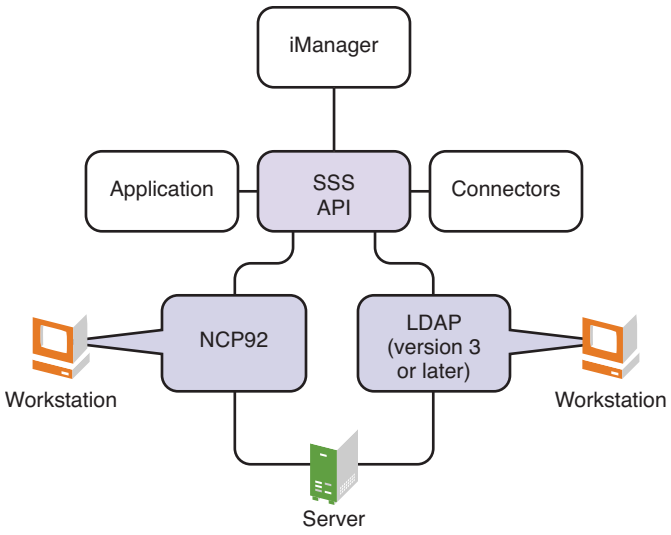
The following figure illustrates the SecretStore client and server architecture:

Figure 1-4 *SecretStore Client and Server Architecture*



The following figure illustrates client software running on a Windows workstation:

Figure 1-5 *SecretStore Components on a Windows Workstation*



The following steps illustrate how SecretStore works:

1. A user logs in to eDirectory by using a password or other login credential.
2. A successful login allows the user's secrets to be downloaded (when necessary) from SecretStore to the workstation.
3. The user accesses a client-based, Web-based, or host-based application. The connection recognizes the application and responds with the appropriate username and password from SecretStore.

   If the connection does not discover matching credentials, the application consuming the SecretStore client SDK prompts the user to add the application.

   credentials are provided which are stored using the writesecret api.

   for retrieving, when users launch the application, application uses ss api, it inturn talks to ss server, fetches the secrets readsecret api and provides.

1.3.1 Single Sign-On Authentication Process

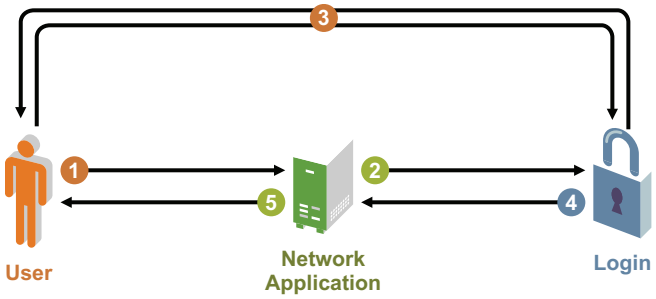
This section describes the process of single sign-on authentication and show how an enabled application can interface with SecretStore, read and write secrets, and authenticate the user.

- “Authentication without SecretStore” on page 15
- “Initial Authentication to a SecretStore-Enabled Application” on page 16
- “Subsequent Authentication to a SecretStore-Enabled Application” on page 16

Authentication without SecretStore

For purposes of comparison, the following figure illustrates how a user might authenticate to a network application that isn’t enabled for single sign-on.

Figure 1-6 *Successful Authentication Before Single Sign-On*

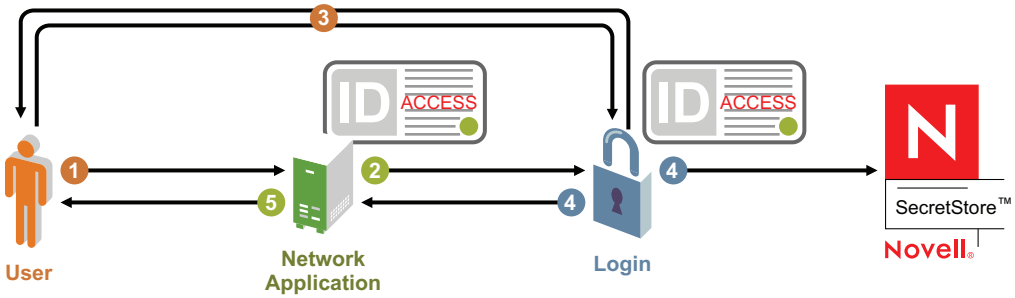


1. The user runs a network application.
2. The application calls the authentication module.
3. The module prompts the user to log in. The user submits credentials (for example, a user ID or smart card) and secrets (for example, a password or PIN), then authenticates.
4. The authentication module notifies the application that access has been granted.
5. The user starts interacting with the application.

Initial Authentication to a SecretStore-Enabled Application

The following figure illustrates the first-time authentication to an application that has been enabled for single sign-on with SecretStore.

Figure 1-7 *First-Time Authentication to Single Sign-On Enabled Application*

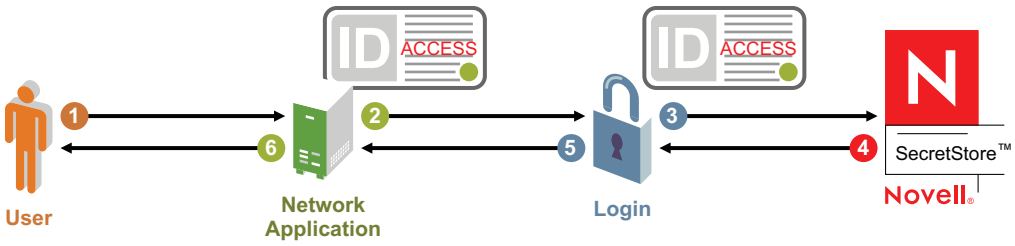


1. The user runs an enabled network application.
2. The application calls the authentication module.
3. The module prompts the user to log in. The user submits credentials (for example, a user ID or Smart Card) and secrets (for example, a password or PIN), then authenticates.
4. The authentication module updates Novell SecretStore with the user's verified authentication information.
5. The authentication module notifies the application that access has been granted.
6. The user starts interacting with the application.

Subsequent Authentication to a SecretStore-Enabled Application

The following figure illustrates the processes involved in subsequent user authentication to a single sign-on-enabled application using SecretStore.

Figure 1-8 *Subsequent User Authentication to a Single Sign-On Enabled Application*



1. The user starts interacting with the application.
2. The application calls the authentication module.
3. The authentication module calls Novell SecretStore to retrieve the user's authentication secrets.
4. Novell SecretStore returns the user's authentication secrets (identification, secrets, etc.) to the authentication module, and the user is authenticated.
5. The authentication module notifies the application that access has been granted.
6. The user runs a single sign-on-enabled network application.

Installing SecretStore

2

The Novell® SecretStore® service is installed as a component of eDirectory™ on NetWare® 6 or later, Windows Server platforms 32-bit and 64-bit, SLES 32-bit and 64-bit, Solaris 32-bit and 64-bit, or AIX servers, as described in the following sections:

After SecretStore is installed on the server, you use the SecretStore client installation program to install the SecretStore client components on your workstation. For more information, see Section 2.4, “Installing the SecretStore Client on Workstations,” on page 22.

A Novell eDirectory administrator should perform the server installation so that the schema is extended properly. Applications enabled for SecretStore ship SecretStore Service client components on their product CDs. You also can download the SecretStore client components from the Novell Developer Kit (NDK) Web site:

- Novell SecretStore Developer Kit for C (http://developer.novell.com/wiki/index.php/Novell_SecretStore_Developer_Kit_for_C)
- Novell SecretStore Developer Kit for Java (http://developer.novell.com/wiki/index.php/Novell_SecretStore_Developer_Kit_for_Java)

2.1 Installing SecretStore on a NetWare Server

2.1.1 NetWare Requirements

- ❑ NetWare 6.5.*x* server.
- ❑ Novell eDirectory.
- ❑ Security domain infrastructure.
- ❑ NICI 2.7.4 or later
- ❑ The latest support pack for your NetWare version.
- ❑ Supervisor rights to the eDirectory tree.
- ❑ The target server must have a read/write replica of the partition that contains the User objects for those who will use SecretStore.

2.1.2 SecretStore Service on NetWare

When you install eDirectory on NetWare, the SecretStore service is automatically installed.

In OES2 SP1 on NetWare 6.5 SP8, SecretStore is installed by default. However, it will not be configured. So, use the sssi.nlm tool to configure SecretStore on NetWare.

The mechanism that loads SecretStore is located in the `autoexec.ncf` file.

2.1.3 Synchronizing Replicas

Because NDS® or eDirectory replicas influence a SecretStore server's operations, make sure that the replicas are properly synchronized. For information on synchronizing replicas, see the *Network Time Management for NetWare Administration Guide* (http://www.novell.com/documentation/oes2/ntwk_timesync_nw/index.html?page=/documentation/oes2/ntwk_timesync_nw/data/hl5k6r0y.html#hl5k6r0y).

2.2 Installing SecretStore on a Windows Server

SecretStore is installed as part of eDirectory 8.8.*x* on Windows Server 32-bit and 64-bit platforms.

- Section 2.2.1, "Windows Server Requirements," on page 20
- Section 2.2.2, "Installing or Upgrading NICI," on page 20
- Section 2.2.3, "Synchronizing Replicas," on page 20

2.2.1 Windows Server Requirements

The Windows Server latest service pack must be installed.

NOTE: The server should have a read/write replica of the partition that contains the User object for all SecretStore users.

2.2.2 Installing or Upgrading NICI

eDirectory automatically installs and configures the latest NICI and SDI. If you need to upgrade NICI, get the version you need from Novell Product Downloads (http://download.novell.com/index.jsp).

2.2.3 Synchronizing Replicas

Because NDS or eDirectory replicas influence a SecretStore server's operations, make sure that the replicas are properly synchronized. For information on synchronizing replicas, see the *Network Time Management for NetWare Administration Guide* (http://www.novell.com/documentation/oes2/ntwk_timesync_nw/index.html?page=/documentation/oes2/ntwk_timesync_nw/data/hl5k6r0y.html#hl5k6r0y).

2.3 Installing SecretStore on a Solaris, SLES, or AIX Server

eDirectory automatically installs and configures the latest NICI and SDI.

2.3.1 Requirements

The following table lists the full system requirements and installation procedures on the server:

Table 2-1 *System Requirements*

Operating System	Documentation
Solaris	*Novell eDirectory 8.8 Installation Guide,* "Installing or Upgrading Novell eDirectory on Solaris" (http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/bs6kbsa.html)
SLES	*Novell eDirectory 8.8 Installation Guide,* "Installing or Upgrading Novell eDirectory on Linux" (http://www.novell.com/documentation/edir88/edirin88/data/bqs8nru.html)
AIX	*Novell eDirectory 8.8 Installation Guide,* "Installing or Upgrading Novell eDirectory on AIX" (http://www.novell.com/documentation/edir88/edirin88/data/ahna8sf.html).

2.3.2 SecretStore Service on Solaris, SLES, or AIX

SecretStore components are installed on all platforms with eDirectory 8.8.*x*.

Configuring SecretStore for Solaris, SLES, or AIX

To configure SecretStore for Solaris, SLES, AIX, use the ssscfg utility. At the command line, enter the following:

```
/usr/sbin/ssscfg [-h hostname[:port]] [-w password] [-a admin FDN] -c/d[-v] [-s schemafile]
```

Examples:

- To configure SecretStore after installing on SLES, enter

  ```
  ssscfg -h 137.65.159.160 -a admin.digitalairlines -c
  ```

- To deconfigure SecretStore, enter

  ```
  ssscfg -h 137.65.159.160 -a admin.digitalairlines -d
  ```

Parameter	Description
hostname/IP address	The hostname or IP address of the server on which Novell SecretStore server components must be configured.
port	(Optional) The NDS or eDirectory server port.
-w	The password that corresponds to *admin FDN*. If you enter the optional parameter at the command line, you won't be prompted for the password.
admin FDN	The fully distinguished name of the eDirectory administrator for the tree. Use the complete context (for example, admin.organizationalunit.organization).

Parameter	Description
-c	The configure command.
-d	The deconfigure command.
-v	Sets the verbose mode.
-s	Refers to the SecretStore schema file in eDirectory format (`ssv3.sch`). The schema file is installed as part of the SecretStore product installation.

2.3.3 Synchronizing Replicas

Because NDS or eDirectory replicas influence a SecretStore server's operations, make sure that the replicas are properly synchronized. For information on synchronizing replicas, see the Network Time Management for NetWare Administration Guide (http://www.novell.com/documentation/oes2/ntwk_timesync_nw/index.html?page=/documentation/oes2/ntwk_timesync_nw/data/hl5k6r0y.html#hl5k6r0y).

2.4 Installing the SecretStore Client on Workstations

If the product that you're installing SecretStore for doesn't include the SecretStore client components in its installation, you might need to use the SecretStore client installation described in this section.

- Section 2.4.1, "Workstation Requirements," on page 22
- Section 2.4.2, "Components," on page 22

2.4.1 Workstation Requirements

- ❑ A Windows XP/Vista 32-bit or 64-bit workstation used exclusively as a client workstation.

  You need to install the latest version of NICI on the workstation if it is not already present. You can download this product from the Novell Download Web site (http://download.novell.com/index.jsp).
- ❑ Supervisor rights to the NDS or eDirectory tree

  This requirement only applies to administrative workstations.

2.4.2 Components

You can administer SecretStore from your workstation by installing the following components there:

- SecretStore client
- NICI client
- iManager
- The SecretStore plug-in to iManager

Consider the following guidelines concerning users:

- To prevent users from getting prompted for passwords, don't install NMAS™ on users' workstations.
- Use Novell ZENworks® to distribute SecretStore to users' workstations.

- "Installing the SecretStore Plug-In to iManager" on page 23
- "Installing the SecretStore Client" on page 23
- "SecretStore Diagnostic Logging" on page 24

Installing the SecretStore Plug-In to iManager

You administer SecretStore through iManager and the SecretStore plug-in to iManager.

To install the SecretStore plug-in to iManager:

1. In iManager, in the *Configure* view, click *iManager Server* > *Configure iManager*.
2. Click *Plug-in Download*.
3. Ensure the *Query Novell download site for new Novell Plug-in Modules (NPM)* option is selected.
4. Select *Show every available Novell Plug-in Module (NPM)*, then click *Save* > *Close*.
5. In the *Configure* view, click *Plug-in Installation* > *Available Novell Plug-in Modules*.

   A list of available Novell plug-in modules is displayed. For example, the iManager 2.7 SecretStore plugin *Novell Identity Manager - Secret Store Administr*
6. Select the *SecretStore* plug-in, then click *Install*.
7. Follow the on-screen instructions.

Installing the SecretStore Client

SecretStore supports several products. You can adapt the following steps to your product:

1. Download the client install from the Novell NDK Web site (http://developer.novell.com).

   NOTE: The client is available for Windows only.
2. Run the `platform relative msi` file from the download directory.
3. Follow the on-screen prompts.

The SecretStore client still delivers a copy of the legacy client `nwsso.dll` for backward compatibility with existing applications and connectors. You can download the latest copy of this file from the Novell Developer Kit Web site (http://developer.novell.com/wiki/index.php/Novell_SecretStore_Developer_Kit_for_C). This legacy client operates in parallel with the new SecretStore client on the same workstation.

Client32™ and NMAS installations automatically install `nwsso.dll`. However, if you need to manually install `nwsso.dll`, place it in the `Windows\System32` directory.

SecretStore Diagnostic Logging

`Nwsso.dll` also has been retrofitted to provide diagnostic logging for troubleshooting problems. The following registry key files allow the user to enable and disable logging by double-clicking on the file from Windows Explorer:

- `EnableNWSSOLogger.reg`
- `DisableNWSSOLogger.reg`

Enabling logging produces an `nwsso.log` file at the root of the current working directory (that is, from where the SecretStore client application is using the `nwsso.dll` file). New entries are added to the existing log until the file is deleted (resulting in the start of a new file) or upon disabling the logging feature.

The SecretStore client also can produce diagnostic logs similar to the legacy client by using the following registry key files:

- `Nsss.dll` high-level client logging:
  - Enable `NSSSLogger.reg`
  - Disable `NSSSLogger.reg`
- `Nssncp.dll` lower-level client NCP™ protocol logging:
  - Enable `NSSNCPLogger.reg`
  - Disable `NSSNCPLogger.reg`
- `Nssldp.dll` lower-level client LDAP protocol logging:
  - Enable `NSSLDPLogger.reg`
  - Disable `NSSLDPLogger.reg`

2.5 Uninstalling the SecretStore Client

The SecretStore Client is only for Windows. To uninstall the SecretStore client, use *Add\Remove Programs* in the Control Panel.

Installing and Activating Novell Audit

3

This section contains instructions for installing and activating Novell Audit on each supported platform.

3.1 Installing on NetWare

Novell Audit can be installed on NetWare® 6.5 SP5 or OES 2.0 SP1 (NetWare kernel).

IMPORTANT: When you install the full version of Novell Audit, the license file (`*.nlf`) 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 Novell Audit Starter Pack, the product is not licensed and you have only limited functionality. If you want to upgrade to the full version, you must purchase a product license. For more information on activating the full version of Novell Audit, see Section 3.5, “Activating Novell Audit,” on page 36.

To install Novell Audit on NetWare:

1. On the NetWare server, insert, and if necessary, mount the Novell Audit installation CD.
2. Load `nwconfig.nlm` at the server console.
3. In NWConfig, select *Product Options* > *Install a Product Not Listed*.
4. 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.
5. Select your install options.

   Unlike previous versions of Novell Audit, the installation options are not specific to new or upgrade installations. For a complete first-time or upgrade installation, we recommend you select all the options.

   The installation options are outlined in the following table.

Option	Description
Install Novell Audit Instrumentation Agents	Installs the NetWare Instrumentation (`auditNW.nlm`) and the eDirectory™ Instrumentation (`auditDS.nlm`). These instrumentations must be installed on any NetWare server that you want to report eDirectory, file system, or NetWare events. This option automatically installs the Platform Agent, regardless of whether the Platform Agent option is selected.
Install Novell Audit Platform Agent	Installs the Novell Audit Platform Agent (`logevent.nlm`) and adds `auditagt.ncf` to the `autoexec.ncf` file. The Platform Agent must be installed on any NetWare server that you want to report events.
Novell Audit Secure Logging Server	Installs the Novell Audit Secure Logging Server (`lengine.nlm`), the Novell Audit Instrumentation Agents (`auditNW.nlm` and `auditDS.nlm`), the Platform Agent (`logevent.nlm`), the Log Parser (`logparse.nlm`), and adds the Novell Audit 2.0 schema extensions to eDirectory. It also adds `auditsvr.ncf` and `auditagt.ncf` to the `autoexec.ncf` file. The Secure Logging Server securely receives reported events. **NOTE:** If you want more than one Secure Logging Server in the tree, we recommend that you create separate eDirectory organizational units as containers for each Secure Logging Server's configuration objects.
Add Schema Extensions	Adds the Novell Audit schema extensions to eDirectory. **NOTE:** If you select only this option, you are automatically exited from the installer after the eDirectory schema is extended.

6 Press F10 to continue.

7 Accept the License Agreement.

8 To add the Novell Audit schema extensions, enter the user name and password of an administrator with rights to the root of the eDirectory tree. This logs you into the AuditExt utility.

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

9 After logging in to AuditExt, select from the following options:

AuditExt Options	Action
Add Schema Extensions	Adds the Novell Audit 2.0 schema objects. **IMPORTANT:** This does not destroy or overwrite any objects in your current eDirectory tree.

AuditExt Options	Action
Remove Schema Extensions	Removes all Novell Audit schema extensions from the eDirectory tree. This option is required to uninstall Novell Audit. **WARNING:** This option deletes all existing Novell Audit objects from eDirectory.
Configure This Server	Configures the Secure Logging Server. Depending on the installation, it performs one of the following actions: ◆ For a new installation, it creates the Secure Logging Server object in Logging Services, creates a File Channel object in the Logging Services Channel container, and configures the Secure Logging Server to log events to the File channel. It also creates a Monitor channel for iManager. ◆ For an upgrade installation, it upgrades the Novell Audit 1.0.3 objects to the Novell Audit 2.0 schema. If you choose to configure the Secure Logging Server, you are prompted as follows: 1. AuditExt automatically creates the Secure Logging Server name as "*server_name* Logging Server." 2. Choose if you want to create all Novell Audit objects in the Logging Services container. **NOTE:** Logging Services is the default container for all Novell Audit objects in eDirectory. If you select *No*, you must provide the name of an existing organizational unit in which AuditExt can create the Secure Logging Server and its associated objects. 3. When you're finished, press Esc, then click *Yes*.
Exit AuditExt	Closes the AuditExt utility.

10 When finished, select *Exit AuditExt*, then click *Yes*.

11 Choose if you want to start the Secure Logging Server now.

If you select *Yes*, the installer loads the Secure Logging Server. It does not reboot the server.

To manually load the Secure Logging Server, enter

```
load lengine
```

or

```
load auditsvr.ncf
```

If you want to prevent the Secure Logging Server from being unloaded by users with access to the server console, you can append the `-n` switch to the server startup script. (For example, `load lengine -n`.)

12 Choose if you want to start logging eDirectory and NetWare events now.

If you select *Yes*, the installer loads the instrumentations and the Platform Agent.

To manually start the NetWare or eDirectory Instrumentation on NetWare, enter

```
load auditnw
```

or

```
load auditDS
```

To load both the NetWare and eDirectory Instrumentations, enter

```
load auditagt.ncf
```

`Auditnw.nlm`, `audit.ds`, and `auditagt.ncf` are located in the `sys:\system` directory.

13 Press Enter to complete the installation.

14 After you install Novell Audit, iManager 2.0 or above detects that you have a new plug-in and prompts you to install it.

3.2 Installing on Linux

Novell Audit 2.0 can be installed on SUSE® Linux Enterprise Server 9 or Red Hat Linux AS and ES (3 and 4).

IMPORTANT: When you install the full version of Novell Audit, the license file (`*.nlf`) 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 Novell Audit Starter Pack, the product is not licensed and you have only limited functionality. If you want to upgrade to the full version, you must purchase a product license. For more information on activating the full version of Novell Audit, see Section 3.5, "Activating Novell Audit," on page 36.

To install Novell Audit on Linux:

1 Log in as root on the host.

2 Enter the following commands at the Linux console to mount the Novell Audit installation CD and go to the setup directory for the Novell Audit Linux install:

Operating System	Commands
SUSE	`mount /media/cdrom`
	`cd /media/cdrom/Linux`
Red Hat	`mount /mnt/cdrom`
	`cd /mnt/cdrom/Linux`

3 From the setup directory for the Novell Audit Linux install, enter the following command at the Linux console to begin the installation:

```
./pinstall.lin
```

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 Accept the license agreement.

5 Select your install options.

Option	Description
Platform Agent	Installs the Novell Audit Platform Agent (`liblogevent.so`) and the Log Parser (`logparse`). The Platform Agent must be installed on any server that you want to report events.
eDirectory Instrumentation Files with Platform Agent	Installs the eDirectory Instrumentation (`libauditDS.so`), the Platform Agent (`liblogevent.so`), and the Log Parser (`logparse`). The eDirectory instrumentation must be installed on any server that you want to report eDirectory events. This option automatically installs the Platform Agent, regardless of whether the Platform Agent option is selected.
Extend Schema	Adds the Novell Audit schema extensions to eDirectory. **NOTE:** If you select only this option, you are returned to the Linux console after the eDirectory schema is extended.
Novell Audit Secure Logging Server	Installs the Novell Audit Secure Logging Server (`lengine`), the Novell Audit eDirectory Instrumentation (`libauditDS.so`), the Platform Agent (`liblogevent.so`), the Log Parser (`logparse`), and adds the Novell Audit 2.0 schema extensions to eDirectory. The Secure Logging Server securely receives reported events. **NOTE:** If you want more than one Secure Logging Server in the tree, we recommend that you create separate eDirectory organizational units as containers for each Secure Logging Server's configuration objects.

6 To add the Novell Audit schema extensions, enter the user name and password of an administrator with rights to the root of the eDirectory tree. This logs you into the AuditExt utility.

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

7 After logging in to AuditExt, select from the following options:

AuditExt Options	Action
Add Schema Extensions	Adds the Novell Audit 2.0 schema objects. **IMPORTANT:** This does not destroy or overwrite any objects in your current eDirectory tree.

AuditExt Options	Action
Remove Schema Extensions	Removes all Novell Audit schema extensions from the eDirectory tree. This option is required to uninstall Novell Audit. **WARNING:** This option deletes all existing Novell Audit objects from eDirectory.
Configure This Server	Configures the Secure Logging Server. Depending on the installation, it performs one of the following actions: ◆ For a new installation, it creates the Secure Logging Server object in Logging Services, creates a File Channel object in the Logging Services Channel container, and configures the Secure Logging Server to log events to the File channel. It also creates a Monitor channel for iManager. ◆ For an upgrade installation, it upgrades the Novell Audit 1.0.3 objects to the Novell Audit 2.0 schema. If you choose to configure the Secure Logging Server, you are prompted as follows: 1. AuditExt automatically creates the Secure Logging Server name as "*server_name* Logging Server." 2. Choose if you want to create all Novell Audit objects in the Logging Services container. **NOTE:** Logging Services is the default container for all Novell Audit objects in eDirectory. If you select *No*, you must provide the name of an existing organizational unit in which AuditExt can create the Secure Logging Server and its associated objects. 3. When you're finished, press Esc, then click *Yes*.
Exit AuditExt	Closes the AuditExt utility.

8 When finished, select *Exit AuditExt*.

9 When the installation is complete, the Secure Logging Server automatically launches.

10 Choose if you want to load the Platform Agent.

11 If you select *Yes*, you are asked if you want to overwrite the pre-existing Platform Agent configuration file (`logevent.conf`).

12 Choose if you want to load the eDirectory Instrumentation.

Novell Audit adds the following command to the `ndsmodules.conf` file to automatically load the eDirectory Instrumentation with eDirectory:

```
auditDS auto #NSure Audit Platform Agent
```

NOTE: On eDirectory 8.7, the path to the `ndsmodules.conf` file is /usr/lib/nds-modules/ndsmodules.conf. On eDirectory 8.8, the path is `/etc/opt/novell/eDirectory/nds-modules/ndsmodules.conf`.

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

To manually start the eDirectory instrumentation, enter:

```
ndstrace -c "load auditDS"
```

13 After you install Novell Audit, iManager 2.0 or above detects that you have a new plug-in and prompts you to install it.

3.3 Installing on Solaris

Novell Audit 2.0 can be installed on Solaris 8, 9, and 10.

Solaris 8 requires GCC 3.3 and zlib 1.2.3 to function as a Secure Logging Server. Without GCC3.3, applications fail to authenticate to the logging server. The resulting error in `nproduct.log` is `Failed SSL Handshake`.

IMPORTANT: When you install the full version of Novell Audit, the license file (`*.nlf`) 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 Novell Audit Starter Pack, the product is not licensed and you have only limited functionality. If you want to upgrade to the full version, you must purchase a product license. For more information on activating the full version of Novell Audit, see Section 3.5, "Activating Novell Audit," on page 36.

To install Novell Audit on Solaris:

1 Log in as root on the host.

2 Insert the CD into the drive.

If the Volume Manager (`vold`) is running on your system, the CD is automatically mounted as `/cdrom/CDROM`.

3 (Optional) If the Volume Manager is not running on your system, complete the following steps to mount the CD:

3a Determine the name of the device by entering the following command:

```
ls -al /dev/sr* |awk '{print "/" $11}'
```

3b Enter the following commands to mount the CD-ROM:

```
mkdir -p /cdrom/CDROM
     mount -F hsfs -o ro device_name /cdrom/CDROM
```

4 Enter the following command to go to the directory for the Novell Audit Solaris install:

```
cd /cdrom/CDROM/Solaris
```

5 From the setup directory for the Novell Audit Solaris install, enter the following command at the Solaris console to begin the installation:

```
./pinstall.sol
```

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.sol`.

6 Accept the license agreement.

7 Select your install options.

Option	Description
Platform Agent	Installs the Novell Audit Platform Agent (`liblogevent.so`) and the Log Parser (`logparse`). The Platform Agent must be installed on any server that you want to report events.
eDirectory Instrumentation Files with Platform Agent	Installs the eDirectory Instrumentation (`libauditDS.so`), the Platform Agent (`liblogevent.so`), and the Log Parser (`logparse`). The eDirectory instrumentation must be installed on any server that you want to report eDirectory events. This option automatically installs the Platform Agent, regardless of whether the Platform Agent option is selected.
Extend Schema	Adds the Novell Audit schema extensions to eDirectory. **NOTE:** If you select only this option, you are returned to the Linux console after the eDirectory schema is extended.
Novell Audit Secure Logging Server	Installs the Novell Audit Secure Logging Server (`lengine`), the Novell Audit eDirectory Instrumentation (`libauditDS.so`), the Platform Agent (`liblogevent.so`), the Log Parser (`logparse`), and adds the Novell Audit 2.0 schema extensions to eDirectory. The Secure Logging Server securely receives reported events. **NOTE:** If you want more than one Secure Logging Server in the tree, we recommend that you create separate eDirectory organizational units as containers for each Secure Logging Server's configuration objects.

8 To add the Novell Audit schema extensions, enter the user name and password of an administrator with rights to the root of the eDirectory tree. This logs you into the AuditExt utility.

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

9 After logging in to AuditExt, select from the following options:

AuditExt Options	Action
Add Schema Extensions	Adds the Novell Audit 2.0 schema objects. **IMPORTANT:** This does not destroy or overwrite any objects in your current eDirectory tree.

AuditExt Options	Action
Remove Schema Extensions	Removes all Novell Audit schema extensions from the eDirectory tree. This option is required to uninstall Novell Audit. **WARNING:** This option deletes all existing Novell Audit objects from eDirectory.
Configure This Server	Configures the Secure Logging Server. Depending on the installation, it performs one of the following actions: ◆ For a new installation, it creates the Secure Logging Server object in Logging Services, creates a File Channel object in the Logging Services Channel container, and configures the Secure Logging Server to log events to the File channel. It also creates a Monitor channel for iManager. ◆ For an upgrade installation, it upgrades the Novell Audit 1.0.3 objects to the Novell Audit 2.0 schema. If you choose to configure the Secure Logging Server, you are prompted as follows: 1. AuditExt automatically creates the Secure Logging Server name as "*server_name* Logging Server." 2. Choose if you want to create all Novell Audit objects in the Logging Services container. **NOTE:** Logging Services is the default container for all Novell Audit objects in eDirectory. If you select *No*, you must provide the name of an existing organizational unit in which AuditExt can create the Secure Logging Server and its associated objects. 3. When you're finished, press Esc, then click *Yes*.
Exit AuditExt	Closes the AuditExt utility.

10 When finished, select *Exit AuditExt*.

11 When the installation is complete, the Secure Logging Server automatically launches.

12 Choose if you want to load the Platform Agent.

13 If you select *Yes*, you are asked if you want to overwrite the pre-existing Platform Agent configuration file (`logevent.conf`).

14 Choose if you want to load the eDirectory Instrumentation.

Novell Audit adds the following command to the `ndsmodules.conf` file to automatically load the eDirectory Instrumentation with eDirectory:

```
auditDS auto #NSure Audit Platform Agent
```

NOTE: On eDirectory 8.7, the path to the `ndsmodules.conf` file is /usr/lib/nds-modules/ndsmodules.conf. On eDirectory 8.8, the path is `/etc/opt/novell/eDirectory/nds-modules/ndsmodules.conf`.

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

To manually start the eDirectory instrumentation, enter:

```
ndstrace -c "load auditDS"
```

15 After you install Novell Audit, iManager 2.0 or above detects that you have a new plug-in and prompts you to install it.

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"
```

3.4 Installing on Windows

The Novell Audit Secure Logging Server can be installed on Windows 2000 and 2003 Server. The Platform Agent and instrumentations can be installed on Windows 2000 and Windows 2000 Server, Windows XP Professional and Home Editions, and Windows 2003 Server.

IMPORTANT: When you install the full version of Novell Audit, the license file (`*.nlf`) 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 Novell Audit Starter Pack, the product is not licensed and you have only limited functionality. If you want to upgrade to the full version, you must purchase a product license. For more information on activating the full version of Novell Audit, see Section 3.5, "Activating Novell Audit," on page 36.

To install Novell Audit on Windows:

1 At the Windows server, log in as Administrator or a user with administrative privileges.

2 Insert the Novell Audit installation CD.

The auto install launches.

3 Accept the license agreements.

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*.

Installation Option	Description
Custom	Allows you to individually select which program components to install. When you select individual program components, the installer automatically selects your dependencies. **IMPORTANT:** For upgrades, the installer automatically installs all channels; you cannot install only specific channels.
Extend Schema	Adds the Novell Audit 2.0 schema objects. **IMPORTANT:** This does not destroy or overwrite any objects in your current eDirectory tree.
Full Installation	Installs the Secure Logging Server (`lengine.exe`), all channel drivers (`lgd*.dll`), the Platform Agent (`logevent.dll`), the eDirectory instrumentation (`auditDS.dlm`), the Windows Instrumentation (`nauditwin.exe`), Novell Audit Report (`lreport.exe`), and the Log Parser (`logparse.exe`).
Instrumentation	Installs the Platform Agent, the eDirectory and Windows instrumentations, and the Log Parser (`logparse.exe`).
Platform Agent	Installs only the Platform Agent (`logevent.dll`).
Reporting Application	Installs only Novell Audit Report (`lreport.exe`).
Server	Installs the Secure Logging Server (`lengine.exe`), all channel drivers (`lgd*.dll`), the Platform Agent (`logevent.dll`), the eDirectory instrumentation (`auditDS.dlm`), the Windows Instrumentation (`nauditwin.exe`), and the Log Parser (`logparse.exe`).

The Custom, Full Installation, and Server options create the Secure Logging Server object in the Logging Services container. 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.

NOTE: If you want more than one Secure Logging Server in the tree, we recommend that you create separate eDirectory organizational units as containers for each Secure Logging Server's configuration objects.

7. (Optional) If you are installing the Platform Agent, specify the IP address of the Secure Logging Server.
8. Confirm your settings, then click *Next*.
9. Verify the location of eDirectory.

   The default location is *`drive`*`:\novell\nds`.
10. (Optional) If you are installing the Secure Logging Server, provide the following information when prompted:

    10a 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.

    10b Specify a name for the Secure Logging Server object.

    10c Select *Yes* or *No* to create all Novell Audit objects in the Logging Services container.

Logging Services is the default container for all Novell Audit objects in eDirectory.

If you select *No*, you must provide the name of an existing organizational unit in which AuditExt can create the Secure Logging Server and its associated objects.

11 Click *OK* to complete the installation.

12 Select *Yes* or *No* to reboot the server now.

You must reboot the server to load Novell Audit.

13 Click *Finish*.

When the server reboots, the Secure Logging Server automatically launches (the Startup Type for the Secure Logging Server Service is Automatic); however, you must manually load the eDirectory Instrumentation.

To load the Windows Instrumentation:

1 Go to *Control Panel* > *Administrative Tools* > *Services*.

2 Select the Novell Audit Windows Instrumentation.

3 Right-click and select *Properties*.

4 In the Properties dialog box, start the Novell Audit Windows Instrumentation Service:

4a To automatically load the Novell Audit Windows Instrumentation each time the server restarts, select *Automatic* in the *Startup type* drop-down list.

4b To manually load the Novell Audit Windows Instrumentation, click *Start*.

5 When finished, click *OK*.

To manually load or unload the eDirectory instrumentation:

1 Load `ndscons.exe`.

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

2 In the list of installed services, select *Novell 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 Audit Component*.

3 Click *Startup*.

4 Select the *Automatic* startup type and click *OK*.

On Windows, if you choose to only extend the schema, it automatically exits you from the installer; however, a Novell Audit entry is created in the Add/Remove Programs menu. To install, go to *Add Programs* and click *Modify* to launch the installer.

3.5 Activating Novell Audit

When you install the full version of Novell 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 Novell 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 Novell Audit Starter Pack is a scaled down version of Novell 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 Novell 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 to upgrade from the Novell Audit Starter Pack to the full version, you receive a license file with an `.nlf` extension. To activate the full version of Novell 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 3-1 *Default lengine Directory*

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

After you copy the license file to the `lengine` directory, you must restart the logging server.

3.6 Activating Novell Audit Report

To activate Novell Audit Report (`lreport`):

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

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

For the latest updates to Novell Audit documentation, refer the Novell Audit Documentation Web site. (http://www.novell.com/documentation/novellaudit20/index.html)

Managing SecretStore

4

This section provides information on the following:

4.1 Managing SecretStore Objects

This section provides information on the following:

4.1.1 SecretStore Objects

When you install the Novell® SecretStore® service on the server, the installation program automatically does the following:

- Creates an sssServerPolicy object.
- Places this object in the Security container.
- Assigns the name SecretStore to the object.

This object contains default settings for all users in the tree. You can customize security requirements for groups or users by creating sssServerPolicyOverride objects. The objects reside in the SecretStore (sssServerPolicy) container.

The SecretStore service first locates the sssServerPolicy object and then locates and uses an sssServerPolicyOverride object (if one exists). For more information on the sssServerPolicyOverride objects, see Section 1.2.2, “sssServerPolicyOverride Object,” on page 12.

For information on how to create an sssServerPolicyOverride object, see “Creating an Override Object” on page 40.

4.1.2 Viewing and Changing Settings on Objects

Settings or policies determine SecretStore behavior in eDirectory™.

To view settings for SecretStore objects:

1. In iManager, in the *Roles and Tasks* view, click *SecretStore* > *Modify Policy*.
2. Browse for and select the sssServerPolicy or an sssServerPolicyOverride object

3 Click *OK*.

4 Click the *General* tab.

- "Setting Minutes between Cache Refresh" on page 40
- "Updating the Time Stamp" on page 40
- "Disabling Master Password Operations" on page 40

Setting Minutes between Cache Refresh

The SecretStore service caches some application-specific settings, such as those needed for NMAS™, to enforce Graded Authentication on ReadSecret operations. This cache helps the service respond to requests more quickly. The default is 30 minutes between refreshes of the server cache. The minimum is 30 minutes (1/2 hour). The maximum is 1,440 minutes (24 hours).

Consider increasing the time for the following situations:

- You don't make frequent changes to the policies that SecretStore uses.
- Taking longer for SecretStore to enforce changes doesn't matter.
- You want to decrease the small overhead of refreshing data in the cache.

If you need to immediately update the cache, unload and reload the SecretStore service.

Updating the Time Stamp

To have the SecretStore service record time stamp information on all ReadSecret operations, select *Update timestamp on read secret*.

By default, the SecretStore service doesn't update the time stamp. If you want to update the time stamp when a secret is read, select the check box. Every read then becomes a write. Updating requires more time.

Disabling Master Password Operations

To disallow all Enhanced Protection Master Password options, select *Disable master password operations*. When this option is selected, users can't set or use a master password to unlock SecretStore.

4.1.3 Customizing Settings for Groups or Users

You can customize settings (for example, security requirements) for groups or users. You provide customized settings by creating and configuring an sssServerPolicyOverride object. When an override object exists, the SecretStore service first identifies settings in the sssServerPolicy object and then uses the customized settings in the sssServerPolicyOverride object.

You create sssServerPolicyOverride objects in the SecretStore (sssServerPolicies) container.

- "Creating an Override Object" on page 40
- "Customizing Security Throughout the Tree" on page 41

Creating an Override Object

1 In iManager, in the *Roles and Tasks* view, click *SecretStore* > *Create Override Policy*.

2 In the *Policy name* field, specify a name for the new override policy.

3 In the *Container name* field, specify or browse to and select the object where you want to create the override policy.

When you assign a policy to a User, the override settings take effect for that User only. When you assign a policy to a container, the override settings take effect for all objects in and below that container.

As a rule, set high-security policies (for example, biomentrics plus passwords) as defaults on the SecretStore object in the Security container. Set lower-priority policies on Policy Override objects.

4 Click *OK*.

After you verify that iManager created the override policy, click *OK*, or click *Repeat Task* to create a new override policy.

Customizing Security Throughout the Tree

Each User or Container object can have an sssServerPolicyOverrideDn attribute that points to a particular sssServerPolicyOverride object. This attribute enables SecretStore to provide customized security for specific users located in various places in the eDirectory tree.

SssServerPolicyOverride objects override default settings found in the sssServerPolicies (SecretStore) object. These override objects can be children of sssServerPolicies, Organization, Organizational Unit, Country, Locality, or domain objects.

You should set the high-security policies (for example, biometrics plus passwords if NMAS is installed) as defaults on the SecretStore object in the Security container. Set lower-priority policies on sssServerPolicyOverride objects, found in the SecretStore container.

If the single sign-on client can't find the SecretStore server that supports override objects, the client searches for any server that supports the default settings found in the SecretStore object.

To provide override policies:

1 Load `sss.nlm` with `-o` *`complete distinguished name of the override object`*.

For example, enter sss `-o 2003specs.develop.digitalairlines`.

A SecretStore server must support the override object. The -o 2003specs.develop.digitalairlines parameter specifies the distinguished name of the sssServerPolicyOverride object. You load this flag so that users have access to customized settings in the override object.

When users use an override object, all user workstation requests go to that server. This feature provides load balancing.

2 In iManager, in the *Roles and Tasks* view, click *SecretStore* > *Assign Policy*.

3 Choose the User or Container object, then select *OK*.

If the override applies to all users in the container, select the Container object.

4 Browse to the desired sssServerPolicyOverride object, select the object, then click *OK*.

The sssServerPolicyOverride object is in the SecretStore (sssServerPolicy) container.

This step points the User (or containers) to the sssServerPolicyOverride object by setting the user's (or container's) sssServerPolicyOverrideDn attribute.

Scenario. Ming and Claire are in the RSDev.digitalairlines context. Markus and Rie are in the design.digitalairlines context. You want all four users to have security options provided in the sssServerPolicyOverride object named 2003SPECS.

You select Ming's User object and then browse to and select 2003SSPECS. You repeat this process for Claire, Markus, and Rie. You load a server with the command line information so that these four users have access to the customized settings in 2003SPECS.

4.2 Setting Up a SecretStore Administrator

A user's SecretStore is locked when either of the following occur:

- Enhanced protection is enabled.
- A network administrator changes a user's eDirectory password.

A SecretStore administrator can unlock locked SecretStores.

However, although the SecretStore administrator can unlock a user's SecretStore, that administrator can't read the user's passwords. Unlocking a user's SecretStore only lets the logged-in user regain access to passwords after a SecretStore lock.

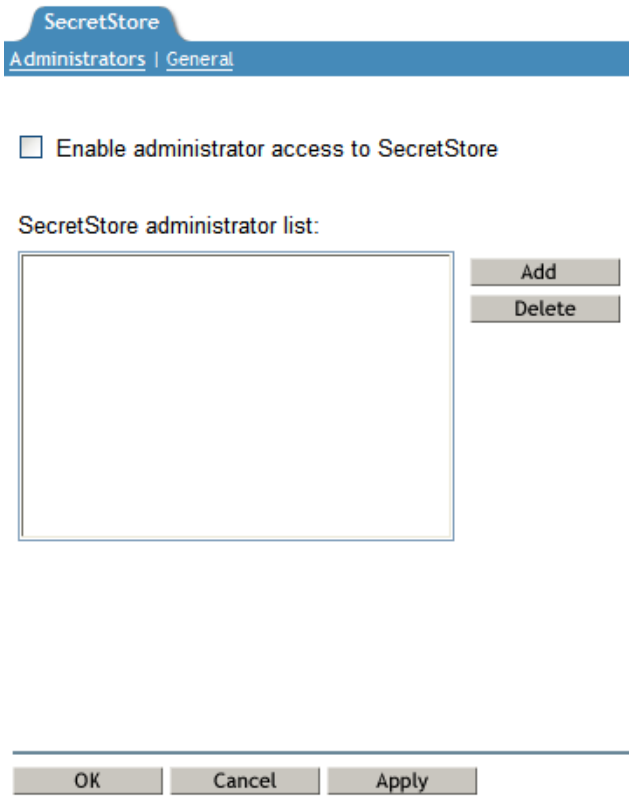
To avoid bypassing enhanced protection, designate two administrators (one eDirectory administrator, one SecretStore administrator).

A SecretStore administrator should not have "normal" network administrator rights. Limiting these rights prevents the administrator from resetting the user's password (as admin), unlocking the user's SecretStore (as SecretStore administrator), logging in as the user (with the reset password), and reading secrets.

To designate a SecretStore administrator, add that user's User object to the SecretStore Administrator List:

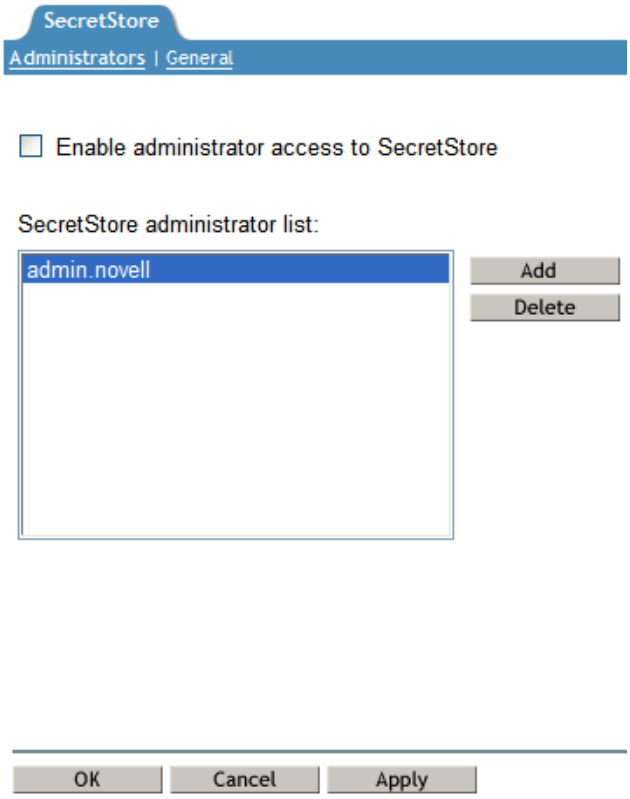
1. In iManager, in the *Roles and Tasks* view, click *SecretStore* > *Modify Policy*.
2. In the *Object name* field, browse to a SecretStore.Security object or an sssServerPolicyOverride object, then click *OK*.

   The installation program automatically creates the sssServerPolicy object (SecretStore.Security).
3. Click *Administrators*.



4 Click *Add*, navigate to and click the desired User object, click *Select*, then click *OK*.

The following figure illustrates the SecretStore Administrator List:



To grant an administrator access to SecretStore, select the *Enable administrator access to SecretStore* check box. If you add additional administrators, the setting still remains disabled until you select the check box.

Therefore, if you add additional SecretStore administrators, make sure that *Enable Administrator Access* to SecretStore is checked. Then the selected SecretStore administrator can unlock a user's SecretStore. This is useful when a user forgets a password.

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

The user is now a SecretStore Administrator.

4.2.1 Adding Advanced Security

SecretStore administrators can unlock a user's SecretStore. To prevent these administrators from misusing this option, we recommend that you use NMAS and specify a strong security label.

If Novell Modular Authentication Service (NMAS) is installed, a Security Label box displays on the SecretStore\Administrator page. This box contains the available security labels as defined by the NMAS snap in. By selecting a label, you designate the level of security that you prefer. This option enables you to increase the security regarding SecretStore administrators.

After you define a security label on the sssServerPolicy object, a SecretStore Administrator must be logged in with a session clearance that is equal to or greater than the security label. Otherwise, that Administrator can't unlock any user's SecretStore.

4.3 Sharing Secrets

Applications and software solutions can share secrets. For example, after you configure a Web site for SecureLogin, Novell Portal Services (NPS) can use the secrets in eDirectory to access that Web site.

In addition, when you change a password in either SecureLogin or NPS, the other software service recognizes and uses that changed password.

So that SecureLogin, NPS, and iChain® can share a secret for an application, provide a common name for that application. Then refer to that common name when configuring the application for SecureLogin, iChain, or an NPS gadget.

4.3.1 Example Configuration: Sharing Secrets with Novell Products

This example uses GroupWise® to explain how secrets are shared among SecureLogin, Portal Services, and iChain.

1. Set up NPS to use SecretStore.

   Make sure that NICI 2.04 or later is installed on the workstation.

   Configure SecretStore as an NPS SecretStore provider, and configure shared secrets for gadget instances.
2. Using the SecureLogin Wizard, set up `groupwise.exe` to use SecureLogin.
3. Using NPS, set up GroupWise as a gadget:
   - **3a** Refer to GroupWise by using the name that is already set up in SecureLogin.

     This name becomes the common name. NPS passes this parameter.

     For example, type

     ```
     grpwise
     ```

     The parameter is case sensitive. Make sure that the case matches the common name.
   - **3b** For the Portal Services gadget, type the same key-value pair (for example, Username, Password) that was used in SecureLogin's configuration for GroupWise.

     NPS automatically uses only Username and Password for the keys in the credentials. These keys aren't case sensitive.

Scenario: Sharing a Secret. SecretStore and eDirectory are running on server DAir23. Portal Services is set up to use SecretStore and eDirectory on DAir23. SecureLogin was installed on Henri's workstation, using the *Novell eDirectory with SecretStore* option.

SecureLogin and a Portal Services gadget are set up to automatically grant users access to GroupWise. Both NSL and NPS use the same naming convention to refer to the shared secret for GroupWise. Because Henri has used GroupWise previously with SecureLogin, Henri's secrets for GroupWise are stored on an attribute in Henri's User object and in Henri's secret store.

Henri authenticates to the network. SecureLogin watches for events on Henri's desktop. Henri launches GroupWise, which returns a password dialog box. Because it has hooks into the system, SecureLogin recognizes the password dialog box and the application. SecureLogin automatically enters access credentials (username and password) for Henri. Henri uses GroupWise.

Both NSL and NPS use the same naming convention to refer to the shared secret. Also, both NSL and NPS specify the same credentials (for example, username and password).

4.4 Managing Secrets

You can manage secrets through iManager. You can perform the following maintenance tasks:

4.4.1 Adding a Secret

1. From the *Roles and Tasks* view, click *SecretStore* > *SecretStore*.
2. Browse for and select the desired User name.
3. Click *OK*.
4. In the *Number of secrets* row, click *View* in the *Action* column.

   The Secrets page is opened.
5. Click *New*.
6. Select the type of secret you want to create: Raw secret, shared secret - SS_App, or Shared secret - SS_Cred.
7. Click *OK*.
8. Fill in at least the required fields, then click *OK*.

4.4.2 Editing a Secret

1. From the *Roles and Tasks* view, click *SecretStore* > *SecretStore*.
2. Browse for and select the desired User name.
3. Click *OK*.
4. In the *Number of secrets* row, click *View* in the *Action* column.

   The Secrets page is opened.
5. In the *Identifier* column, click the name of the secret.
6. Click *Edit*.
7. Enter the master password in the *Password* field, then click *OK*.

4.4.3 Removing a Secret

1. From the *Roles and Tasks* view, click *SecretStore* > *SecretStore*.
2. Browse for and select the desired User name.
3. Click *OK*.

4 In the *Number of secrets* row, click *View* in the *Action* column.

The Secrets page is opened.

5 Select the secret you want to remove, then click *Delete*.

4.4.4 Unlocking a SecretStore

1 From the *Roles and Tasks* view, click *SecretStore* > *Unlock SecretStore*.

2 Browse for and select the desired User name.

3 Click *OK*.

4 The SecretStore is unlocked. Click *OK*.

To unlock another SecretStore, click *Repeat Task*.

4.4.5 Viewing a Secret

1 From the *Roles and Tasks* view, click *SecretStore* > *SecretStore*.

2 Browse for and select the desired User name.

3 Click *OK*.

4 In the *Number of secrets* row, click *View* in the *Action* column.

5 In the *Identifier* column, click the name of the secret.

4.4.6 Viewing a Secret's Status

You can find out the following information about the status of a secret:

- Whether the secret is locked
- Whether the secret has enhanced protection
- When the secret was created
- When the secret was last accessed
- When the secret was last modified

To view a secret's status:

1 From the *Roles and Tasks* view, click *SecretStore* > *SecretStore*.

2 Browse for and select the desired User name.

3 Click *OK*.

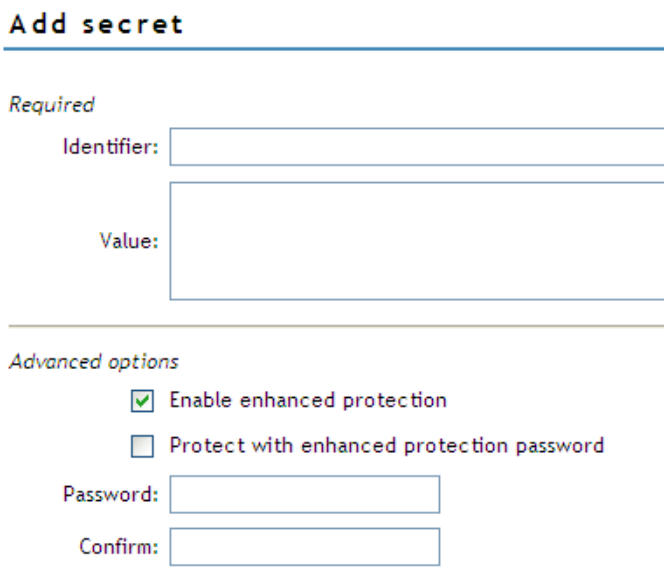
4 In the *Number of secrets* row, click *View* in the *Action* column.

5 In the *Identifier* column, click the name of the secret.

4.5 Using Enhanced Protection

The Enhanced Protection feature provides additional security for users' secrets. By default, a user's secrets have enhanced protection.

Figure 4-1 *Enhanced Protection*



This option is visible when you create a secret. For information on how to create a secret, see Section 4.4.1, “Adding a Secret,” on page 46.

This section provides information on the following:

- Section 4.5.1, “Locking SecretStore,” on page 48
- Section 4.5.2, “Setting a Master Password and Hint,” on page 49

4.5.1 Locking SecretStore

With the Enhanced Protection option enabled for any secret in Novell SecretStore, if the network administrator changes the user's NDS password, SecretStore enters a locked state. When SecretStore is locked, no secrets stored with the Enhanced Protection option can be read until SecretStore is unlocked.

SecretStore can be unlocked only if the user provides the last NDS password that was set. Because an administrator should not know the user's previous NDS password, secrets that have enhanced protection are kept safe.

NDS and SecretStore can distinguish between user-initiated password changes and those done by an administrator. SecretStore only locks when an administrator changes a user's password. An encrypted hash of the user's previous password is updated in SecretStore only if the user initiates the change.

If the user has changed an NDS password at least once since the account was created and before enhanced protection secrets are stored, this protection is completely secure. When a user does this, the administrator doesn't know the previous password. As a standard practice when you set up new User objects in NDS, require the user to change the password at first login.

Users who have Administrator-equivalent rights (that is, they have Supervisor rights but are not the actual network administrator) need to be careful when setting their own passwords. If a user sets a password when logged in as an Administrator-equivalent user, the user's SecretStore is then locked.

4.5.2 Setting a Master Password and Hint

The Master Password feature enables users to store and update a persistent password in SecretStore. If the Enhanced Protection feature is enabled and you (the administrator) reset a user's eDirectory password, SecretStore locks.

Also, a master password is useful if your secrets are locked and you can't remember your previous eDirectory password. By entering a master password, you gain access to your SecretStore.

By default, your master password isn't set. Only you can set your master password.

If the SecretStore client isn't installed and running on the workstation, you can't set a master password.

If you use SecureLogin with SecretStore, your master password is set when you create a passphrase answer in SecureLogin.

To set your master password:

1. Make sure that you are logged in to eDirectory as the user (not as Admin or another role).
2. In iManager, in the *Roles and Tasks* view, click *SecretStore* > *SecretStore*.
3. Browse for and select your username, then click *OK*.

   The SecretStore - Monitor SecretStore page is displayed.

4. In the Master Password row, click *Set* in the *Action* column.
5. Open the Set Master Password dialog box by clicking *Set*.
6. Type and confirm the master password.
7. Type a hint that's easy for you to remember the answer to, but isn't obvious to an onlooker.
8. Click *OK* to save the changes.

Other interfaces that unlock SecretStore (such as those built in to the Lotus* Notes* and Entrust* connectors) accept the master password in place of the previous eDirectory password. However, these interfaces might not be capable of displaying the hint.

4.6 Using Server Commands

You can use the following command line options at the server console:

NOTE: The commands are specific to Windows and NetWare.

```
Load sss [/a] [/d] [/t] [/m] [/c=# of Mins] [/o=DN] [/? | /h]
```

Table 4-1 *Server Command Line Options*

Option	Description
/a	Enables Novell Audit
/d	Clears the ACS file and load sss.dlm without command line parameters
/t	Enables Last Accessed Time Stamp
/m	Disables Master Password
/c=*Minutes*	Caches Refresh Period in Minutes (Minimum 30)
/o=*DN*	The NSSO object DN to use. NSSO DN form: my_nsso_obj.my_orgunit.my_org
/h	Displays Help
/?	Displays Help

With the SecretStore 3.3.3 release, the need to enable the cache with a separate command line parameter was eliminated. You now don't need to use the /e option, because it has been deprecated.

The autoexec.ncf file in NetWare® saves startup commands as a batch file. The commands are then executed when the SecretStore server starts. If you want to use command line options with the SecretStore server, you must first load the server sss.nlm before nldap.nlm. Otherwise, nldap.nlm auto-loads the sss.nlm without the command line option. Both sss.nlm and nldap.nlm are called from the autoexec.ncf file.

To take advantage of the Novell Audit logging features, load the logging NLM files in the autoexec.ncf file before loading SecretStore. Because the SecretStore service can connect to Novell Audit logging server only at load time, you must reload SecretStore if the connection to the logging server is lost.

For a detailed description on installing and configuring Novell Audit, refer the

Because eDirectory for Windows Server doesn’t have an autoexec.ncf file, DHost provides Active Configuration Services (ACS) that work as follows:

1. In the Windows Server plus eDirectory environment, the command line options are saved into an ACS file.
2. After the DLM (server) is loaded with a set of options for the first time, DHost saves the command line options to the ACS file.
3. Subsequent loadings of the server (DLM) cause the DHost to automatically read the same options from the ACS file.

On subsequent startups, there is no need to pass command line options.

If you must change the command line options, use the following procedure to reset the ACS file. Save the new options in the file for future use.

1. Take the server (DLM) down.
2. Restart the server by using the /d switch.

   This is a Windows Server-specific option. It deletes the Windows Server command line options from the ACS file.
3. Restart the server again with the new command line options to be written to the ACS file.
4. Take the server down again.

   After Step 4, loading the server does not require the command line options. The command line options are automatically read from the ACS file.

   Whenever new command line options are supplied, the previous options saved into the ACS file are automatically reset. However, in the presence of ACS command line configuration, the /d switch can be used to clear the ACS file and load `sss.dlm` without command line parameters.

   Otherwise, the command line parameters are read from the ACS file on every load of the server, just like commands are read from the `autoexec.ncf` file for NetWare.

Troubleshooting SecretStore

5

This section provides information on the following:

5.1 Where to Install

Install Novell SecretStore on a server that has a read/write replica.

5.2 Reading Preferences

SecretStore doesn't read preferences set up one level from the user. Users require Read/Compare ACL to the Prot:SSO attributes on the OUs that they will read.

For example, user Markus is in OU=RSDev.design.digitalairlines. The corporate scripts are in OU=design.digitalairlines. The SecureLogin client does not enforce (for Markus) preferences in design.digitalairlines. You require Read/Compare ACL to the Prot:LSSO attributes on the RSDev OU. The SecureLogin client now enforces the preferences.

5.3 Merging Trees

If SecretStore is running in separate trees, you can't merge the trees without any hit to SecretStore. After the merge, only SecretStore data in the destination tree is valid.

Before merging, delete SecretStore data from the source tree. After authenticating to the new tree, you must resave your single sign-on data.

See “Merging Novell eDirectory Trees” (http://www.novell.com/documentation/edir88/edir88/index.html?page=/documentation/edir88/edir88/data/af8cipa.html) in the *Novell eDirectory 8.8 Administration Guide*.

Novell SecretStore Error Codes

A

This section contains information on error codes that the Novell® SecretStore® service can generate.

A.1 SecretStore Return Codes

-800 NSSS E OBJECT NOT FOUND

Source: Novell® SecretStore®

Explanation: Can't find the target object DN in NDS® or Novell eDirectory™. (Resolve name failed).

Possible Cause: The server is unable to verify the user that is trying to read a SecretStore. The User object is not in NDS or is in a different partition or replica.

Possible Cause: The server that holds the read/write replica containing the User object is not up.

-801 NSSS E NICI FAILURE

Source: Novell SecretStore

Explanation: NICI operations have failed.

-802 NSSS E INVALID SECRET ID

Source: Novell SecretStore

Explanation: The secret ID is not in the User SecretStore.

-803 NSSS E SYSTEM FAILURE

Source: Novell SecretStore

Explanation: Some internal operating system services are not available.

-804 NSSS E ACCESS DENIED

Source: Novell SecretStore

Explanation: Access to the target SecretStore has been denied.

-805 NSSS E NDS INTERNAL FAILURE

Source: Novell SecretStore

Explanation: Some internal eDirectory or NDS services are not available.

-806 NSSS E SECRET UNINITIALIZED

Source: Novell SecretStore

Explanation: A secret has not been initialized with a write.

-807 NSSS E BUFFER LEN

Source: Novell SecretStore

Explanation: The size of the buffer is not in a nominal range between minimum and maximum.

Possible Cause: The programmer or vendor who wrote the connector for the application did not meet requirements.

-808 NSSS E INCOMPATIBLE VERSION

Source: Novell SecretStore

Explanation: Client and server component versions are not compatible.

Possible Cause: The version of Novell SecretStore that is running on the server is earlier than the version of SecretStore that is running on a client workstation.

Action: Upgrade your server to the latest version of SecretStore.

-809 NSSS E CORRUPTED STORE

Explanation: SecretStore data on the server has been corrupted.

Possible Cause: A key has become corrupted and cannot decrypt data.

If corruption occurs in the data, SecretStore repairs corrupted data. Whenever you add new secrets to SecretStore, the first read after a write automatically repairs and synchronizes SecretStore.

If corruption occurs in the key, SecretStore discards the data and begins anew.

-810 NSSS E SECRET ID EXISTS

Source: Novell SecretStore

Explanation: The secret ID already exists in the SecretStore.

Possible Cause: You are trying to add a secret ID using the Add option. The system informs you that the secret already exists.

-811 NSSS E NDS PWORD CHANGED

Source: Novell SecretStore

Explanation: The network administrator has changed the user's eDirectory or NDS password. SecretStore is now locked.

-812 NSSS E INVALID TARGET OBJECT

Source: Novell SecretStore

Explanation: The target eDirectory or NDS User object is not found.

Possible Cause: During a logon process, you passed the ResolveName process. However, the SecretStore service cannot find the target eDirectory or NDS User object to read a SecretStore in eDirectory.

-813 NSSS E STORE NOT FOUND

Source: Novell SecretStore

Explanation: The target eDirectory or NDS User object does not have a SecretStore.

Possible Cause: The User object exists but does not have a SecretStore on it. This message usually comes while you are attempting to read (or enumerate) SecretStore. If you add or write to SecretStore, the SecretStore service automatically creates a secret.

-814 NSSS E SERVICE NOT FOUND

Source: Novell SecretStore

Explanation: SecretStore is not on the network.

Possible Cause: The client pinged to find a server that is running the SecretStore service, but no SecretStore was found.

Action: Install SecretStore on a server.

Action: Make sure that `sss.nlm` is running on a SecretStore server.

-815 NSSS E SECRET ID TOO LONG

Source: Novell SecretStore

Explanation: The length of the Secret ID buffer exceeds the limit.

Possible Cause: An application has attempted to pass in a secret ID that is longer than 256 characters.

Action: Contact the vendor of the application.

-816 NSSS E ENUM BUFF TOO SHORT

Source: Novell SecretStore

Explanation: The length of the enumeration buffer is too short.

Possible Cause: A programmer needs to make a call again to a larger buffer. NSSS returns what data it can in the buffer that was passed.

Action: The maximum buffer size is 128 KB. The maximum packet size is also 128 KB. If you have more secrets IDs in SecretStore than 128 KB, use wild cards to change the scope of your enumerations. Change the scope at the API level or in SecretStore utilities.

-817 NSSS E NOT AUTHENTICATED

Source: Novell SecretStore

Explanation: The user is not authenticated.

Possible Cause: A SecretStore server was found, but the SecretStore client was unable to open a connection.

Action: Log in to eDirectory again.

-818 NSSS E NOT SUPPORTED

Source: Novell SecretStore

Explanation: Unsupported operations.

Possible Cause: A feature was published during beta but is not yet implemented.

-819 NSSS E NDS PWORD INVALID

Source: Novell SecretStore

Explanation: The eDirectory or NDS password is not valid.

Possible Cause: You tried to unlock SecretStore, but you incorrectly entered a password.

Action: Enter the correct password.

-820 NSSS E NICI OUTOF SYNC

Source: Novell SecretStore

Explanation: The session keys of the client and server NICI are out of sync.

Possible Cause: A server went down and the connection was lost. When the server came up again and Novell Client32™ re-established a connection, the SecretStore client tried several times to get a session key from the SecretStore server and failed. SecretStore's session keys are not valid anymore.

Action: Try to run the application again.

-821 NSSS E SERVICE NOT SUPPORTED

Source: Novell SecretStore

Explanation: The requested service is not yet supported.

Possible Cause: The SecretStore client tried to call a plug-in (service) that SecretStore doesn't know about. Novell does not support that particular service.

-822 NSSS E TOKEN NOT SUPPORTED

Source: Novell SecretStore

Explanation: The eDirectory or NDS authentication type is not supported.

Possible Cause: Although SecretStore recognizes the requesting service, SecretStore does not recognize the eDirectory authentication credential. The SecretStore plug-in might be a later version than the SecretStore version.

-823 NSSS E UNICODE OP FAILURE

Source: Novell SecretStore

Explanation: A Unicode* text conversion operation failed.

Possible Cause: SecretStore tried to translate Unicode but was unable to.

Action: Try again.

-824 NSSS E TRANSPORT FAILURE

Source: Novell SecretStore

Explanation: The server connection has been lost.

Action: Wait for the server to reboot, or log in again.

-825 NSSS E CRYPTO OP FAILURE

Source: Novell SecretStore

Explanation: A cryptographic operation failed.

Possible Cause: When SecretStore tried to encrypt or decrypt data, the key or data was corrupted.

Action: Try again.

-826 NSSS E SERVER CONN FAILURE

Source: Novell SecretStore

Explanation: An attempt to open a connection to the server failed.

Possible Cause: The Transport plug-in `ssncp.nlm` or `ssldp.nlm` is not running on the server.

Action: Ask the system administrator to load the Transport plug-in modules on the server.

-827 NSSS E CONN ACCESS FAILURE

Source: Novell SecretStore

Explanation: Access to a server connection failed.

Possible Cause: A SecretStore client could not get exclusive hold of a connection table on the client.

-828 NSSS E ENUM BUFF TOO LONG

Source: Novell SecretStore

Explanation: The size of the enumeration buffer exceeds the 128-KB limit.

-829 NSSS E SECRET BUFF TOO LONG

Source: Novell SecretStore

Explanation: The size of the Secret buffer exceeds the limit.

Action: Make the secrets smaller.

-830 NSSS E SECRET ID TOO SHORT

Source: Novell SecretStore

Explanation: The length of the secret ID should be greater than zero.

Possible Cause: The secret ID is zero. You have specified a null ID.

Action: Contact the application vendor.

-831 NSSS E CORRUPTED PACKET DATA

Source: Novell SecretStore

Explanation: Protocol data was corrupted on the wire.

Possible Cause: While sending data to the server or reading data from the server, SecretStore discovered that the data packets don't match.

Action: Try again.

-832 NSSS E EP ACCESS DENIED

Source: Novell SecretStore

Explanation: Enhanced protection password validation failed for the application. Access to the secret is denied.

Possible Cause: For reading this particular secret, you need to pass a particular application enhanced protection password.

Action: Try again. Pass the enhanced protection password or enter a master password. Otherwise, contact the application vendor.

-833 NSSS E SCHEMA NOT EXTENDED

Source: Novell SecretStore

Explanation: The eDirectory or NDS schema is not extended to support SecretStore on the target tree.

Possible Cause: SecretStore is not properly installed. `sss.nlm` or `sss.dlm` is running on a server, but the eDirectory or NDS schema has not been extended.

Action: Reinstall SecretStore.

-834 NSSS E ATTR NOT FOUND

Source: Novell SecretStore

Explanation: One of the optional service attributes is not instantiated.

Possible Cause: You are trying to open a set of configuration attributes, but a particular attribute is missing.

Action: Configure the system.

-835 NSSS E MIGRATION NEEDED

Source: Novell SecretStore

Explanation: The server has been upgraded. The user's SecretStore should be updated.

Possible Cause: Internally, the SecretStore service has detected an older format in a user's SecretStore. The service reads the older format and then writes (migrates) the data by using the new format.

-836 NSSS E MP PWORD INVALID

Source: Novell SecretStore

Explanation: The master password could not be verified to read or unlock the secrets.

Possible Cause: You entered an incorrect master password.

Action: Correctly enter the master password.

-837 NSSS E MP PWORD NOT SET

Source: Novell SecretStore

Explanation: The master password has not been set on SecretStore.

Possible Cause: You are trying to read enhanced protected secrets or unlock SecretStore, but a master password is not set on SecretStore.

Action: Set a new master password.

-838 NSSS E MP PWORD NOT ALLOWED

Source: Novell SecretStore

Explanation: The administrator has disabled the ability to use the master password.

Possible Cause: While configuring the SecretStore service, you checked the Disable Master Password Operations check box.

-839 NSSS E WRONG REPLICA TYPE

Source: Novell SecretStore

Explanation: Not a writable replica of eDirectory or NDS.

Possible Cause: The replica is read-only. SecretStore is unable to write to or modify the replica. Several replicas might be running on the server, but the particular replica is read-only.

Action: Go to a different replica. Set up SecretStore so that a user can always go to a writable replica.

-840 NSSS E ATTR VAL NOT FOUND

Source: Novell SecretStore

Explanation: The SecretStore service didn't find an attribute value (secret ID) that you are trying to read.

-841 NSSS E INVALID PARAM

Source: Novell SecretStore

Explanation: An API parameter is not initialized. A null or out-of-range parameter was passed to a client NDK API.

Action: Don't pass null parameters to the APIs.

-842 NSSS E NEED SECURE CHANNEL

Source: Novell SecretStore

Explanation: An LDAP request to SecretStore is trying to make a clear-text connection, which is not allowed. The connection to SecretStore needs to be over SSL.

Action: Use an SSL connection.

-843 NSSS E CONFIG NOT SUPPORTED

Source: Novell SecretStore

Explanation: A user or a container has been assigned to use a particular configuration that is not available.

Possible Cause: Servers that support the configuration are all out of service.

Action: Make sure that the servers are functioning properly. Also make sure that the SecretStore service on those servers is loaded with the proper command line parameter.

-844 NSSS E STORE NOT LOCKED

Source: Novell SecretStore

Explanation: An attempt to unlock SecretStore failed because the store isn't locked.

-845 NSSS E TIME OUT OF SYNC

Source: Novell SecretStore

Explanation: The servers holding read/write replicas of the user's SecretStore are out of sync with the time source on the network.

Action: Force a time sync by using the available time services on the servers. See Performing Synchronization Operations (http://www.novell.com/documentation/edir88/edir88/index.html?page=/documentation/edir88/edir88/data/aese2hi.html) in the *Novell eDirectory 8.8 Administration Guide*.

-846 NSSS E VERSION MISMATCH

Source: Novell SecretStore

Explanation: Versions of the client files don't match. For Windows, the files are nsss.dll, nssldp.dll, and nssncp.dll. For NetWare®, the files are corresponding `.nlm` files. For UNIX, the files are corresponding `.lib` files.

Action: Install the latest client files.

-847 NSSS E SECRET BUFF TOO SHORT

Source: Novell SecretStore

Explanation: The buffer supplied for the secret is too short.

Action: Use the proper buffer sizes out of nssscl.h to allocate for API use.

-848 NSSS E SH SECRET FAILURE

Source: Novell SecretStore

Explanation: Shared-secret processing and operations failed on the client.

Action: Make sure that the shared secrets are in the correct format.

-849 NSSS E PARSER FAILURE

Source: Novell SecretStore

Explanation: Shared-secret parser operations failed on the client.

Action: Make sure that the shared secrets are in the correct format.

-850 NSSS E UTF8 OP FAILURE

Source: Novell SecretStore

Explanation: Utf8 string operations failed on the client. This is an internal LDAP failure.

Action: Check LDAP NDK components (`.dll`, `.nlm`, or `.lib` files).

-851 NSSS E CTX LESS CN NOT UNIQUE

Source: Novell SecretStore

Explanation: More than one DN contains the user's Common Name in eDirectory. The contextless name for an LDAP bind does not resolve to a unique DN.

Action: Specify the DN instead of the Common Name.

-852 NSSS E UNSUPPORTED BIND CRED

Source: Novell SecretStore

Explanation: The login credential required for the advanced bind operation is not supported by this version.

Action: Refer to the list of supported protocols in the documentation.

-853 NSSS E CERTIFICATE NOT FOUND

Source: Novell SecretStore

Explanation: The LDAP Root certificate required for bind operations is not found.

Action: Verify the accuracy of the user's LDAP DN, password, or servers IP address.

-888 NSSS E NOT IMPLEMENTED

Source: Novell SecretStore

Explanation: This feature is not yet implemented.

Possible Cause: A feature was published during beta but is not yet implemented.

-899 NSSS E BETA EXPIRED

Source: Novell SecretStore

Explanation: The product's beta life has expired.

Action: Purchase an officially released copy.

Documentation Updates

B

The documentation was updated on the following dates:

B.1 May, 2009

Location	Change
Entire	Defect fixes
	Updated the supported eDirectory version.
Figure 1-1 on page 13	Updated the graphics
Figure 1-2 on page 13	
Chapter 3, “Installing and Activating Novell Audit,” on page 25	Added a section on installing and activating Novell Audit.

B.2 August 8th, 2008

Updates were made to the following sections. The changes are explained below.

Location	Change
Entire Document	Removed all information concerning SecretStore Manager and SecretStore Status. These are not supported for this version of SecretStore.
Entire Document	Removed all information concerning ConsoleOne. iManager is now the preferred administration tool for SecretStore. Procedures that were accomplished through ConsoleOne are now accomplished through iManager. Documentation now reflects this.
Entire Document	Changed ConsoleOne screenshots to iManager screenshots.
Entire Document	Updated guide to current Novell style.
“Installing the SecretStore Plug-In to iManager” on page 23	Added information describing how to install the SecretStore plug-in for iManager.
	Removed sections about using disconnected authentication, testing SecretStore, and viewing information about SecretStore, as these tasks were performed through SecretStore Manager.