Novell SecretStore

3.0

www.novell.com

ADMINISTRATION GUIDE

103-000229-001

Novell®

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A

www.novell.com

SecretStore Administration Guide
March 7, 2003

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

Novell Trademarks

ConsoleOne is a trademark of Novell, Inc.
eDirectory is a trademark of Novell, Inc.
GroupWise is a registered trademark of Novell, Inc. in the United States and other countries.
NDS is a registered trademark of Novell, Inc. in the United States and other countries.
NetWare is a registered trademark of Novell, Inc. in the United States and other countries.
Novell is a registered trademark of Novell, Inc. in the United States and other countries.
Novell Certificate Server is a trademark of Novell, Inc.
Novell Client is a trademark of Novell, Inc.
Novell Modular Authentication Services is a trademark of Novell, Inc.
Novell SecretStore is a trademark of Novell, Inc.
ZENworks is a trademark of Novell, Inc.

Third-Party Trademarks

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

Contents

About This Guide

This guide is for network administrators. It provides information on the following:

- Chapter 1, “Overview,” on page 9
- Chapter 2, “Installing SecretStore,” on page 19
- Chapter 3, “Administering SecretStore,” on page 33
- Chapter 4, “Troubleshooting Novell SecretStore,” on page 55
- Appendix A, “Sharing Secrets with Novell Portal Services,” on page 67

Additional Documentation

For information on Novell® SecureLogin, see the following:

- SecureLogin Administration Guide
- Configuration Guide for Terminal Emulators

Documentation Updates

For the most recent version of the *Novell SecretStore Administration Guide*, see SecretStore (http://www.novell.com/documentation-index/index.jsp) on the Novell® documentation Web Site.

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

1 Overview

Novell® SecretStore™ is a simple and secure password management solution. Using the power of Novell eDirectory™ and the security of Novell SecretStore, users can access most Windows*-, Web-, and mainframe-based applications with a single password.

After you've authenticated to eDirectory, SecretStore-enabled applications 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.

The following sections can help you get a big picture of SecretStore.

- Key Terms

  This topic is a glossary of key terms concerning what runs on the server, what runs on the workstation, and SecretStore components in eDirectory.

- How SecretStore Works

  The second topic explains how SecretStore server components, workstation components, and eDirectory objects work together. This background prepares you for installing, setting up, managing, using, and troubleshooting SecretStore.

Key Terms

Server Components

SSSI.NLM— Extends the eDirectory schema, installs the Novell SecretStore service, and initializes and/or validates the Security Domain Infrastructure (SDI).

You use nwconfig.nlm to load sssi.nlm (Novell SecretStore Installation NetWare® Loadable Module). Sssi.nlm does the following:

- Extends the eDirectory schema
- Installs the SecretStore server components (sss.nlm)
- Configures the eDirectory LDAP server to enable SecretStore extensions
- Modifies the startup script to load SecretStore services

SSS.NLM—The Novell SecretStore service.

The equivalent file for Windows NT*/2000 servers is sss.dlm. The equivalent file for UNIX* servers is libsss.so.

SecretStore provides a secure infrastructure for storing and retrieving secrets and credentials in eDirectory. SecretStore uses NICI and Security Domain Infrastructure (SDI) to safely and securely store a user's secrets.

Novell SecureLogin is a single sign-on application that uses SecretStore.

Upon a successful authentication of the user to an application, the SecretStore-enabled application stores the application's 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.

Lsss.nlm allows applications to use the Light Weight Directory Access Protocol (LDAP) to store secrets. The equivalent file for Windows NT/2000 servers is lsss.dll.

sssnapin.exe—The SecretStore snap-in to ConsoleOne.

Sssnapin.exe enables you (the administrator) to configure and administer SecretStore components.

Novell eDirectory automatically installs ConsoleOne™ on a server. However, to use ConsoleOne, you install the SecretStore snap-in to ConsoleOne on a client workstation (or to a directory on a server) and run ConsoleOne from a workstation. The SecretStore installation program installs the snap-in.

For more information on SecretStore, see the following:

- SecretStore-related information in Novell Developer Kits, available at the Novell Developers Web site (http://developer.novell.com)
- Novell Developer Notes, November 1999 (http://developer.novell.com/research/devnotes/1999/november/05/index.htm)
- Novell Developer Notes, April 2000 (http://developer.novell.com/research/devnotes/2000/april/02/d000402.htm)

Workstation Components

For the SecretStore 3.0 release, the SecureLogin installation program (setup.exe) installs the following components on your administrative Windows workstation. Workstation components are currently not available for UNIX platforms.

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.

Novell SecureLogin—Enables applications to communicate with SecretStore as a universal connector.

The Novell SecureLogin client embodies the APIs for accessing the SecretStore service.

NMAS client—Enables single sign-on users (online or offline) to authenticate to eDirectory.

The NMAS client can confirm authentication during the following situations:

- You are not logged in to eDirectory.
- You are logged in to an eDirectory tree that is different from the one that the single sign-on client synchronizes with.
- A default timeout has occurred.

SecretStore client—Provides the mechanism to access the SecretStore service and ensure secure transmission 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.

ConsoleOne—Enables you to administer (from a workstation) secrets in SecretStore.

SecretStore ConsoleOne snap-in—Enables you to create, configure, and administer single sign-on objects in eDirectory.

You can run the ConsoleOne snap-in on your workstation provided you have also installed the NICI and Novell SecureLogin client components.

SecretStore Manager—Enables users to perform basic maintenance tasks on their SecretStore.

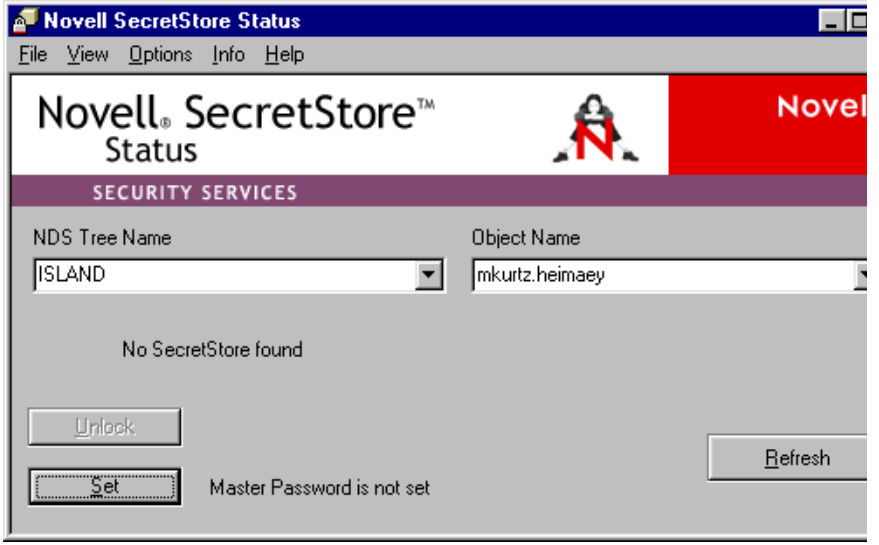
SecretStore Manager protects secrets by requiring NMAS authentication before a user can view secrets.

Although SecretStore Manager is not intended as the primary interface to SecretStore, it helps users manage SecretStore secrets outside the interfaces provided by the SecureLogin-enabled applications.

The following figure illustrates SecretStore Manager:

SecretStore Status—Enables users to set their master password, unlock SecretStore, switch between eDirectory trees, or switch between eDirectory usernames associated with different trees or servers.

SecretStore Status is a lite version of SecretStore Manager. The following figure illustrates SecretStore Status:



SecretStore Service Objects

SecretStore—A Container object that can hold default SecretStore service settings.

This object is automatically named SecretStore and placed in the Security container.

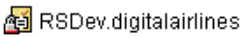
The SecretStore system requires at least one SecretStore Container object. The SecretStore object can contain sssServerPolicyOverride objects.

The following figure illustrates a SecretStore object.

sssServerPolicyOverride object—Objects that enable you to customize access to applications, depending on group or user needs for different parts of the tree.

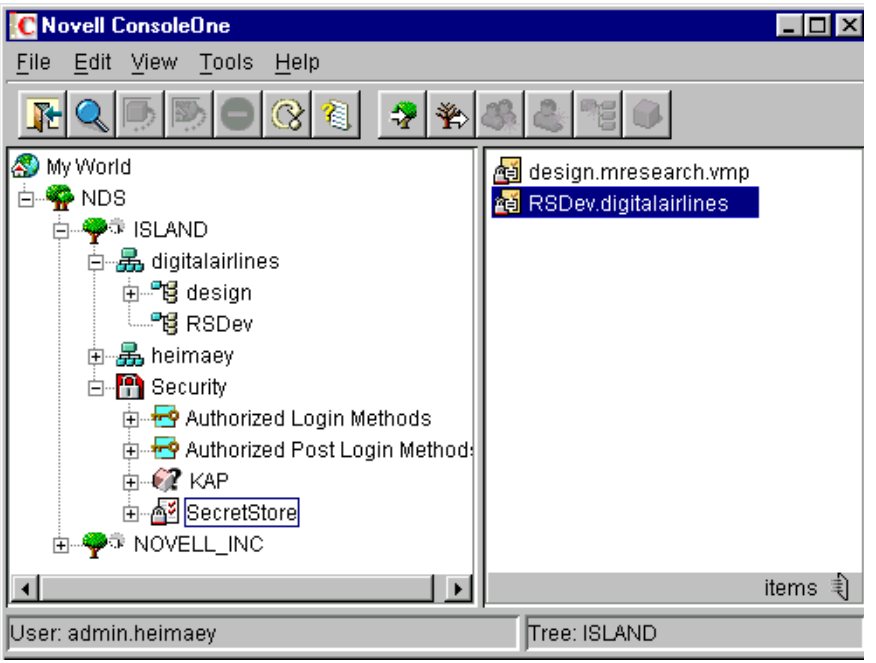
sssServerPolicyOverride objects reside in the SecretStore Container object. Each sssServerPolicyOverride object must take the name of the context that the Group or User objects are in.

The following figure illustrates an sssServerPolicyOverride object:



Scenario. You want to provide more liberal restrictions for groups and users in the RSDev context. This object is in the digitalairlines Organization object. In ConsoleOne, you create a new sssServerPolicyOverride object, name it RSDev.digitalairlines, and configure server options for this new object.

The following figure illustrates the name-and-context relationship.



How SecretStore Works

Architecture

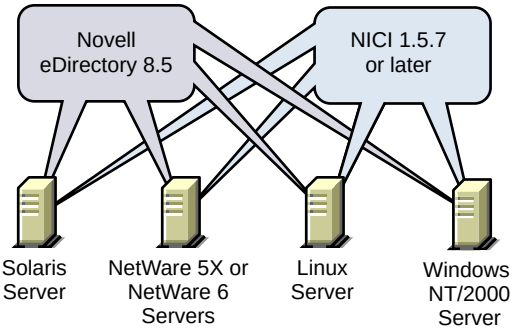
SecretStore 3.0 runs on Solaris*, Linux*, NetWare 5.x, NetWare 6, and Windows 2000/NT.

The Solaris and Linux servers require Novell eDirectory 8.5 or Corporate Edition 8.5 or later. (NICI is automatically installed during server installation.)

The NetWare 5.x and NetWare 6 servers can run NDS 7, as long as NICI 1.5.4 or later is installed. However, we recommend that you upgrade to Novell eDirectory 8.5 or later.

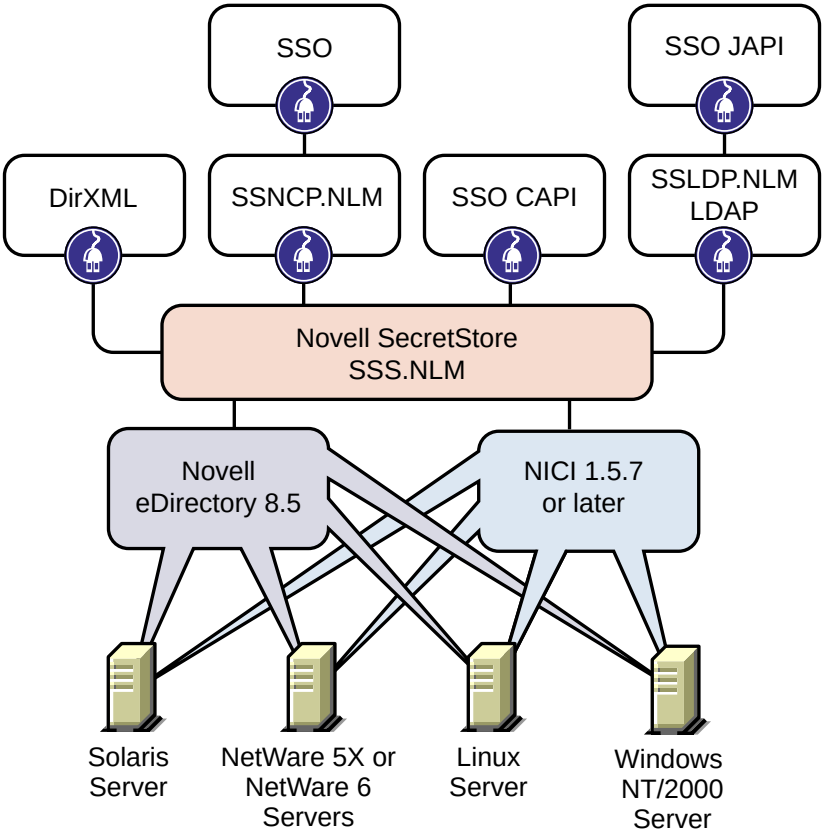
Windows NT/2000 servers require eDirectory 8.6*x* and NICI 2.02.

The following figure illustrates SecretStore running on these platforms:



When you install SecretStore on these servers, the installation program installs the SecretStore service on top of eDirectory and NICI. SecretStore plug-ins run on top of SecretStore.

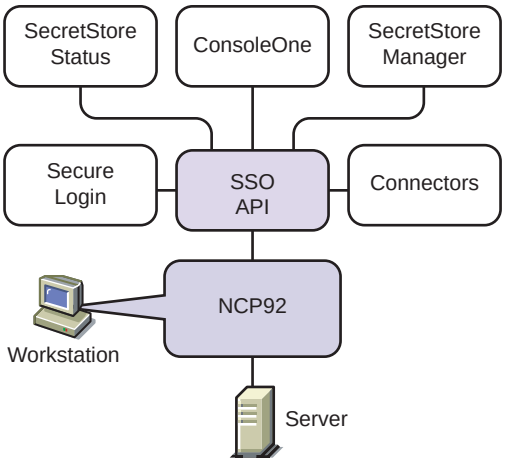
The following figure illustrates this software:



SecretStore plug-ins include DirXML™, client APIs, NCP™, and an LDAP extension.

You install administrative and SecretStore components on a Windows workstation and administer SecretStore from there.

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



The following steps illustrate how SecretStore works:

1. A user logs in to eDirectory by using a password.
2. A successful login allows the user's secrets to be downloaded (when necessary) from SecretStore to the workstation. Through the use of SecureLogin, this process enables disconnected use.
3. The user accesses a Windows, Web-based, or host-based application. SecureLogin recognizes the application and responds with the appropriate username and password fetched from SecretStore.

   If SecureLogin does not discover matching credentials, the client prompts the user to add the application. Secrets are synchronized when certain events occur or when the user connects to or disconnects from eDirectory.

For illustrations concerning how SecretStore works, see Novell SecretStore (http://developer.novell.com/research/devnotes/1999/november/05/03.htm) in the November 1999 AppNotes. This article illustrates the following:

- How applications authenticate before SecretStore is enabled
- A user's first-time authentication to SecretStore-enabled applications
- A user's subsequent authentications

2 Installing SecretStore

You can install the Novell® SecretStore™ service on NetWare® 5.x or NetWare 6, Windows* NT*, Windows 2000, Windows XP, Linux*, or Solaris*.

The SecureLogin client installation program installs the SecretStore client on your workstation. You don't have to install it separately. However, you need to install the SecretStore snap-in to ConsoleOne and (if it isn't already installed on your workstation) ConsoleOne. These files are on the SecureLogin CD or downloaded file.

A Novell eDirectory™ administrator should perform the server installation so that the schema is extended properly.

Installing SecretStore on a NetWare 5.*x* or NetWare 6 Server

The SecretStore installation program installs two server components:

- The server version of Novell International Cryptographic Infrastructure (NICI) 1.5.7 or later.
- Novell SecretStore.

Requirements

- ❑ A NetWare 5.*x* or NetWare 6 server.
- ❑ Novell eDirectory or NDS® Corporate Edition.

- ❑ Security Domain Infrastructure.

  NDS or eDirectory must have a tree key that is properly set up. If you are running eDirectory 8.5 or later, the tree key is already set up. NetWare 5.1, later NetWare versions, and Novell Certificate Server automatically set up the tree key.

  If you are running NDS or a version of eDirectory earlier than 8.5, download and install the latest Novell Certificate Server, which is available from www.novell.com\products.

- ❑ The latest support pack for your NetWare version.
- ❑ Supervisor rights to the NDS or eDirectory tree on the NetWare server.
- ❑ The server must have a read/write replica of the partition that contains the User objects for those who will use SecretStore.
- ❑ For a server to correctly extend LDAP functionality to include SecretStore, the server must hold a read/write replica of the Root partition.

Installing NICI

Novell SecretStore 3.0 requires NICI 1.5.7 or later for a tree running Novell Directory Services or Novell eDirectory on NetWare. The *Novell SecureLogin CD* includes two versions of Server NICI.

- NICI 1.5.7

  Install NICI 1.5.7 on NetWare servers in the trees running Novell Directory Services earlier then 85.0.1.

- NICI version 2.*x* on Windows servers and newer NetWare servers running eDirectory 8.6*x*.

  Only install NICI2.*x* in trees running Novell eDirectory 85.0.1 or later.

  IMPORTANT: If you install NICI 2.0 into a tree running Novell Directory Services earlier than 85.0.1, NICI services won't be available.

1. At the NetWare server, insert the *Novell SecureLogin* CD.
2. Mount the *Novell SecureLogin* CD as a NetWare volume by entering **CDROM**.

3. From nwconfig.nlm, select Product Options > Install a Product Not Listed.
4. (Conditional) If paths appear, select any path, then press Enter.

   If you have a new server or haven't used nwconfig.nlm to install products not listed, no paths appear.
5. Press F3 > enter the path to the NICI files (for example, nsl_30:\nici\nici_1.57).
6. Follow the on-screen instructions to accept the license agreement and copy files.

   This step adds the following line to the autoexec.ncf file:

   ```
   Load sasdfm.xlm
   ```
7. Exit nwconfig.nlm, then shut down and restart the server.

Installing the SecretStore Service

1. Mount the *Novell SecureLogin* CD as a NetWare volume by entering **`CDROM`**.
2. From nwconfig.nlm, select Product Options > Install a Product Not Listed.
3. Select any path, then press Enter.
4. Press F3, then enter the path to the Novell SecretStore files (for example, secstore:\server\netware\).

   The sss.ips script file resides here.
5. Follow the on-screen instructions to accept the license agreement, copy files, and configure the server.

   This step does the following:

   - Installs the SecretStore service (sss.nlm, ssncp.nlm, ssldp.nlm, and lsss.nlm).
   - Extends the NDS or eDirectory schema to accommodate SecretStore objects.
   - Adds the following lines to the autoexec.ncf file:

- Load nicisdi.xlm
- Load sasdfm.xlm
- Load ssncp.nlm

  This NLM automatically loads sss.nlm. Always place this line before the following line, if it is present:

  ```
  Load nldap.nlm
  ```

6. Exit nwconfig.nlm.
7. (Conditional) Shut down and restart the server.

   If you are installing SecretStore on a NetWare 5.1 or NetWare 6 server, you can skip this step.

Synchronizing Time

Because NDS or eDirectory replicas influence a SecretStore server's operations, make sure that the replicas are properly synchronized.

For information about time synchronization, see Synchronizing Time (http://www.novell.com/documentation/lg/ics12/index.html?page=/documentation/lg/ics12/ics12/data/h2zrv92j.html) in the *Novell eDirectory 8.7 Administration Guide*.

Installing SecretStore on a Windows Server

You can install SecretStore on a Windows NT, Windows 2000, or Windows XP server. The SecretStore installation program installs the server version of NICI 2.*x*.

Windows NT/2000/XP Requirements

- ❑ Windows NT Server 4.0 with Service Pack 2 or later, Windows 2000 Server, or Windows XP Server.
- ❑ Novell eDirectory 8.5.0.*x* or later with a functioning NDS tree.

  IMPORTANT: Make sure that the Windows NT/2000/XP server running Novell eDirectory is being used only as a server and not a Novell client.

- Supervisor rights to the eDirectory tree on the Windows NT/2000/XP server.
- The server has a read/write replica of the partition that contains the User objects for those who will use SecretStore.

Installing NICI 1.5.7 or Later

NICI 2.0.2 is provided so that you can install SecretStore on Windows Servers running eDirectory 85.0.*x* or later.

1. Log in as Administrator on the Windows NT/2000/XP server

   IMPORTANT: You must be logged in as Administrator for the NICI software to be installed correctly.

2. On the Windows NT/2000/XP server running Novell eDirectory or NDS Corporate Edition, close all applications.
3. Insert the *Novell SecureLogin* CD, then exit the auto-start client installation program if it starts.
4. run the program wcniciu0.exe from the nici\windows directory on the *novell securelogin* cd.
5. Overwrite all files, then restart the server.
6. If it is not already open, launch the NDS Services console window (ndscons.exe) from the Novell eDirectory or NDS Corporate Edition directory (c:\novell\nds by default) on the Windows NT/2000 server.

   The NICI NCP Handlers service (NICIEXT) should now start automatically.

Installing the SecretStore Service

1. Run setup.exe and follow the on-screen instructions.

   This file is in the secstore\server\windows directory on the *Novell SecureLogin* CD.

   IMPORTANT: Make sure that the destination directory corresponds to the directory where Novell eDirectory or NDS Corporate Edition resides on your Windows NT/2000 server (c:\novell\nds by default).

2. If necessary, launch the NDS Services console window (ndscons.exe).

If the NDS Services console window is already open, you must close and reopen the window to see the SecretStore service.

Synchronizing Time

Because NDS or eDirectory replicas influence a SecretStore server's operations, make sure that the replicas are properly synchronized.

For information about time synchronization, see Synchronizing Time (http://www.novell.com/documentation/lg/ics12/index.html?page=/documentation/lg/ics12/ics12/data/h2zrv92j.html) in the *Novell eDirectory 8.7 Administration Guide*.

Installing SecretStore on a Solaris/Linux Server

Requirements

Requirements for Solaris

- ❑ Solaris 2.6, Solaris 7, or Solaris 8
- ❑ Access to the [Root] of the server
- ❑ Admin rights to the NDS or eDirectory tree on the server
- ❑ Novell eDirectory 8.6.2 or later with a functioning eDirectory tree

Requirements for Linux

- ❑ Linux 2.2 and glibc 2.1.3 or later
- ❑ Red Hat Package Manager (RPM)
- ❑ Access to the [Root] of the server
- ❑ Admin rights to the NDS or eDirectory tree on the server
- ❑ Novell eDirectory 8.6.2 or later with a functioning eDirectory tree

Installing the SecretStore Service

You can use the ss-install utility to install SecretStore components on Solaris or Linux systems. This utility is located in the Setup directory on the CD under the Solaris or Linux Platform directories of the *Novell SecureLogin* CD.

1. Mount the *Novell SecureLogin* CD.
2. Change to the platform/setup directory on the CD.

   The platform can be Solaris or Linux.
3. Log in as the root user on the host server where SecretStore has to be installed.
4. Run the sso-install script.

   When prompted, accept the license agreement.

   Select the components that you are prompted to install.
5. Configure SecretStore for UNIX.

Configuring SecretStore for Solaris or Linux

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

/usr/sbin/ssscfg [**-h** *hostname*[:*port*]] [**-w** *password*] [**-a** <*admin FDN*>] **-c** [**-f**] [**-v**] [**-s** *schemafile*]

Parameter	Description
hostname	The hostname of the server on which Novell SecretStore server components have to be configured.
port	(Optional) The NDS or eDirectory server port.
-w	The password that corresponds to <*admin FDN*>. If you enter the optional parameter is entered.
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.
-f	Allows operations on a filtered replica. By default, this option is disabled.
-v	Sets the verbose mode.
-s	Refers to the SecretStore schema file in eDirectory format (SSSV3.SCH). The schema file is installed as part of the SecretStore product installation.

Synchronizing Time

Because NDS or eDirectory replicas influence a SecretStore server's operations, make sure that the replicas are properly synchronized.

For information about time synchronization, see Synchronizing Time (http://www.novell.com/documentation/lg/ics12/index.html?page=/documentation/lg/ics12/ics12/data/h2zrv92j.html) in the *Novell eDirectory 8.7 Administration Guide*.

Installing the SecretStore Client on Workstations

This section might not apply to all products. For example, SecretStore Client components are automatically installed by the Novell SecureLogin 3.0 Client installation program when the SecretStore option is selected.

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

Requirements

- A Windows 95, Windows 98, Windows NT 4.0, or Windows 2000/XP workstation used exclusively as a client workstation
- For Windows 2000 workstations, have Power User or Administrator desktop privileges

- ❑ Novell Client™ 3.21 or later for Windows 95 and Windows 98 workstations; Novell Client 4.71 or later for Windows NT and Windows 2000/XP workstations.
- ❑ ConsoleOne™ 1.3.2 or later.

  The SecretStore snap-in to ConsoleOne requires ConsoleOne 1.3.2 or later. The installation program for SecureLogin 3.0 can install ConsoleOne 1.3.3. The files are copied to the consoleone\1.2 directory.
- ❑ Supervisor rights to the NDS or eDirectory tree

These requirements are for installing on an administrative workstation. Users don't need Supervisor rights to the tree.

Components

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

- SecretStore client
- NICI client
- ConsoleOne

  You administer SecretStore through ConsoleOne on your administrative workstation.

  You can copy the SecretStore snap-in file (sssnapin.exe) from the consoleone\snapins directory on the Novell SecureLogin CD to a network directory (sys:\public\mgmt\consoleone\ 1.2). Then run SecretStore options from various workstations. ConsoleOne must also be running on those workstations.
- The SecretStore snap-in to ConsoleOne

Users won't need the snap-in to ConsoleOne. Also, consider the following guidelines concerning users:

- To prevent users from seeing passwords, don't install NMAS™ on users' workstations.
- Use ZENworks™ to distribute SecretStore to users' workstation.

Installing the SecretStore Client

By default, the installation program for Novell SecureLogin 3.0 installs the SecretStore client. For information on installing Novell SecureLogin, see Installing SecureLogin in the *Novell SecureLogin Administration Guide.*

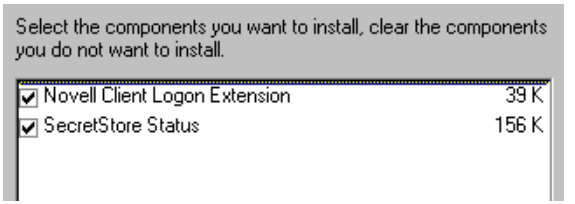
SecretStore supports several products. You can adapt the steps to your product.

1. From the client workstation, log in to the eDirectory tree and server where the SecretStore service is located.

   IMPORTANT: For the NICI software to be installed correctly on Windows NT or Windows 2000, you must be logged in as a user with Administrator rights.

2. Insert the *Novell SecureLogin* CD.
3. Run setup.exe from the secstore\client directory.
4. Follow on-screen prompts to accept the license agreement, provide company information, and select a destination folder.
5. Select components, then click Next.

   The following figure illustrates the Components dialog box:



   As administrator, you'll most likely want all the components on your administrative workstation, even though all the functionality of SecretStore Status is in SecretStore Manager.

   For information about SecretStore Manager, see "SecretStore Manager—Enables users to perform basic maintenance tasks on their SecretStore." on page 12.

   The Novell Client Logon Extension option enables you to automatically be logged in to the servers and trees specified in your login script. See the User Administration\Edit Login Script option, available through the Novell Client icon on the system tray.

SecretStore Status provides an efficient way for a user (or help desk) to test connectivity to the SecretStore service. For information about SecretStore Status, see "SecretStore Status—Enables users to set their master password, unlock SecretStore, switch between eDirectory trees, or switch between eDirectory usernames associated with different trees or servers." on page 13.

6. Select whether to view the readme.txt file, then click Finish.
7. Restart the workstation.

Installing Administrative Tools

To manage SecretStore, you use ConsoleOne and the SecretStore snap-in to ConsoleOne.

1. Install ConsoleOne on your workstation.

   From the Novell SecureLogin CD, run consoleone\c1.exe.

   You might have already installed ConsoleOne when you installed administrative tools for SecureLogin.
2. Install the SecretStore snap-in to ConsoleOne.

   Run consoleone\snapins\sssnapin.exe.

   You might have already installed this snap-in if you installed administrative tools for SecureLogin.

Uninstalling SecretStore

Uninstalling SecretStore on NetWare Servers

You can't uninstall SecretStore from a server. However, you can disable SecretStore.

1. At the server console, unload SecretStore modules from the server.
   - nldap.nlm (LDAP for NDS)
   - ssncp.nlm (The Novell SecretStore NCP Transport plug-in)
   - ssldp.nlm (the Novell SecretStore LDAP Transport plug-in)

You must unload ssldp.nlm and ssncp.nlm before you can unload sss.nlm.

- sss.nlm (the SecretStore service)

2. At a workstation and while logged in as system administrator, map a drive to sys\system: for the server where SecretStore is running.
3. Rename or remove SecretStore NLM files.
   - ssncp.nlm
   - ssldp.nlm
   - sss.nlm
4. In the autoexec.ncf file, comment out or remove the commands that load SecretStore modules.

   If the server is running ldap, simply removing commands from the autoexec.ncf file won't prevent the SecretStore NLMs from loading.
5. Reboot the server.

Although you uninstall SecretStore from a Windows server or disable SecretStore from a NetWare server, the following SecretStore items remain:

- The SecretStore container (the sssServerPolicy object) created by the installation.
- Override (sssServerPolicyOverride) objects that you created.
- Schema extensions.
- Any instantiated SecretStore attributes on User objects.

Uninstalling SecretStore on Solaris and Linux

To uninstall the SecretStore service on a Solaris or Linux server, use the ssscfg utility.

1. Log in as the root user.

   Log in to the host server where you will uninstall the SecretStore service.
2. Run ssscfg.

   Specify the deconfigure option -d as follows:

/usr/sbin/ssscfg [**-h** *hostname*[*:port*]] [**-w** *password*]

[**-a** <*admin FDN*>] **-d** [**-f**] [**-v**]

3. Run the ss-uninstall utility.

Uninstalling SecretStore on Workstations

To uninstall the SecretStore client, use Add\Remove Programs in the Control Panel.

Although you uninstall the SecretStore client, the following SecretStore items remain:

- Users' SecureLogin cache files (c:\program files\novell\securelogin\cache...).
- Any modifications to configuration files such as TLaunch.ini
- Registry settings created during execution (post-install) of the product.

3 Administering SecretStore

This section provides information on the following:

Managing SecretStore Objects

SecretStore Objects

When you install the 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.

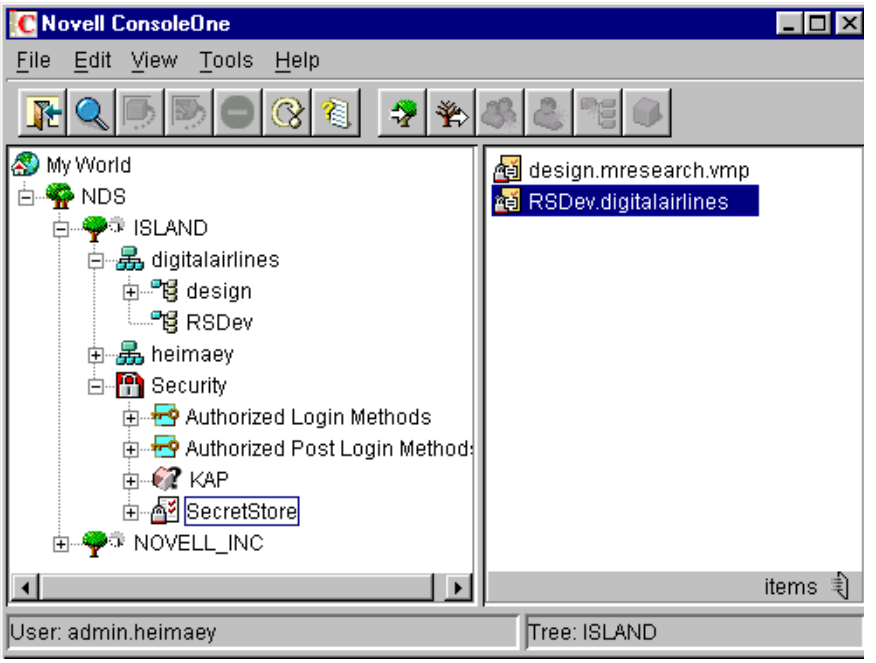
The following figure illustrates this object:

(Figure Description) The SecretStore 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 following figure illustrates an override object:

(Figure Description) sssServerPolicy Override Objects



The SecretStore service first locates the sssServerPolicy object and then, (if one exists) locates and uses an sssServerPolicyOverride object.

Viewing and Changing Settings on Objects

Settings or policies determine SecretStore behavior in eDirectory™.

To view settings for SecretStore objects:

1. In ConsoleOne®, select the sssServerPolicy or an sssServerPolicyOverride object.
2. Right-click, then click Properties > Novell® SecretStore.
3. Select an option (for example, General).

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 an immediate update of the cache is needed, unload and reload the SecretStore service.

Updating the Timestamp

To have the SecretStore service record timestamp information on all ReadSecret operations, check the check box for this setting.

By default, the SecretStore service doesn't update the timestamp. If you want to update the timestamp when a secret is read, check 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, check the check box for this setting. Then users cannot set or use their master password to unlock SecretStore.

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 SSS.NLM program (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

1. Right-click the SecretStore (sssServerPolicy) object, then select New.
2. Select sssServerPolicyOverride, then click OK.
3. In the Name field, enter the name of the group or user that the customized settings will apply to.

   Enter the complete context (for example, design.mresearch.vmp). If the name is incomplete or incorrect, the SecretStore service is unable to match the sssServerPolicyOverride object with the group or user.
4. Set server settings.

   Select the Define Additional Settings check box and customize settings (for example, Disable Master Password Operations). The help system provides information about each setting.

   You can also select the Novell SecretStore > Administrator option to specify SecretStore administrators for this object.

Customizing Security throughout the Tree

Each User or Container object has an sssServerPolicyOverrideDn attribute that can point 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.

As a rule, 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, do the following:

1. Load sss.nlm with -o [complete distinguished name of the override object].

   For example, enter sss -o 2002specs.develop.digitalairlines.

   A SecretStore server must support the override object. The -o 2002specs.develop.digitalairlines flag 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. Right-click the User or Container object, then select Properties.

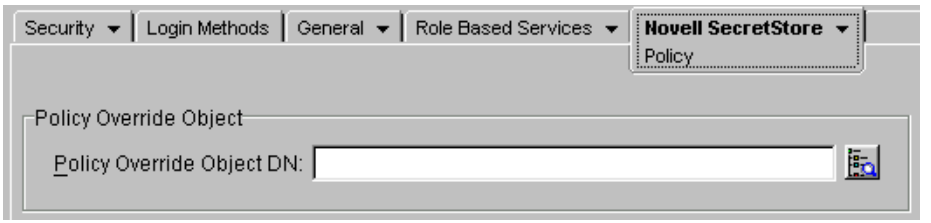
   If the override applies to all users in the container, select the Container object.

3. Click the Novell® SecretStore tab, then click Policy.

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

   This step points the User (or containers) to the sssServerPolicyOverride object by setting the user's (or container's) sssServerPolicyOverrideDn attribute. The following figure illustrates the field where you make this setting:

(Figure Description) Setting an sssServerPolicyOverrideDn Attribute



   The sss/ServerPolicyOverride object is in the SecretStore (sssServerPolicy) container.

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 2002SPECS.

You select Ming's User object and then browse to and select 2002SSPECS. 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 2002SPECS.

Setting Up a SecretStore Administrator

A SecretStore administrator can unlock locked SecretStores. To designate a SecretStore administrator, add that user's User object to the SecretStore Administrator List.

Also, you might want to add additional security. See "Adding Advanced Security" on page 41.

To designate a SecretStore Administrator:

1. In ConsoleOne, right-click the sssServerPolicy object or an sssServerPolicyOverride object, then click Properties.
2. Click Novell SecretStore, then select Administrators from the drop-down list.

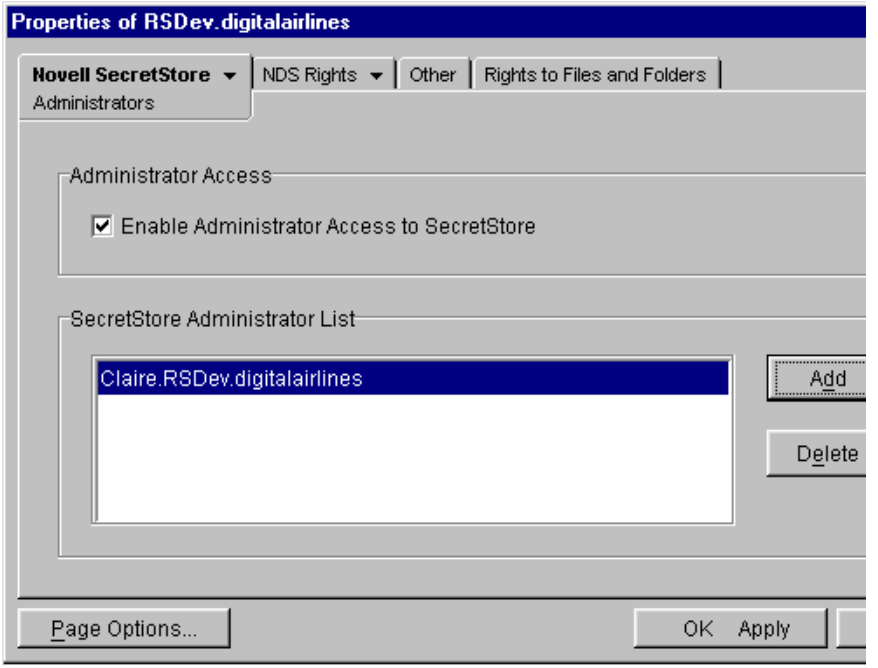
(Figure Description) The Administrators option in ConsoleOne

3. Click Add, navigate to and click the desired User object, then click Select > OK > OK.

   The user is now a SecretStore Administrator.

The following figure illustrates the SecretStore Administrator List:

(Figure Description) The list of SecretStore Administrators



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. (A SecretStore lock occurs when an administrator changes a user's eDirectory password.)

A SecretStore administrator should not have “normal” network administrator rights. This caution 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 avoid bypassing enhanced protection, the two-administrator feature must be split between two or more administrators (one eDirectory administrator, one SecretStore administrator).

If you check the Enable Administrator Access to SecretStore check box, a SecretStore administrator can unlock a user's SecretStore. This is useful when a user forgets a password.

The first time that you add a user to the list, the Enable Administrator Access to SecretStore check box is checked. That user has access to SecretStore.

If you disable the setting and add users, the setting remains disabled until you check the check box.

For more information about this feature, see ““Not Available” Displays for Last Admin Unlock TimeStamp” on page 56.

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.

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.

Example Configuration: Sharing Secrets with Novell Products

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

1. Set up NPS to use SecretStore.

   Make sure that NICI 2.02 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 secretstore.

Henri authenticates to the network. SecureLogin watches for events on Henri's desktop. Henri launches GroupWise, which returns a password dialog. Because it has hooks into the system, SecureLogin recognizes the password dialog and 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
- Both NSL and NPS specify the same credentials (for example, username and password)

For more information on shared secrets, see the following:

- Appendix A, "Sharing Secrets with Novell Portal Services," on page 67
- The Need for Shared Secrets in the *Novell SecureLogin Administration Guide*

Managing Secrets

SecretStore Manager lets users perform basic maintenance tasks on their SecretStore. SecretStore Manager is not intended to be a primary interface to single sign-on functionality. However, it is a relatively simple-to-use tool that can help you manage SecretStore.

To use SecretStore Manager, run SSMANAGER.EXE. For the Novell SecureLogin 3.0 release, this file is on the Novell SecureLogin CD, in the SECSTORE\TOOLS\UTILS directory.

SecretStore Status (SSStatus.exe) is the lite version of SecretStore Manager.

Adding a Secret

1. At the SecretStore Manager main screen, click Options > Add Secret.

   You can also press Insert.

2. Enter a secret identifier.
3. Enter and confirm a secret.
4. (Optional) Check the Add Enhanced Protection check box, then click OK.

   For information about enhanced protection, see "Using Enhanced Protection" on page 46.

Editing a Secret

To edit a secret:

1. At the SecretStore Manager main screen, click Options > Edit Secret.
2. Make changes, then click OK.

   If the secret is a shared secret, you can't edit it. See The Need for Shared Secrets in the *Novell SecureLogin Administration Guide*.

Editing a secret in SecretStore Manager does not change the application's password.

Removing a Secret

To remove a secret:

1. From the SecretStore Manager main screen, select a secret identifier from the Secret Identifier box.
2. Click Options > Remove Secret > Yes.

   You can also use the Delete key.

To quickly remove all test secrets from the Secret Identifiers box, click Tests > Remove All Test Secrets.

Unlocking a Secret

To unlock a locked secret:

1. From the SecretStore Manager main screen, select the locked secret.
2. Click Options > Unlock SecretStore.
3. Type and confirm the previous NDS® password, then click OK.
4. Follow on-screen prompts.

You can also use the Unlock feature in ConsoleOne.

1. In ConsoleOne, right-click the User object, then click Properties.
2. Select the Novell SecretStore tab, then click SecretStore > Unlock.

   The Unlock feature unlocks all secrets that have become locked due to a network administrator changing a user's eDirectory password.

   Only those secrets that were created with enhanced protection have the ability to become locked. See "Using Enhanced Protection" on page 46. You are prompted to enter the previous eDirectory password. If you cannot provide the password, the secret remains locked. You must then delete and recreate the secret.

Viewing a Secret

To view a secret:

1. From the SecretStore Manager main screen, select a secret identifier.
2. Click View > View Secret.
3. Confirm that you are in a secure area by clicking Yes.

You can also view a secret by doing either of the following:

- Select a secretID, then press Enter.
- Double-click a secretID.

Viewing a Secret's Status

You can find out 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
- Who modified the secret

To view a secret's status:

1. At the SecretStore Manager main screen, select a secret identifier.
2. Click Info > Secret Status.

Using Enhanced Protection

Novell SecretStore enables you to provide additional protection by

- Locking SecretStore
- Setting a master password and hint

Locking SecretStore

With the Enhanced Protection option enabled for any secret in Novell SecretStore, if you change 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 only be unlocked if the user provides the last NDS password that was set. Since an administrator should not know the user's previous NDS password, Enhanced Protection-protected secrets 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-protected 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 that 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 will be locked.

Setting a Master Password and Hint

The Enhanced Protection Master Password feature provides an alternative way for users to unlock SecretStore. The Master Password feature enables users to store and update a persistent password in SecretStore. If you (the administrator) reset a user's eDirectory password, SecretStore locks. The user can unlock SecretStore by using the master password instead of the previous eDirectory password.

SecretStore Manager (ssmanager.exe) provides an interface to the master password. This utility enables users to store a hint along with the master password. If users later enter an incorrect password when unlocking SecretStore, SecretStore Manager can display the hint to remind users of the master password.

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

To set a master password and hint, use SecretStore Manager or SecretStore Status.

Using SecretStore Manager

1. Run ssmanager.exe.

   This file is in the secstore\tools\utils directory.

2. Click Options > Set Master Password.

3. Enter a new password, confirm the password, enter a hint, then click Store.

4 Confirm the new password by clicking OK.

Also, you can set the master password from SecretStore Manager by entering the following at the command line:

```
ssmanager.exe /sp
```

This command opens the Create/Edit Master Password dialog box.

Using SecretStore Status

1 Run SSStatus.exe.

2 At the Master Password field, click Set.

3 Enter a new password, confirm the password, enter a hint, then click Store.

4 Confirm the new password by clicking OK.

Using Disconnected Authentication

For performance, secrets from SecretStore in eDirectory or NDS are cached to an encrypted information store on the workstation's Windows directory. This local store persists after the eDirectory authenticated session is closed. For laptop users, this functionality provides access to login data while on the road.

Synchronization occurs when the workstation is started in the eDirectory-connected network, whenever login data is updated in the local store, or when SecretStore shuts down. Access to the local store is granted when the user logs in to Windows.

Single sign-on software (for example, SecureLogin) installation programs include and install the Novell Modular Authentication Service (NMAS) Enterprise Edition client. This client provides single sign-on programs with eDirectory disconnected authentication and password reveal re-authentication features.

By default, single sign-on installation programs (for example, setup.exe in SecureLogin) install the NMAS client and configure the Novell Client™ to display the eDirctory Password fields on the eDirectory login dialog box.

An eDirectory password post-login method stores an NICI-encrypted, hashed copy of the eDirectory password in the registry. SecureLogin then compares

this encrypted password with username and password credentials that the user enters in response to disconnected authentication or re-authentication events.

If users use non-eDirectory password methods, each user must use the eDirectory password method once to establish the password credentials on the workstation. You can then remove the eDirectory password method from the logon process for normal biometric, smartcard, or token authentication to the directory.

Copying SecretStore from One Tree to Another

Using SecretStore Manager, you can copy your SecretStore content from one tree to another.

Scenario: Digital Airlines purchases the AdVentureCo company. The former AdVentureCo employees are given accounts in the DA tree. These employees can authenticate to both trees and copy their secrets from their account in AdventureCo to their new account in the DA tree.

For security, require the user to re-authenticate to the source tree object and ensure that SecretStore is not locked before the copy of information is permitted. Otherwise, someone could steal secrets.

To copy SecretStore to another tree:

1. At the SecretStore Manager main screen, enter the target tree name in the NDS Tree Name field.
2. Enter your distinguished name (for example, sandy.salem.digital) in the Object Name field, then press Enter.

Testing SecretStore

Using SecretStore Manager, you can test the SecretStore service.

Testing the Service

SecretStore reads and writes secrets. The Run SS Test feature in SecretStore Manager enables you to find out whether SecretStore is functional.

For example, you can use Run SS Test if you suspect that secrets are not being created. By default, when you run SS Test from the main window, SecretStore Manager creates five enhanced-protected secrets in SecretStore. You immediately verify the write capabilities of SecretStore.

SS Test also tells you whether your client/server setup is correct and running properly.

To test SecretStore:

1. At SecretStore Manager main screen, click Run SS Test.
2. (Optional) View the secret (data) that was created during the test by double-clicking a secret identifier.

Making Advanced Tests

The Advanced Tests option in SecretStore Manager enables you to test the write APIs.

Add Secret IDs

Use the Add Secret IDs option to test adding a secret, writing a secret, or both. This option uses the AddSecret call and then the WriteSecret call.

Write Secrets Using ID_Create

Use this option to create or write a secret by using the "NSSO_CREATE_ID_F" flag in the API call. This option creates and populates a secret ID with secret data in one step rather than by calling the two-step process.

The difference, however, is that using the NSSO_CREATE_ID_F flag will not prevent a Secret ID name collision in the event that the Secret ID name already exists. This option overwrites the existing secret data in that pre-existing secret ID.

WARNING: You might not want to overwrite a secret.

Number of Secret IDs

Select the number of test secrets. When you run SS Test, SecretStore Manager displays this number of secret identifiers in the Secret Identifier box.

Viewing a Proxy SecretStore

Novell's Proxy SecretStore provides an alternative, secure store for a user's IDs, passwords, and other authentication information that authorized proxy services can access on the user's behalf.

Proxy SecretStore is protected by the same 168-bit triple DES encryption used for “normal” SecretStore. Proxy SecretStore is inaccessible except by authorized server applications. Novell authentication services can read Proxy SecretStore when performance or scalability considerations might not permit the user's initial authenticated connection to eDirectory to be maintained throughout the application session.

A user or administrator might want to check or manage a user's proxy SecretStore. If this user or administrator has proper access rights, that entity might be able to read the secrets stored in proxy SecretStore.

Proxy SecretStore is only available for SecretStore 2.2 and later. Proxy SecretStore might not be represented in the schema or be instantiated on the User object until implemented by a proxy authentication service.

To view a Proxy SecretStore, from SecretStore Manager’s main screen click Options > Proxy SecretStore.

Viewing Information about SecretStore

You can find out the following information about the Novell SecretStore system:

- The level of cryptography running on the server and on the workstation.
- The version of Novell SecretStore running on the server and on the workstation.
- When (timestamp) a SecretStore administrator last unlocked the SecretStore.
- Then distinguished name of the SecretStore administrator that unlocked the SecretStore

To view information about SecretStore, click Info > GetServiceInfo.

The following information is available through Info > GetServiceInfo, provided the administrator has enabled this functionality on the server:

- When a SecretStore administrator unlocked a secret (Last Admin Unlock TimeStamp)
- Who unlocked the secret (Last Admin Unlock DN)

If the functionality hasn't been enabled, these lines display Not Available. See ""Not Available" Displays for Last Admin Unlock TimeStamp" on page 56.

Using Server Commands

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

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

Option	Description
/a	Enable SecretStore administrators
/d	Clear the ACS file and load SSS.DLM without command line parameters
/t	Enable Last Accessed Time Stamp
/m	Disable Master Password
/c=*Minutes*	Cache Refresh Period in Minutes (Minimum 30)
/o=*DN*	NSSO object DN to use. NSSO DN Form: my_nsso_obj.my_orgunit.my_org
/h	For Help
/?	For Help

For the SecretStore 3.0 release, the need to enable the cache with a separate command line parameter has been eliminated. You don't need to use the **/e** option.

An autoexec.ncf file saves command line options in a batch file. These commands are executed when the server starts up. When command line

options are used with server, load the SecretStore Server sss.nlm before nldap.nlm on NetWare inside the autoexec.ncf file. Otherwise, ldap.nlm auto loads the sss.nlm without command line option.

Because eDirectory for Windows NT/2000 does not have an autoexec.ncf file, DHost provides Active Configuration Services (ACS) that work as follows.

In the Windows NT/2000 plus eDirectory environment, the command line options are saved into an ACS file. 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. 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 NT/2000-specific option. It deletes the Windows NT/2000 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, the loading of the server does not require the command line options. The command line options will automatically be read out of 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 option can be used to clear the ACS file and load SSS.DLM without command line parameters.

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

4 Troubleshooting Novell SecretStore

This section contains FAQs and information about error codes.

Frequently Asked Questions

Where to Install

Where do I install the SecretStore service?

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

Setting Up a Tree Key

How do I set up a tree key for eDirectory?

If you are running Novell eDirectory™ 8.5 or later, the tree key is already set up. NetWare® 5.1, later NetWare versions, and the Novell Certificate Server™ automatically set up the tree key.

If you are running NDS® or a version of eDirectory earlier than 8.5, download and install the latest Novell Certificate Server, which is available from the Novell Product Downloads (http://download.novell.com/filedist/PublicSearch) Web site.

Reading Preferences

Why doesn't SecretStore 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.

Scenario: 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.

Merging Trees

If SecretStore is running in separate trees, can I merge the trees without any hit to SecretStore?

No. After the merge, only SecretStore data in the destination tree will be 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/lg/edir87/index.html) in the *Novell eDirectory 8.7 Administration Guide*.

“Not Available” Displays for Last Admin Unlock TimeStamp

Why does Not Available display at the GetServiceInfo screen in SecretStore Manager? The SecretStore Information screen displays “Not Available” for the Last Admin Unlock Timestamp setting.

Most likely, no SecretStore administrator has ever unlocked the user's SecretStore. SecretStore Manager has nothing to report.

SecretStore Manager can’t display any information for the following situations:

- No one has been added to the SecretStore Administrator List in ConsoleOne. See “Setting Up a SecretStore Administrator” on page 39.
- Although someone has been added to the SecretStore Administrator List, the network administrator disabled SecretStore Administrator access to SecretStore before SecretStore was locked.

If someone unlocks a user's SecretStore and then disables SecretStore Administrator access to SecretStore, SecretStore Manager nevertheless reports the timestamp and distinguished name of whoever unlocked the SecretStore.

- Although a SecretStore has been locked, no one has unlocked it.

Error Codes

This section contains a list of error codes that can be generated by the Novell SecretStore service, along with a short description of the error.

Error Code	Description
-800 NSSO_E_OBJECT_NOT_FOUND	Can't find the target object DN in NDS. (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 NSSO_E_NICI_FAILURE	NICI operations have failed.
-802 NSSO_E_INVALID_SECRET_ID	Secret ID is not in the User SecretStore.
-803 NSSO_E_SYSTEM_FAILURE	Some internal operating system services are not available.
-804 NSSO_E_ACCESS_DENIED	Access to the target SecretStore has been denied.
-805 NSSO_E_NDS_INTERNAL_FAILURE	Some internal NDS services are not available.
-806 NSSO_E_SECRET_UNINITIALIZED	Secret has not been initialized with a write.

Error Code	Description
-807 NSSO_E_BUFFER_LEN	Size of the buffer is not in a nominal range between minimum and maximum. Possible cause: The programmer or vendor that wrote the connector for the application did not meet requirements.
-808 NSSO_E_INCOMPATIBLE_VERSION	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. Possible action: Upgrade your server to the latest version of SecretStore.
-809 NSSO_E_CORRUPTED_STORE	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.

Error Code	Description
-810 NSSO_E_SECRET_ID_EXISTS	Secret ID already exists in the SecretStore. Possible cause: Using the Add option, you are trying to add a secret ID. The system informs you that the secret already exists.
-811 NSSO_E_NDS_PWORD_CHANGED	The network administrator has changed the user's NDS password. SecretStore is now locked. Possible action: If an application is locked, use SecretStore Manager or SecretStore Status to unlock SecretStore.
-812 NSSO_E_INVALID_TARGET_OBJECT	Target NDS User object not found. Possible cause: During a logon process, you passed the ResolveName process. However, the SecretStore service cannot find the target NDS User object to read a SecretStore in eDirectory.
-813 NSSO_E_STORE_NOT_FOUND	Target 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.

Error Code	Description
-814 NSSO_E_SERVICE_NOT_FOUND	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. Possible actions: ◆ Install SecretStore on a server. ◆ Make sure that SSS.NLM is running on a SecretStore server.
-815 NSSO_E_SECRET_ID_TOO_LONG	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. Possible action: Contact the vendor.
-816 NSSO_E_ENUM_BUFF_TOO_SHORT	The length of the enumeration buffer is too short. Possible cause: A programmer needs to make a call again to a larger buffer. NSSO returns what data it can in the buffer that was passed. Possible action: The maximum buffer size is 128KB. The maximum packet size is also 128KB. If you have more secrets IDs in SecretStore than 128KB, use wild cards to change the scope of your enumerations. Change the scope at the API level or in SecretStore utilities.

Error Code	Description
-817 NSSO_E_NOT_AUTHENTICATED	The user is not authenticated. Possible cause: A SecretStore server was found, but the SecretStore client was unable to open a connection. Possible action: Log in to eDirectory again.
-818 NSSO_E_NOT_SUPPORTED	Unsupported operations. Possible cause: A feature is published during beta but is not yet implemented.
-819 NSSO_E_NDS_PWORD_INVALID	The NDS password is not valid. Possible cause: You tried to unlock SecretStore, but you incorrectly entered a password. Possible action: Enter the correct password.
-820 NSSO_E_NICI_OUTOF_SYNC	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 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. Possible action: Try to run the application again.

Error Code	Description
-821 NSSO_E_SERVICE_NOT_SUPPORTED	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 the particular service.
-822 NSSO_E_TOKEN_NOT_SUPPORTED	The 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 NSSO_E_UNICODE_OP_FAILURE	A Unicode* text conversion operation failed. Possible cause: SecretStore tried to translate Unicode but was unable to. Possible action: Try again.
-824 NSSO_E_TRANSPORT_FAILURE	The server connection has been lost. Possible action: Wait for the server to reboot, or log in again.
-825 NSSO_E_CRYPTO_OP_FAILURE	A cryptographic operation has failed. Possible cause: When SecretStore tried to encrypt of decrypt data, the key or data was corrupted. Possible action: Try again.

Error Code	Description
-826 NSSO_E_SERVER_CONN_FAILURE	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. Possible action: Ask the system administrator to load the Transport plug-in modules on the server.
-827 NSSO_E_CONN_ACCESS_FAILURE	Access to a server connection failed. Possible cause: A SecretStore client could not get exclusive hold of a connection table on the client.
-829 NSSO_E_SECRET_BUFF_TOO_LONG	The size of the secret buffer exceeds the limit. Possible action: Make the secrets smaller.
-830 NSSO_E_SECRET_ID_TOO_SHORT	The length of the secret ID should be greater than zero. Possible cause: The secret ID is zero. You have specified a null ID. Possible action: Contact the application vendor.
-831 NSSO_E_CORRUPTED_PACKET_DATA	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. Possible action: Try again.

Error Code	Description
-832 NSSO_E_EP_ACCESS_DENIED	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. Possible action: Try again. Pass the enhanced protection password or enter a master password. Otherwise, contact the application vendor.
-833 NSSO_E_SCHEMA_NOT_EXTENDED	The 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 NDS schema has not been extended. Possible action: Reinstall SecretStore.
-834 NSSO_E_ATTR_NOT_FOUND	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. Possible action: Configure the system.
-835 NSSO_E_MIGRATION_NEEDED	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.

Error Code	Description
-836 NSSO_E_MP_PWORD_INVALID	The master password could not be verified to read or unlock the secrets. Possible cause: You entered an incorrect master password. Possible action: Correctly enter the master password.
-837 NSSO_E_MP_PWORD_NOT_SET	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. Possible action: Set a new master password.
-838 NSSO_E_MP_PWORD_NOT_ALLOWED	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 NSSO_E_WRONG_REPLICA_TYPE	Not a writable replica of 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. Possible action: Go to a different replica. Set up SecretStore so that a user can always go to a writable replica.
-840 NSSO_E_ATTR_VAL_NOT_FOUND	The SecretStore service didn't find an attribute value (secret ID) that you are trying to read.

Error Code	Description
-843 NSSO_E_CONFIG_NOT_SUPPORTED	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 for whatever reason. Possible actions: 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.
-888 NSSO_E_NOT_IMPLEMENTED	This feature is not yet implemented. Possible cause: A feature is published during beta but is not yet implemented.
-899 NSSO_E_BETA_EXPIRED	The product beta life has expired. Purchase an officially released copy.

A Sharing Secrets with Novell Portal Services

Novell® SecretStore® stores secrets in eDirectory™. Other information solutions, for example, Novell Portal Services (NPS) and Novell iChain®, can share these secrets. This section explains how to set up NPS 1.5 to use shared secrets:

- "Specifying an NPS SecretStore Provider" on page 67
- "Configuring NPS to Share Secrets" on page 69

Specifying an NPS SecretStore Provider

IMPORTANT: Novell SecretStore must communicate with LDAP through Secure Sockets Layer (SSL). For instructions on setting up SSL, see Secured Sockets Layer (SSL) in the *Novell Portal Services Configuration Guide*.

To configure SecretStore as the NPS secretstore provider, add a setting to one of the following:

- The PortalServlet properties file
- The Portal Configuration

Adding a Setting to the PortalServlet.properties file

1. Open the PortalServlet.properties file.

   In NetWare 6, this file is typically in the sys:\webapps\nps\web-inf directory.

   In UNIX, LINUX, and Windows 2000, this file is wherever you installed the webapps\nps\web-inf directory.

2. Add the following line:

   ```
   AuthSSProvider=com.novell.nps.authentication.sso.NovellSSAPI Impl
   ```

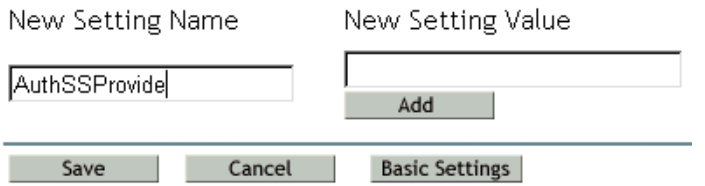
3. Save the file.

Adding a Setting to the Portal Configuration Object

1. In Novell Portal Services, click Administer the Portal > Portal > Configuration > All Settings.

   In the New Setting Name text box, type AuthSSProvide.

(Figure Description) The New Setting Name text box



2. In the New Setting Value box, type the following:

   ```
   =com.novell.nps.authentication.sso.NovellSSAPI Impl
   ```

3. Click Add > Save > OK.

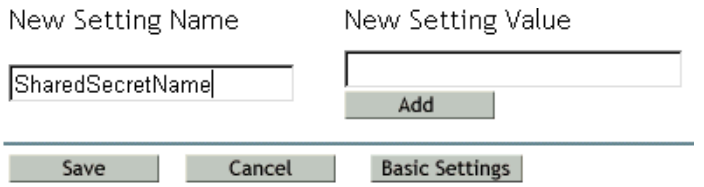
Configuring NPS to Share Secrets

Novell Portal Services can share secrets with other Novell technologies, such as SecureLogin and Novell iChain.

To configure NPS to share secrets for gadget instances:

1. In Novell Portal Services, click Administer the Portal > Pages.
2. Click a currently configured page (for example, Portal Administration) > Edit.
3. Click a gadget assignment configured on this page (for example, AdminService) > Edit.
4. Click All Settings.
5. In the New Setting Name text box, type SharedSecretName.

(Figure Description) The New Setting Name text box



6. In the New Setting Value text box, type the name of the shared secret.

   If the secret that you want to share already exists in Novell SecretStore, use SecretStore Manager to discover the secret that you need to type. See “Viewing a Secret” on page 45.

B Documentation Updates

This section contains new or updated information on installing and managing Novell® SecretStore.

This documentation is also provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section. See Novell SecretStore 3.0 (http://www.novell.com/documentation/lg/secretstore30/index.html).

If you need to know whether a copy of the PDF documentation you are using is the most recent, check the date that the PDF file was published. The date is in the Legal Notices section, which immediately follows the title page.

The documentation was updated on the following dates:

January 15, 2003

The Sharing Secrets topic was updated:

Sharing Secrets

Location	Change
"Sharing Secrets" on page 42	Added information on sharing secrets that are accessed remotely.

March 7, 2003

Location	Change
Appendix A, “Sharing Secrets with Novell Portal Services,” on page 67	Added information on how SecretStore and Novell Portal Services can share secrets.