Novell SecureLogin

6.0

www.novell.com

INSTALLATION GUIDE

March 24, 2006

Novell®

Legal Notices

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

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

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

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

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

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This document contains information on the following:

Documentation Conventions

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

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

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

Feedback

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

Documentation Updates

For the most recent version of the *Installation Guide*, visit the Novell Documentation Web site (http://www.novell.com/documentation).

Additional Documentation

This *Installation Guide* is a part of documentation set for SecureLogin 6.0. Other documents include:

- The SecureLogin 6.0 Administration Guide (tools and tasks to manage SecureLogin and configure terminal emulators)
- The SecureLogin 6.0 Application Definition (concepts concerning scripting, scripting commands, and example scripts for applications)
- The SecureLogin 6.0 User Guide

- The SecureLogin 6.0 Terminal Services Guide
- The SecureLogin 6.0 Guide for Terminal Emulators

Overview

1

This section provides information on the following:

1.1 Supported Platforms

Novell® SecureLogin 6.0 supports the platforms given below. The latest support packs are recommended for all platforms.

1.1.1 Servers

- OES SP 1 server with eDirectory 8.7.3
- eDirectory 8.8 on OES SP 1 (Netware only) and eDirectory 8.8 on SLES 9.1
- Novell eDirectory on NetWare 6.5 SP 4

  If you run Novell SecretStore® on Linux, refer to the following table:

Table 1-1 *SecretStore Versions*

eDirectory Version	Version of SecretStore to Use
eDirectory 8.7.3	SecretStore 3.3.5
eDirectory 8.8	SecretStore 3.4

  You can download the server version of SecretStore 3.3.5 from the Novell Web site (http://developer.novell.com/ndk/ssocomp.htm)

  In the non-SecretStore mode, SecureLogin runs against eDirectory on any platform.

  SecureLogin 6.0 for eDirectory supports only iManager® 2.5 or later.
- Microsoft* Windows 2000 Server, Terminal Server, or Advanced Server with Active Directory*.
- Microsoft Windows 2003 Server or Terminal Server with Active Directory.
- Servers running LDAP-compliant directories.

1.1.2 Browsers

- Internet Explorer 5.5 or later
- Netscape 4.7.x
- Mozilla Firefox 1.0.x

NOTE: If you install the Mozilla Firefox browser after the installation of SecureLogin, you have to manually add the following extension file using the command line:

```
firefox.exe -install-global-extension
"<securelogin_dir>\slomoz.xpi"
```

Depending on workstation configurations, the browsers might behave differently.

1.1.3 Workstations

- Windows 2000 Professional
- Windows 2003
- Windows XP

If SecureLogin is to access eDirectory over Netware Core Protocols™, Windows 2000 or Windows XP machines should have Novell Client 4.90 SP2 or 4.91 SP2. If you use LDAP, the Novell client is not required.

SecureLogin supports the default Windows shell, `explorer.exe`.

The SecureLogin snap-in to iManager requires iManager 2.5.

1.2 Deploying SecureLogin

This section provides information on the following:

1.2.1 Installing Java

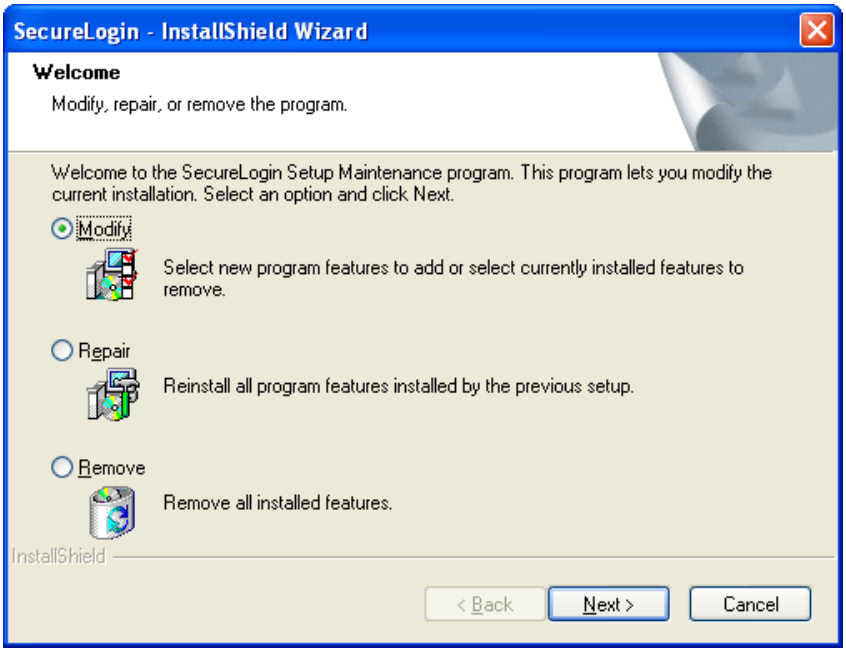
SecureLogin 6.0 supports Java applications. However, during installation the Java Applications component is displayed and available only if Java is installed on your workstation. To check if Java is installed in your system and to download the Java Application:

1. Go to Add/Remove Programs in the Control Panel and verify if Java is installed in your system.
2. If Java is not installed, download and install the Java Runtime Environment from the Java Download Web site (http://www.java.com/en/index.jsp).

1.2.2 Selecting Modify, Repair, or Remove

If you previously installed SecureLogin, InstallShield detects the installation and displays the following dialog box:

Figure 1-1 *InstallShield Wizard*



You can use the Modify operation to change components listed in the Select Components dialog box.

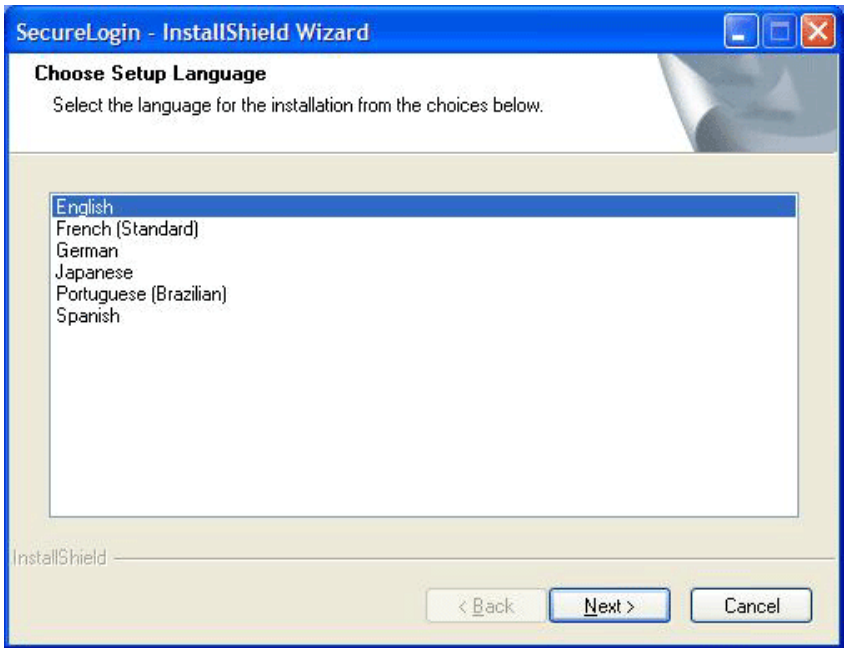
However, you can’t change options that aren’t listed. For example, you can't use Modify to change the platform.

Scenario: Changing a SecureLogin Platform. You previously installed the Standalone option to evaluate SecureLogin. After a successful evaluation, you install SecureLogin throughout the company, which is using eDirectory. Because you can’t migrate from Standalone to eDirectory, you select Remove, uninstall SecureLogin, restart the workstation (if prompted), then reinstall.

You can select the Repair option if you want to install any missing components. The installation program detects previously installed components and reinstalls them.

1.2.3 Selecting a Setup Language

You can install SecureLogin by inserting the CD or by running `setup.exe` found in the `securelogin/client` directory. The following dialog box is displayed.



Select a language for installation, from the list and click *Next.* The installation proceeds in the language of your choice.

1.2.4 Using a Silent Install

A silent install provides InstallShield Wizard with instructions for installing SecureLogin. To use a silent install, you have to create and use a response file. The response file contains your responses to the dialog boxes that you encounter during the installation.

1. Run the installation in the environment that you want the silent installation to run.

   Do this before you create a response file, so that you are familiar with the installation process.

2. Set up a response file by typing

   ```
   Setup.exe -r -f1"c:\setup.iss"
   ```

   The -r parameter instructs InstallShield to record the installation.

   The -f1 parameter specifies a filename and absolute path where the response file will be saved. If you omit this parameter, InstallShield saves the file to a default directory.

   No space exists between f1 and the first double quotation mark (f1"). Even if you choose not to use double quotation marks, don't place a space after f1.

   Although the double quotation marks aren't always required, they are required for long paths. You're safer by always including them.

   The path must be absolute, rooted with a drive letter (for example, c). Don't use a relative path.

   The default filename is setup.iss. However, you can specify any name, including the extension. Setup.iss is a text file.

Also, the data in the response file depends on the workstation and options that you select to create the response file.

Scenario: Incompatible Workstations. You create the response file on a Windows 2000 workstation and then silently install on a Windows 2003 workstation. The installation fails.

Scenario: Missing Software. You create a response file on a workstation that has the Novell Client. You then install silently on a workstation that doesn't have the Novell Client. The installation fails.

3 (Optional) Set up a log file by adding the following parameters:

```
-f2"C:\setup.log"
```

The path to the log file is also absolute.

The complete entry, with the command, parameters for a response file, and parameters for a log file, appears as follows:

```
Setup.exe –r -f1"C:\setup.iss" -f2"C:\setup.log"
```

A silent install doesn't display the user interface. If problems arise, you need some mechanism to identify what isn't working as expected

4 Run the installation.

InstallShield records all your responses to options in the dialog boxes.

5 Use the response file and the log for silent installs.

A log file captures install information as result codes. If the result code is 0, the installation was successful. If other result codes appear, refer to the InstallShield documentation.

If you run setup.exe on a workstation that already has SecureLogin, the installation program goes to the Modify/Repair/Remove dialog box. Therefore, if you test the response file by running the silent install on the same workstation, uninstall SecureLogin first. Otherwise, the installation launches the maintenance dialog box and then writes an error code to the log file, indicating that the .iss file wasn't able to respond to the dialog boxes.

IMPORTANT: After a silent install, you have to reboot the system for SecureLogin to take effect. Otherwise, you might encounter the error message Unable to instantiate ScriptBroker module: 80040154.

You can also create silent Modify, Repair, and Remove response files.

Scenario: Using Silent Modify to Update Workstations. During a Phase 1 rollout, you silently installed SecureLogin on users' workstations, but didn't install the Secure Workstation component. Wanting users to have Secure Workstation functionality during the Phase 2 rollout, you create a response file by selecting Modify and the Secure Workstation component. You then update users' workstations by running silent installs with the new response file.

1.2.5 Automating the Installation

By editing the `automate.ini` file, you can automate parts of the installation and customize it before distributing SecureLogin to users or other installers.

1 Open `automate.ini`, found in the `\securelogin\client directory`

Read the explanatory paragraphs so that you understand how to customize the installation.

2 Make changes.

The following figure illustrates the dialog box that enables you to pre-select a Complete or Custom installation.

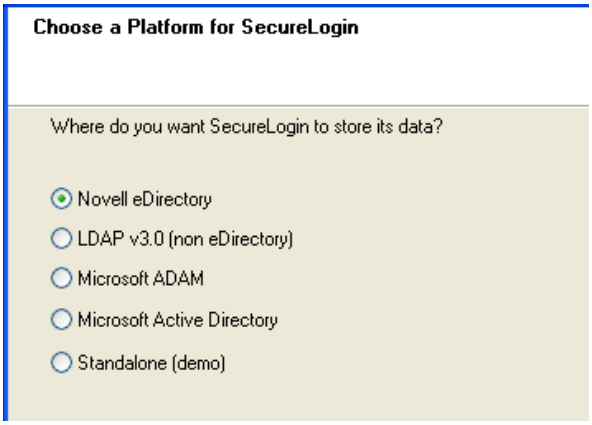
The [SetupType] section in automate.ini determines whether the dialog box appears

```
[SetupType]
;ShowDialog=No
;Selection=Complete
;Selection=Custom
```

By default, the dialog box displays. If you uncomment the `ShowDialog` line, the dialog box does not appear, and the installation program installs the Complete option by default.

The following figure illustrates the dialog box that enables users to select a platform:

Figure 1-2 *Choosing a Platform*



The [Platform] section in automate.ini determines whether the dialog box appears:

```
[Platform]
;ShowDialog=No
;Selection=eDirectory
;Selection=LDAP
;Selection=ADAM
;Selection=ActiveDirectory
;Selection=Standalone
```

By default, the Choose a Platform dialog box displays. If you uncomment the ShowDialog and Selection=eDirectory lines, the dialog box does not appear. Instead, the installation program installs the eDirectory option by default.

3 Save and exit.

Smartcard Configuration for automate.ini

If you want to use smart card and if ActivClient is installed on your workstation do the following:

- Comment the lines that begin with `Selection` and `Location`.
- Uncomment the line that begins with `SecondaryStorage`.
- Change `SecondaryStorage` to `SmartCard`.

NOTE: Make sure you write SmartCard exactly the way shown above as it is case sensitive.

If you want to use smart card and if ActivClient is not installed on your workstation do the following

- Uncomment the lines that begin with `Selection`, `Location`, and `SecondaryStorage`.
- Change `SecondaryStorage` to `SmartCard`.

NOTE: Make sure you write SmartCard exactly the way shown above as it is case sensitive.

- Change `Selection` to the required Cryptographic Service Provider.
- Change `Location` to the path where the PKCS#11 compatible library is present.

If you do not want to use smart card, then do the following:

- Comment the lines that begin with `Selection` and `Location`.
- Equate SecondaryStorage to FILE.

NOTE: Make sure FILE is written in upper case as it case sensitive.

NMAS Methods Configuration for automate.ini

If you want to install NMAS methods, uncomment and equate the corresponding method to `Yes`.

If you do not want to install NMAS methods, leave the corresponding method commented.

1.3 Installing SecureLogin on Servers

1.3.1 SecureLogin on Windows

You can install SecureLogin on Windows 2000 or Windows 2003 server.

To administer SecureLogin in an Active Directory environment, you must install SecureLogin on a Windows 2000 server. The installation process is the same for these servers as for installing SecureLogin on workstations

If an error appears during an attempted login immediately after you install SecureLogin on an Active Directory server, click *OK* in the error message, wait for a few minutes, then try again. This error occurs because Active Directory takes time to synchronize. If the error continues, you might need to restart the server.

1.3.2 SecureLogin and SecretStore in NetWare Environments

To administer SecureLogin, you use an administrative tool on the desktop such as iManager in the eDirectory environments.

SecureLogin has a SecretStore client option that you can use in Novell eDirectory environments. The SecretStore option provides additional security. If you want to use the SecretStore option along

with SecureLogin, you must install SecretStore server components on a NetWare server and then install the SecretStore client on workstations.

You have to install SecretStore server components on the server before installing SecureLogin on a workstation. The SecretStore client is installed while installing SecureLogin on a workstation. The current primary tree and server connections must be set to the tree where the SecretStore service has been installed. For information on installing SecretStore, see "Installing SecretStore" (http://www.novell.com/documentation/secretstore33/index.html) in the SecretStore 3.3.3 Administration Guide.

1.4 Some Tips Concerning Workstations

SecureLogin 6.0 does not support workstations running Windows 95 or 98 and NT Domain environments.

For Windows 2000 and Windows XP Professional workstations using NetWare Core Protocol, install the Novell Client ™ 4.90 SP2 or 4.91 SP2.

This section contains the follwoign information:

- Section 1.4.1, "NICI," on page 18
- Section 1.4.2, "NMAS," on page 18

1.4.1 NICI

The Novell International Cryptographic Infrastructure (NICI) is required for you to use SecureLogin on the following:

- eDirectory LDAP platform
- An LDAP platform that does not use eDirectory
- The SecretStore Client feature
- The NMAS™ Client feature

If NICI is not already installed on your workstation, the SecureLogin installation program automatically installs it. If you have an earlier version of NICI, the installation program detects it and then updates it to the later version. NSL 6.0 requires NICI 2.6.8.

If you uninstall SecureLogin, NICI is not uninstalled.

The path to the NICI installation is in the `SecureLogin/Client/automate.ini` file found in the SecureLogin Installation CD. You can turn off the NICI autolaunch by commenting out the paths for NICI.

1.4.2 NMAS

When you install SecureLogin, the Novell Modular Authentication Service (NMAS) clientcan be installed as well. SecureLogin 6.0 requires NMAS 3.2.

If you have an earlier version of NMAS, the installation program detects it and then updates it to the later version.

If you uninstall SecureLogin, NMAS is not uninstalled.

To turn off the NMAS autolaunch, comment out the paths for NMAS in the `SecureLogin/Client/automate.ini` file found in the SecuerLogin Installation CD.

IMPORTANT: Make sure Novell Client 4.91or later is installed in your machine, before installing NMAS 3.x .

Installing in Novell eDirectory Environments

2

This section provides information on the following:

WARNING: If you are upgrading and are using SecretStore, upgrade SecretStore on your server to version 3.3.5 before installing SecureLogin 6.0. Otherwise, secrets might be lost.

2.1 Extending the eDirectory Schema

The Novell® eDirectory™ schema must be extended in order to enable SecureLogin to save users' single sign-on information. Ndsschema.exe extends the eDirectory schema and grants rights to existing users so that they can use SecureLogin.

To extend the schema of a given tree, you must have sufficient rights over the [root] of the tree.

1 Run `ndsschema.exe`.

Typically, this file is in the `securelogin\tools` directory. However, if you unzipped it to the Temp directory on a Windows 2000 workstation, you might need to unhide the Local Settings directory and then locate ndsschema.exe in the following path:

```
c:\Documents and settings\Administrator\Local
Settings\Temp\Securelogin\Tools
```

Make sure that you have the Novell Client 4.91 or later installed in your machine. Extending the schema might take some time to filter throughout your network, depending on the size of your network and the speed of the links.

When the NDS® or eDirectory schema is extended, the following attributes are added:

- Prot:SSO Auth
- Prot:SSO Entry
- Prot:SSO Entry Checksum
- Prot:SSO Profile
- Prot:SSO Security Prefs
- Prot:SSO Security Prefs Checksum

For information on these attributes, see Section 4.4, “Extending the Active Directory Schema,” on page 50.

2 Specify an eDirectory context so that SecureLogin can assign rights to User objects under that context.

You will be prompted to define a context where you want the User objects' rights to be updated, allowing users access to their own single sign-on credentials. The following figure illustrates this prompt:

If you don’t specify a context, rights begin at the root of the eDirectory tree.

Only the rights on Container objects are inherited. These rights flow to subcontainers, so that users can read attributes. User rights aren’t inherited.

If the installation program displays a message similar to -601 No Such Attribute, you have probably entered an incorrect context or included a leading dot in the context.

3 (Conditional) Grant rights to local cache directories.

Users on Windows 2000, and Windows XP must have workstation rights to their local cache directory locations. To grant rights, do one of the following:

- Grant rights to the user’s cache directory (for example, `c:\programfiles\novell\securelogin\cache\v2slc\username`)

  The default location is the user’s profile directory. By default, the user already has rights to this directory. However, if the user specified an alternative path during the installation, you might need to grant rights to the cache directory.
- During the installation, specify a path to a location that the user has rights to (for example, the user’s documents folder).

2.1.1 Granting SSO Rights to New Users

The SecureLogin iManager plug-in does not assign SSO rights to any newly created users after the schema is extended. To give write permission for SSO attributes:

1 Log in to iManager.

2 Click the *Modify Trustees* link from the Rights task.

3 Select the context to which you need to apply SSO rights.

4 Click the *Assigned Rights* link corresponding to that context.

5 Click the *Add Property* button.

6 Select *Prot:SSO* Entry attribute, then click *OK*.

7 Repeat Step 5 and Step 6 to add all properties beginning with ‘Prot’.

8 Check the *Write* and *Inherit* checkboxes for all the newly-added attributes.

9 Click *Done*.

10 Click *OK*.

11 Click *OK*.

2.2 If You Plan to Use the SecretStore Client

You can use SecureLogin along with the patented Novell SecretStore® client/server system to provide the highest possible level of security for user login data. SecretStore requires server components on the eDirectory server and SecureLogin client software with SecretStore client, on workstations.

To determine whether SecretStore is installed on a NetWare server:

1 At the server console, type `nwconfig`, then press Enter.

2 Select *Product Options* > *View/Configure/Remove Installed Products*, then press Enter.

3 Scroll to find the SecretStore product (for example, SS 3.3.5 Novell SecretStore).

You can also use iManager. If SecretStore is installed, the SecretStore object is displayed in the Security container.

If SecretStore is not installed, see "Installing SecretStore" in the SecretStore 3.3.3 Administration Guide (http://www.novell.com/documentation/secretstore33/index.html)

To install the SecretStore client:

1 Upgrade SecretStore on the server.

Upgrade SecretStore on your server to version 3.3.5 if you are using eDirectory 8.7.3 and SecretStore 3.4 if you are using eDirectory 8.8.

WARNING: If you do not upgrade SecretStore on your server, secrets might be lost.

---

2 Select the *SecretStore* option when you install SecureLogin on workstations.

2.3 Installing SecureLogin: eDirectory

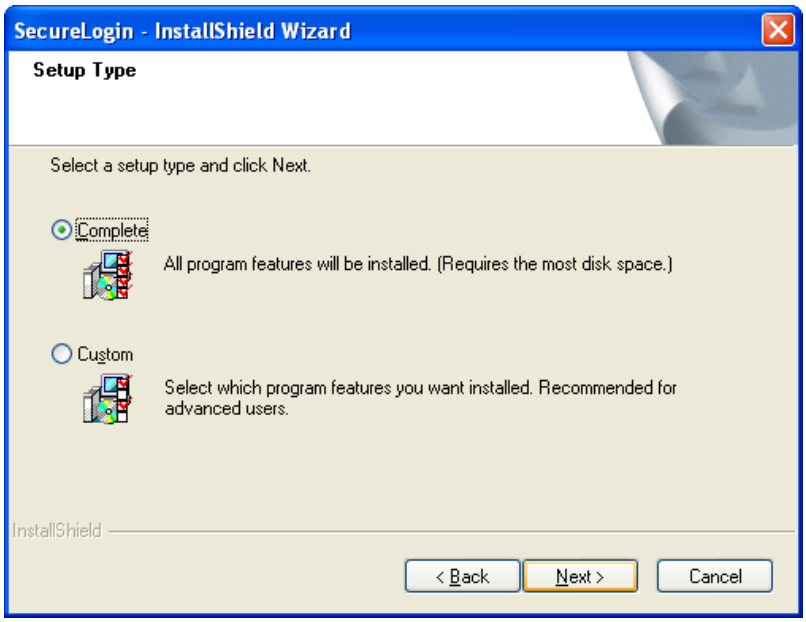
The Novell eDirectory option installs SecureLogin onto networks that are running eDirectory. This option provides secure, centralized storage of user login data by performing encryption once on the workstation before the data is saved to eDirectory.

1 Run `setup.exe`, found in the `securelogin\client` directory.

2 Select a language, click *Next*.

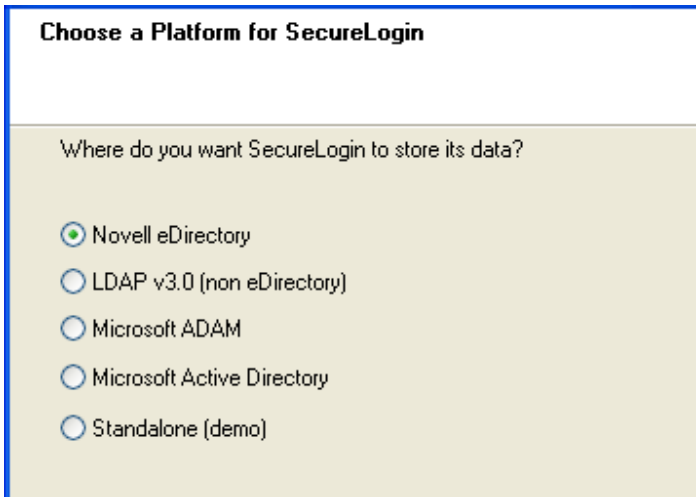
3 Accept the license agreement, then click *Next*.

4 Select *Complete*, then click *Next*.

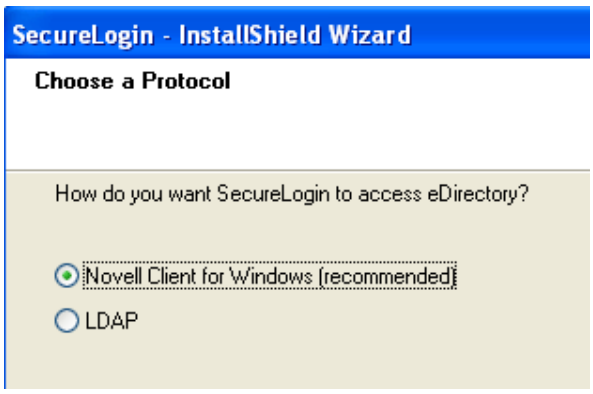


The Complete option uses default values and installs SecureLogin in `c:\program files\novell\securelogin`. For options available through the Custom option, Section 2.3.1, "Using the Custom Option for Novell eDirectory," on page 28.

5 Select *Novell eDirectory* as the platform where SecureLogin will store its data, then click *Next*.



6 Select *Novell Client for Windows or LDAP*, then click *Next*.

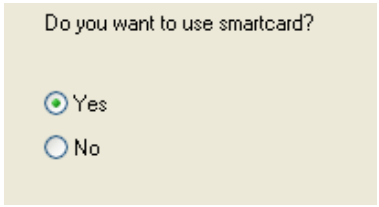


If the Novell Client™ is installed, the installation program recommends that option. Otherwise, LDAP is recommended.

NOTE: The above screen is displayed only if you have Novell Client for Windows installed on your machine. Otherwise, LDAP is auto-selected as the protocol.

---

7 (Conditional) If you don't want to use smartcard, select *No,* click *Next,* then continue with Step 10.

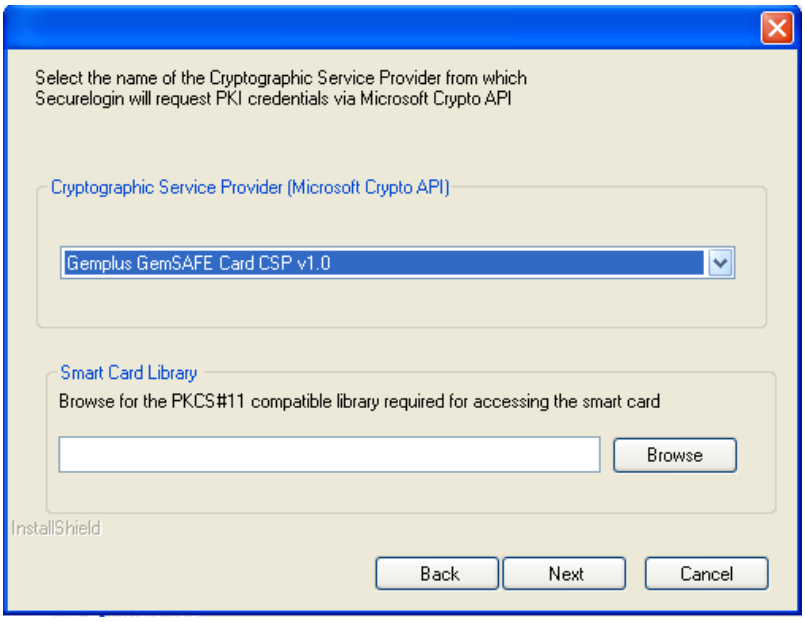


8 (Conditional) If you want to use smartcard and if ActiveClient is detected in your system, select *Yes,*Click *Next,* then continue with Step 10.

9 (Conditional) If you want to use smartcard and if ActiveClient is not detected in your system:

9a Select *Yes,* click *Next.*

9b (Conditional) Select a cryptographic service provider from which SecureLogin will request PKI credentials via Microsoft Crypto API.



9c Select a PKCS#11 compatible library required for accessing the smartcard, then click *Next*.

NOTE: This will speciy the location of the Cryptographic Token Interface installed as part of the smartcard vendor's software. These API files will be used by SecureLogin to communicate with the smartcard.

Manually configuring the third party smartcard PKCS library Assumes a high level of understanding the Cryptographic Service Provider's product.

For more information and instructions about smartcard settings and cryptographic tokens, see the *Novell SecureLogin 6.0 Administration Guide*.

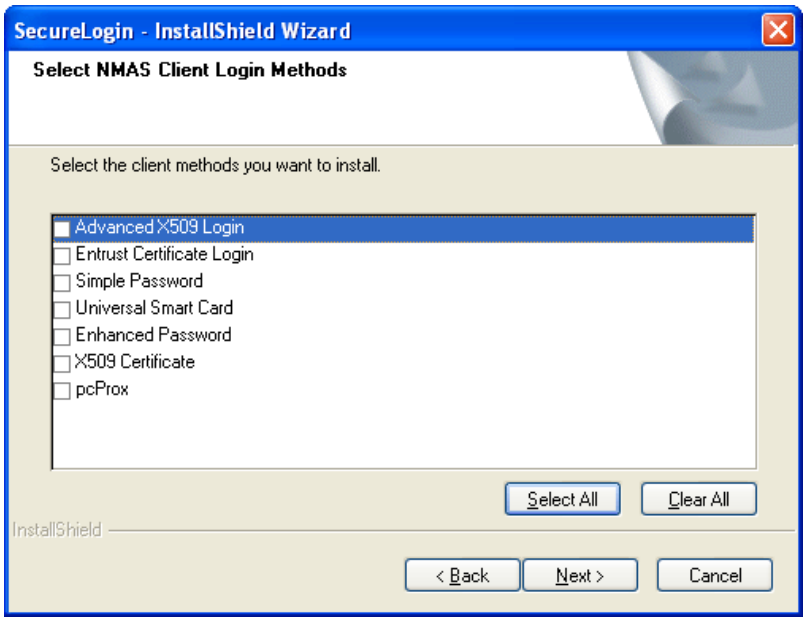
---

10 Select whether SecureLogin is to install the SecretStore client, the NMAS™ client, or both, then click *Next*.

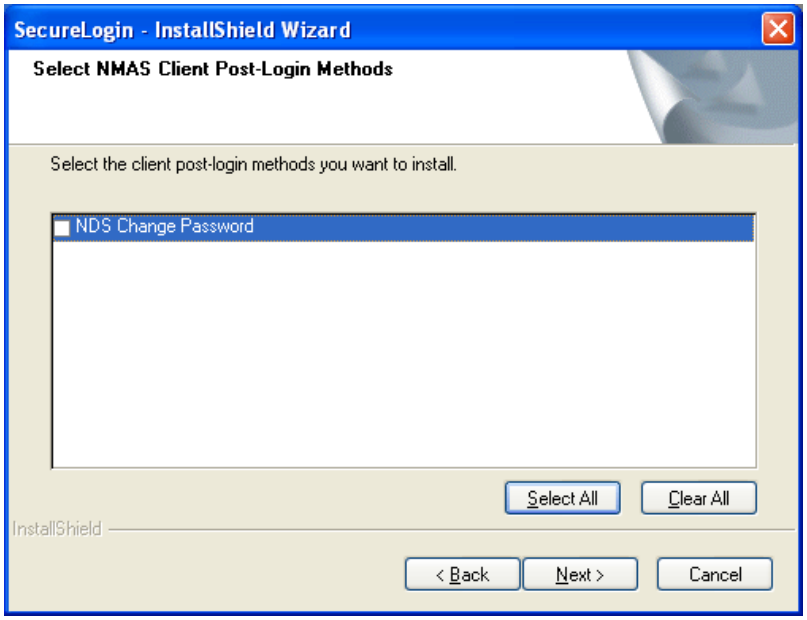
IMPORTANT: Select Novell SecretStore only if SecretStore is installed on a server. For information on SecretStore, see the *SecretStore 3.3.3 Administration Guide* (http://www.novell.com/documentation/secretstore33/index.html)

---

11 (Conditional) If you selected the NMAS client, select one or more NMAS login methods, then click *Next*.



12 Select post-login methods, then click *Next*.



13 Click *Install*.

14 By default, the Launch Readme option is selected. Click *Next*.

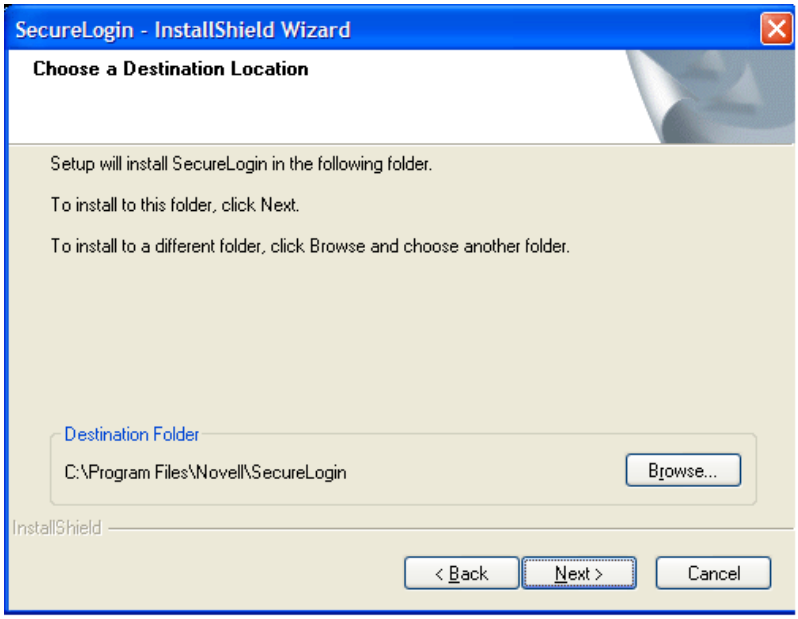
15 Click *Finish*.

16 Select when you want to restart your workstation, then click *OK*.

2.3.1 Using the Custom Option for Novell eDirectory

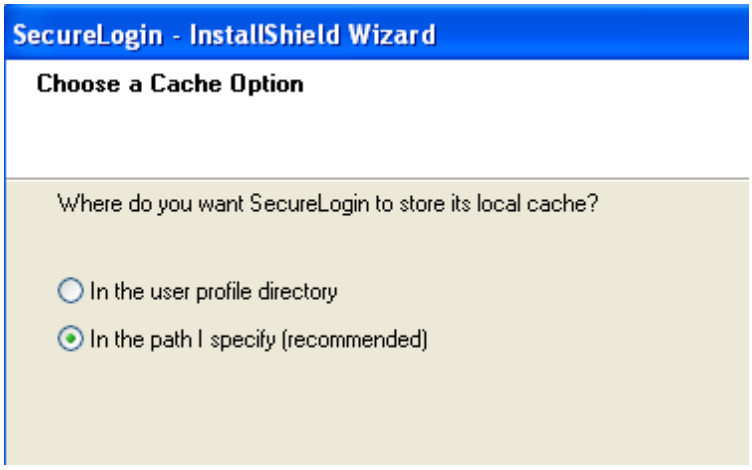
The Custom option provides the same defaults as does the Complete option, but enables you to do the following:

- Specify where SecureLogin files will be stored.



You can use the default path or specify a different one.

- Specify a path for SecureLogin's local cache.

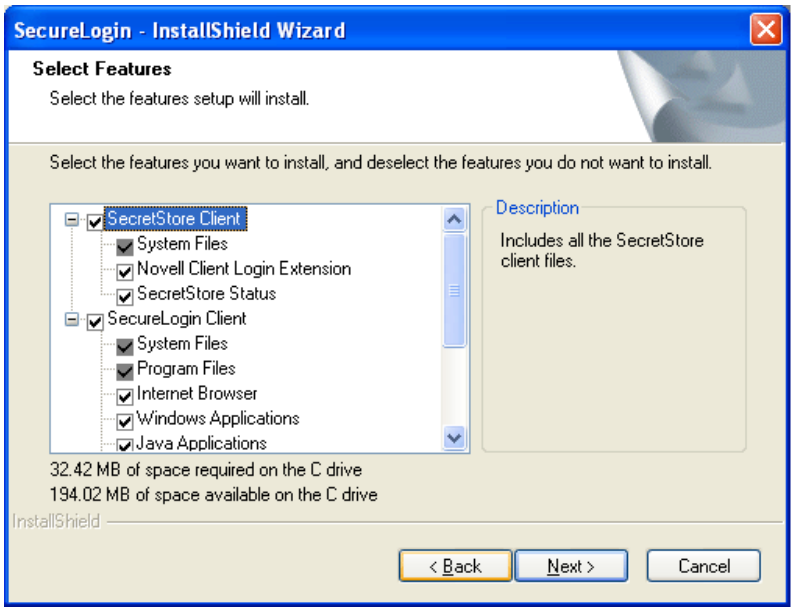


The user profile directory is the default path.

User profiles for Windows 2000 and Windows XP will be in `Documents and settings\Username`.

In earlier versions of SecureLogin, you could modify the cache file location by altering a key in the registry. This is no longer necessary because the installation program automates this step. Also, you can use the `automate.ini` file to customize the location.

- Select SecureLogin components (for example, Terminal Launcher) and SecretStore client components (for example, SecretStore Status).



  If you select the Novell eDirectory with SecretStore option, the installation program installs SecureLogin components and SecretStore components by default

  The Description panel provides information about a component or subcomponent that you select.

2.4 Installing Administrative Tools for eDirectory

This section contains inforamtion on the following:

- Section 2.4.1, “Accessing iManager,” on page 29
- Section 2.4.2, “Installing Plug-Ins for iManager,” on page 30

2.4.1 Accessing iManager

You can run iManager from a directory on a server or a workstation.

In a supported Web browser, type the following in the Address (URL) field:

```
http://server_IP_address/nps/imanager.html
```

For details on accessing iManager, go to the Novell Documentation Web site for iManager (http://www.novell.com/documentation/imanager25/index.html)

2.4.2 Installing Plug-Ins for iManager

The iManager plug-ins are `.npm` files. SecureLogin 6.0 has Plug-ins for SecureLogin, Secure workstation, secretstore, and pcProx. They are found in the `\imanager\snapin` directory on the SecureLogin 6.0 CD. These plug-ins must be installed for iManager as follows:

1. Log in to iManager. Click the *Configure* tab.
2. Click *Module Installation*, then select *Available Novell Plug-in Modules*.
3. Click *New*.
4. Browse and select `sso.npm` from the `\imanager\snapin` directory.
5. Click *OK*.
6. Repeat Step 4 and Step 5 to add *pcprox.npm, sw.npm,* and *secretstore.npm*.
7. Click *Install*.
8. Restart web server after the installation (which may take several minutes) is complete.

For more information on installation and Role Based Server (RBS) configuration, visit the Novell Documentation Web page (http://www.novell.com/documentation/imanager25/index.html)

Additional Information on Installing pcProx Plug-Ins for iManager

Prerequisites for installing pcprox plug-ins for iManager are:

- iManager must be running on a windows machine on which the pcProx client method is installed.
- A pcProx scanner must be connected to the same machine.

Configuring iManager for LDAP SSL Connection to eDirectory

The pcProx and Secure Workstation plug-ins require secure LDAP access in order to store information into eDirectory or retrieve information from eDirectory. To set up secure LDAP access, you must import a root certificate from the eDirectory server into the keystore where iManager runs.

For details on importing a root certificate, visit the Novell Documentation Web site for iManager (http://www.novell.com/documentation/imanager20/index.html?page=/documentation/imanager20/imanager20/data/am4ajce.html).

The following table lists scenarios where you need to import a root certificate, for Secure Workstation and pcProx plug-ins:

Table 2-1 *Scenarios*

Server	Scenario	Whether Certificate Configuration is Required
NetWare	iManager and eDirectory are located on the same machine	Not required for Secure Workstation Not applicable to pcProx
NetWare	iManager and eDirectory are located on different machines	Required for Secure Workstation Not applicable to pcProx

Server	Scenario	Whether Certificate Configuration is Required
Linux	iManager and eDirectory are located on the same machine	Required for Secure Workstation Not applicable to pcProx
Linux	iManager and eDirectory are located on different machines	Required for Secure Workstation Not applicable to pcProx
Windows	iManager and eDirectory are located on the same machine	Required for Secure Workstation Required for pcProx
Windows	iManager and eDirectory are located on different machines	Required for Secure Workstation Required for pcProx

Installing in LDAP Environments

3

LDAP is an open-directory structure that provides fast access to the directory.

SecureLogin in LDAP mode does not require the Novell® Client™ to be installed on the client. However, LDAP does not provide drive mappings or connections to file servers or print servers.

SecureLogin 6.0 provides an LDAP Authentication client, which uses LDAP to connect to a server and securely administer enabled applications.

SecureLogin supports LDAP authentication over SSL connections only.

This section provides information on the following:

3.1 LDAP with eDirectory

eDirectory 8.6.2 or later supports LDAP. If you have eDirectory with LDAP functionality enabled, you have an LDAP server.

NOTE: If Universal Password is not enabled or configured in the eDirectory, and if users are to log in to an eDirectory server by using SecureLogin LDAP Authentication and using any NMAS method, you must install the NMAS Simple Password. Also, all users authenticating using NMAS via LDAP must have a simple password assigned to them.

3.1.1 Preparing for an LDAP Directory

This section provides information on the following:

Extending the eDirectory Schema

If you are installing on workstations that use Novell® eDirectory™, do the following:

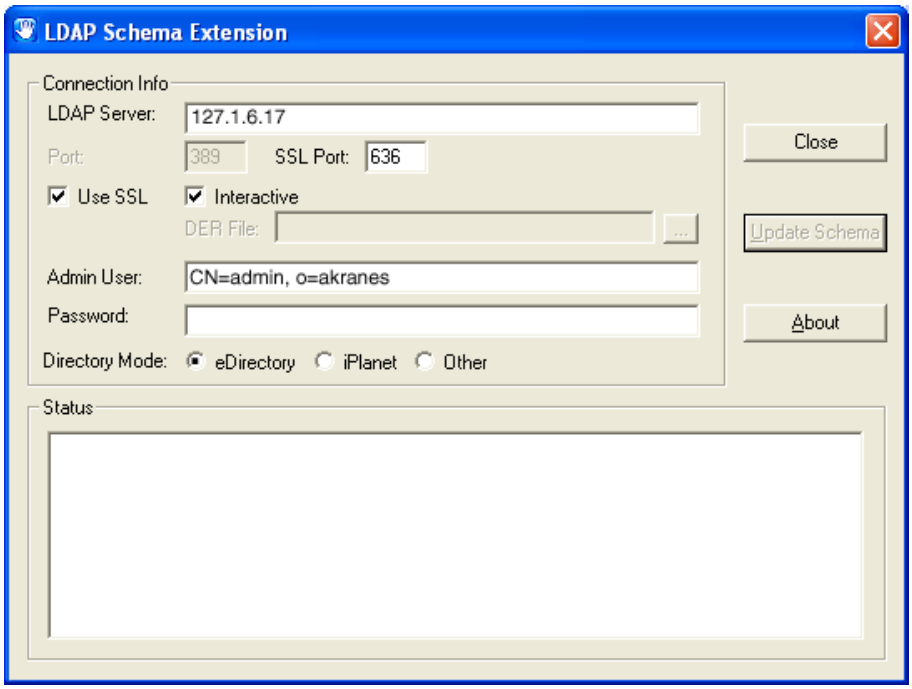
1. Login from your workstation to a tree as admin, using Novell Client.
2. Extend the eDirectory schema by running `ndsschema.exe`.

   This utility assigns rights, but `ldapschema.exe` does not.

   The *ndsschema.exe* is found in the *\securelogin\tools* direcoty of the installation CD.

Extending the LDAP Directory Schema

1. Run `ldapschema.exe`, found in the `\securelogin\tools` directory.
2. Provide information in the LDAP Schema Extension dialog box.



In the LDAP Server edit box, type the LDAP server name or IP address.

In the Admin User edit box, type the fully distinguished name of the admin user that you log in as. For example, type cn=admin,o=akranes.

For SecureLogin to be able to save user single sign-on information, the directory schema must be extended. `Ldapschema.exe` extends the schema and automatically maps LDAP attributes in the extended LDAP schema. The following table illustrates these mappings:

Attribute To Be Mapped	LDAP Mapping
Prot:SSO Auth	protocom-SSO-Auth-Data
Prot:SSO Entry	protocom-SSO-Entries
Prot:SSO Entry Checksum	protocom-SSO-Entries-Checksum
Prot:SSO Profile	protocom-SSO-Profile
Prot:SSO Security Prefs	protocom-SSO-Security-Prefs
Prot:SSO Security Prefs Checksum	protocom-SSO-Security-Prefs-Checksum

These mappings are case-sensitive.

IMPORTANT: You have to extend the LDAP schema on all servers if you want them to act as failover servers.

3.1.2 Installing SecureLogin: LDAP with eDirectory

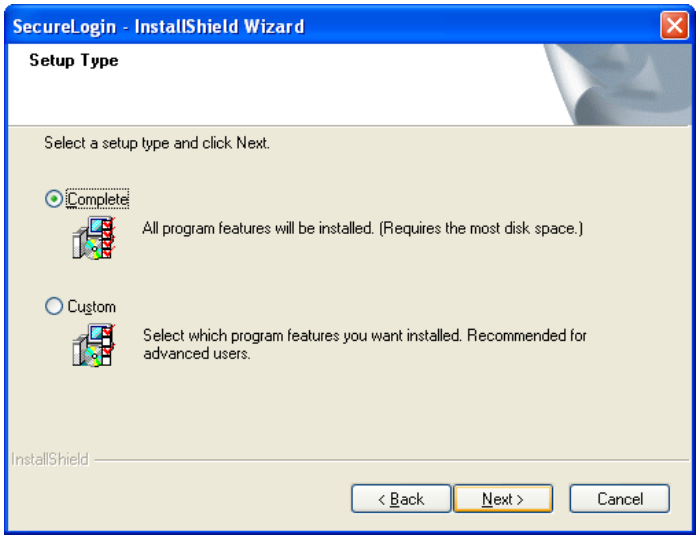
The LDAP option installs SecureLogin into LDAP v3.0 directory environments (for example, Novell eDirectory 8.5 or later).

You can specify more than one LDAP server for the SecureLogin installation. Although the dialog box in the installation program only allows you to specify one LDAP server, you can specify additional servers by modifying the *automate.ini* file.

The LDAP option does not require the Novell Client for Windows. However, if Novell Client32 is installed on the workstation, Client32 is the initial authentication or GINA. If you want LDAP authentication to be the initial authenticator, you must uninstall Novell Client32.

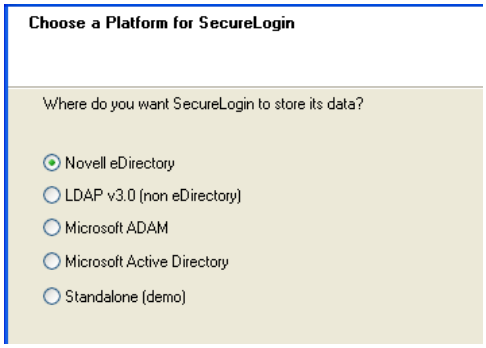
To install the LDAP option:

1. Run `setup.exe` found in the `securelogin/client` directory.
2. Select a language, click *Next*, and accept the license agreement.
3. Select *Complete*, then click *Next*.

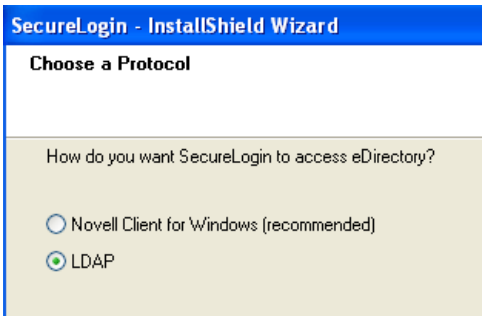


The Complete option uses default values and installs SecureLogin in `c:\program files\novell\securelogin`. For options available through the Custom option, see Section 3.1.3, “Using the Custom Option for LDAP on eDirectory,” on page 39.

4. Select eDirectory as the platform where SecureLogin stores its data, then click *Next*.



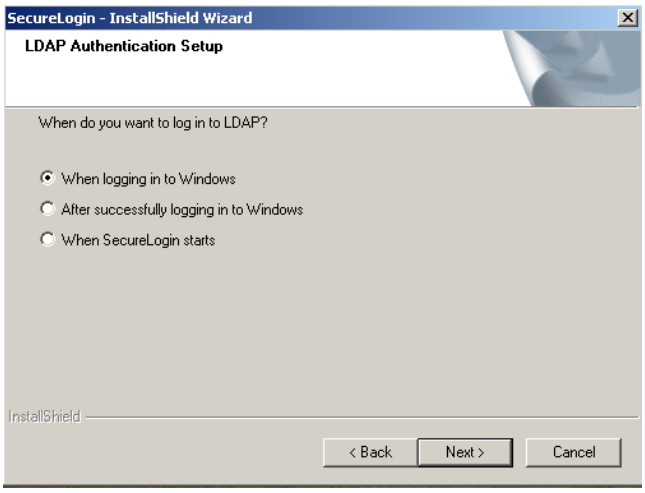
5 Click *LDAP* as the protocol.



LDAP is recommended if the Novell Client is not installed or if LDAP was previously installed but you are overwriting that installation (even if the Novell Client is installed).

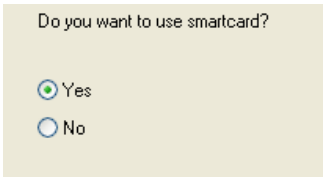
NOTE: The above screen is displayed only if you have Novell Client for Windows installed on your machine. Otherwise, LDAP is auto-selected as the protocol.

6 Select when to log in to LDAP, then click *Next*.



If the workstation is running Novell Client software, the When Logging In to Windows option is not provided and the Primary authentication is always done through the Novell Client.

7 (Conditional) If you do not want to use smartcard, select *No,* click *Next,* then continue with Step 10.

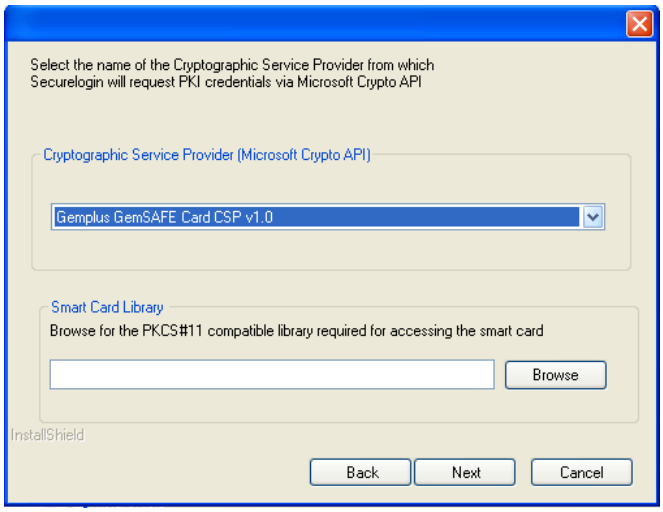


8 (Conditional) If you want to use smartcard and if ActiveClient is detected in your system, select Click *Yes,*click *Next,* then continue with Step 10.

9 (Conditional) If you want to use smartcard and if ActiveClient is not detected in your system:

9a Select *Yes,* then click *Next.*

9b (Conditional) Select a cryptographic service provider from which SecureLogin will request PKI credentials via Microsoft Crypto API.



9c Select a PKCS#11 compatible library required for accessing the smart card, then click *Next*.

NOTE: This will speciy the location of the Cryptographic Token Interface installed as part of the smartcard vendor's software. These API files will be used by SecureLogin to communicate with the smartcard.

Manually configuring the third party smart card PKCS library Assumes a high level of understanding the Cryptographic Service Provider's product.

For more information and instructions about smartcard settings and cryptographic tokens, see the *Novell SecureLogin 6.0 Administration Guide*.

---

10 Select whether SecureLogin is to install the SecretStore client, the NMAS client, or both, then click *Next*.

NOTE: Select Novell SecretStore only if SecretStore is installed on a server. For information on SecretStore, see the *SecretStore Administration Guide* (http://www.novell.com/documentation/secretstore33/index.html).

The Novell SecretStore option installs the SecretStore client, which provides additional security. If you deselect this option and want to install it later, you must uninstall SecureLogin, then run the SecureLogin installation again.

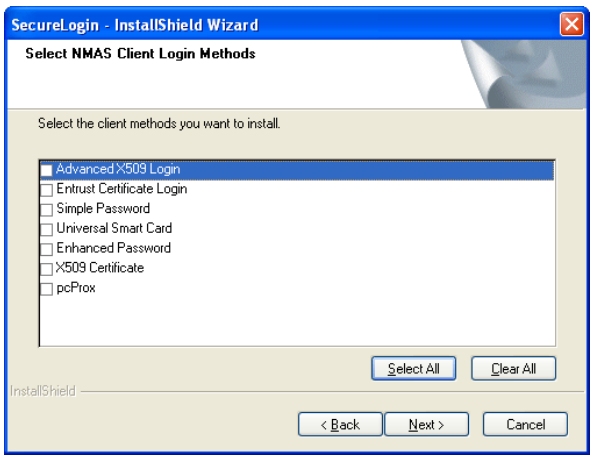
However, if you install the SecretStore client and then later run the install program and deselect the SecretStore client, you will cause problems to the directory cache. All the credential sets that are stored in SecretStore will be unavailable to the eDirectory client. Nevertheless, as long as the local cache is enabled, you can still run SecureLogin. The local cache will populate the eDirectory cache.

The uninstall program does not delete user credentials.

The Novell NMAS Client option installs the NMAS client. SecureLogin uses this option with the AAVerify command, to enable advanced authentication access to an application and also for NMAS authentication using LDAP.

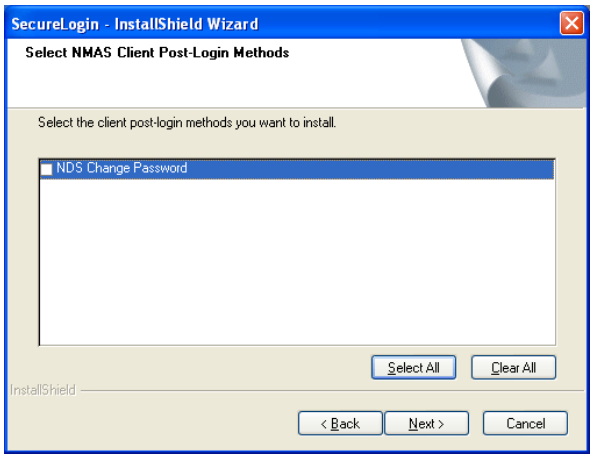
11 Click *Install*.

12 (Conditional) If you selected the NMAS client, select one or more NMAS login methods, then click *Next*.



Here, selecting the *Simple Password* option is mandatory if Universal Password is not created or configured on the eDirectory.

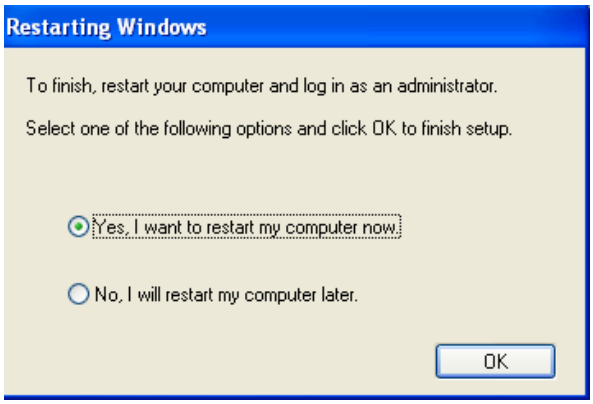
13 Select post-login methods, then click *Next*.



14 By default, the Launch Readme option is selected. Click *Next*.

15 Click *Finish*.

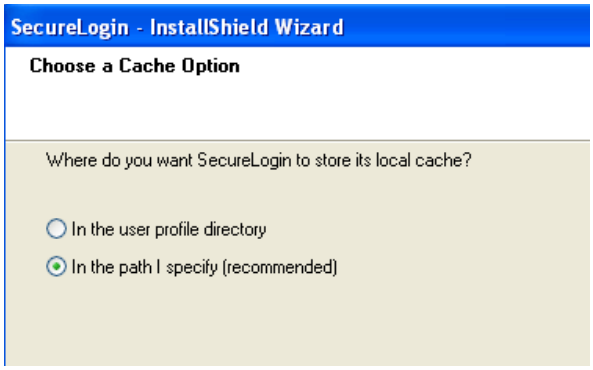
16 Specify when you want to restart computer and click *OK*.



3.1.3 Using the Custom Option for LDAP on eDirectory

The Custom option provides the same defaults as does the Complete option, but enables you to do the following:

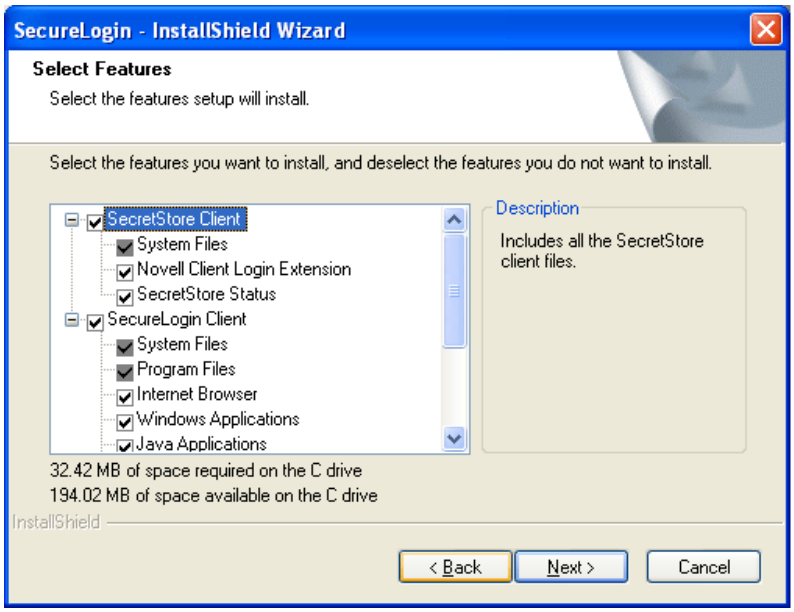
- Specify LDAP server information.
- Specify a path for SecureLogin's local cache.



The user profile directory is the default path.

User profiles for Windows 2000 and Windows XP are in located in `Documents and Settings\Username`.

- Select the SecureLogin components.



The Description panel provides information about a component that you select.

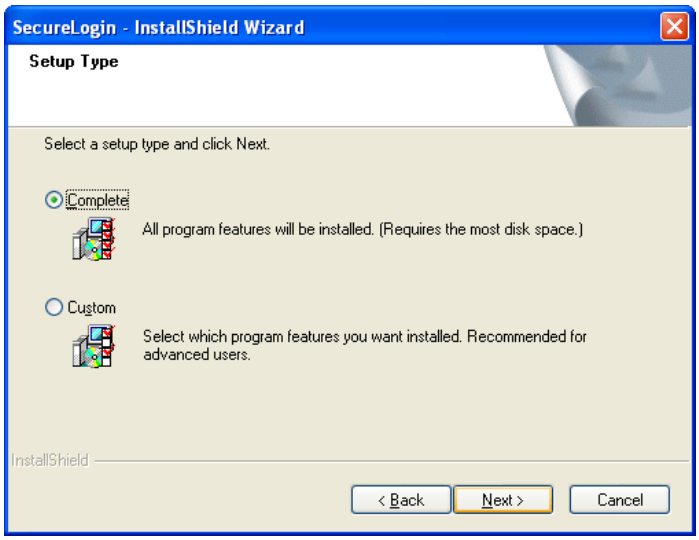
3.2 Installing SecureLogin: LDAP without eDirectory

The LDAP option installs SecureLogin into LDAP v3.0 directory environments.

You can specify more than one LDAP server for the SecureLogin installation. Although the dialog box in the installation program only allows you to specify one LDAP server, you can specify additional servers by modifying the automate.ini file.

1. Run `setup.exe`, found in the `securelogin\client directory`.
2. Select a language, click *Next*, and accept the license agreement.

3 Select *Complete*, then click *Next*.



The Complete option uses default values and installs SecureLogin in `c:\program files\novell\securelogin`. For options available through the Custom option, see Section 3.2.1, "Using the Custom Option for LDAP without eDirectory," on page 42.

4 Select LDAP v30 as the platform where SecureLogin stores its data, then click *Next*.

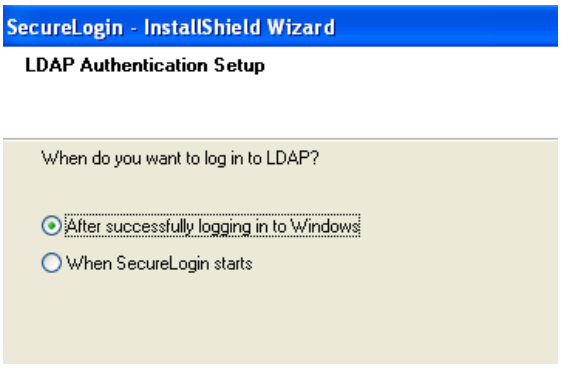
5 Select when to log in to LDAP, then click *Next*.

The After Successfully Logging in to Windows option is called the credential manager mode.

To configure a workstation to use the LDAP GINA as the primary authentication:

5a If the Novell Client is installed on the workstation, remove it.

5b During the SecureLogin installation, select the *LDAP* option and the *When Logging In to Windows* option.



6 At the Ready to Install SecureLogin dialog box, click *Install*.

7 Click *Finish*, click *Yes*, then restart the computer by clicking *OK*.

8 After the computer restarts, log in to LDAP before SecureLogin starts, then provide necessary information.

The first time that you log in to LDAP, you need to provide the server's IP address and the port number.

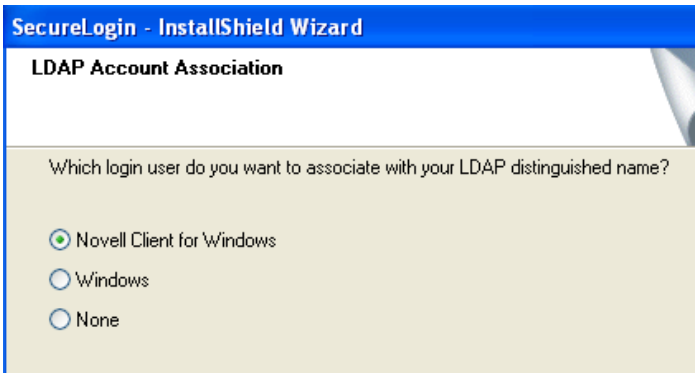
New users must also provide a passphrase question and answer.

3.2.1 Using the Custom Option for LDAP without eDirectory

The Custom option provides the same defaults as does the Complete option, but enables you to do the following:

1 Specify a folder where SecureLogin will be installed.

2 Specify whether to associate your Windows username with your LDAP distinguished name, if LDAP is installed in the Credential Manager Mode.



3 Specify an LDAP server address and port.

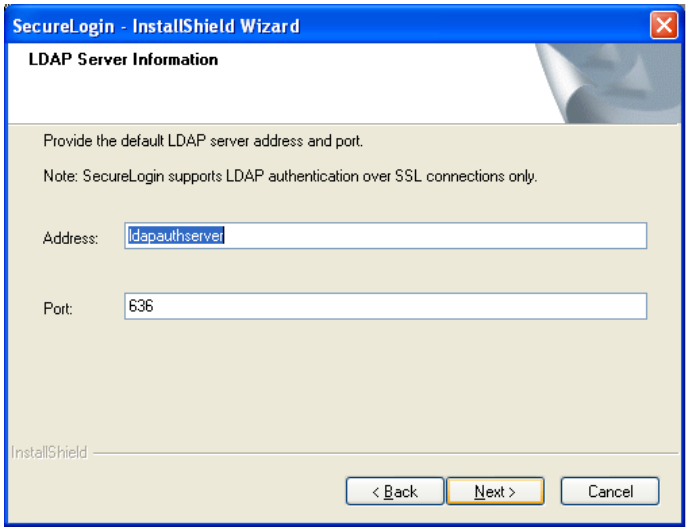
Providing Information for Users: As an internet standard, LDAP does not require more than a TCP/IP protocol installation on a client workstation. When using the LDAP connectivity option, the user must provide LDAP server information during the first login. For subsequent logins, this information is automatically saved and entered into the login dialog box.

You must provide users with the following:

- The registered DNS name or IP address
- The TCP port for Secure LDAP

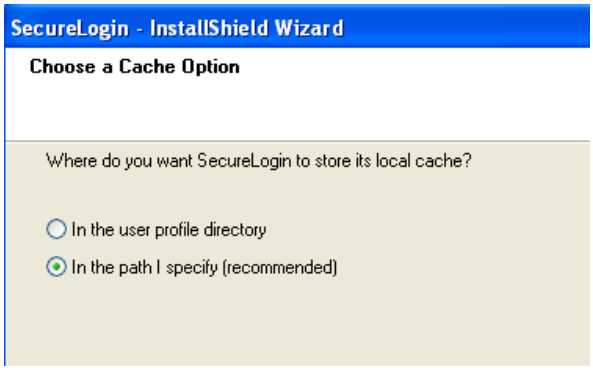
  By default, this is port 636. When entered, it is saved in the workstation's registry for subsequent logins.

NOTE: By selecting the *Custom* option, the administrator or the user can provide this information during installation.



4 The name (ldapauthserver) that appears in the Address field is a placeholder name. Specify a server name or IP address.

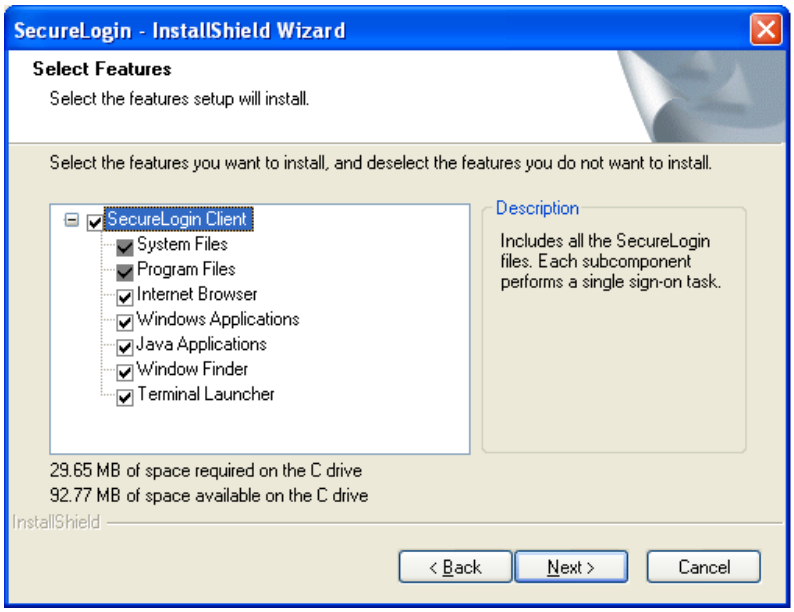
5 Specify a path for SecureLogin's local cache.



6 The user profile directory is the default path.

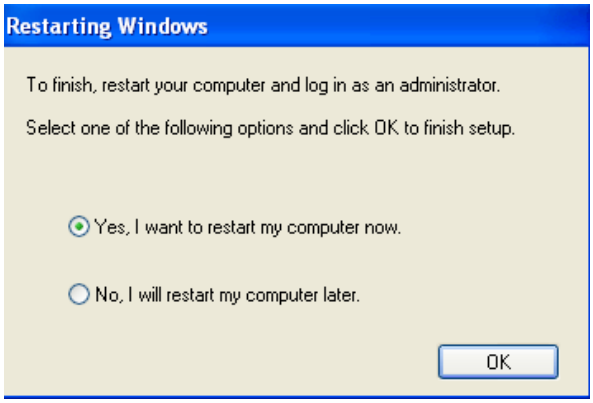
User profiles for Windows 2000 and Windows XP are located in `Documents and Settings\Username`.

7 Select SecureLogin components.



The Description panel provides information about a component that you select. Click *Next*.

8 Select options for starting SecureLogin.



If you say No, make sure to reboot your computer before you start SecureLogin. If you select Yes, your computer will be restarted.

3.3 Granting Rights

For LDAP-compliant directories, grant rights by using whatever tool is used for other administrative tasks in that directory.

Users on Windows 2000, and Windows XP must have workstation rights to their local cache directories. To grant rights there, do one of the following:

- Grant rights to the user's cache directory (for example, `c:\program files\novell\securelogin\cache\v3slc`).

- The default location is the user's profile directory. By default, the user already has rights to this directory. However, if the user specified an alternative path during the installation, you might need to grant rights to the cache directory.
- Use the registry setting to relocate the user's cache to a location that the user has rights to (for example, the user's documents folder).

3.4 Installing Administrative Tools for LDAP

To administer SecureLogin for LDAP, have eDirectory running on a network server. Then use the administrative tool that you typically use to manage the server.

You can also use `slmanager.exe` to manage LDAP. This utility is found in the `\securelogin\tools` directory.

The SSO plug-in to iManager enables you to define an LDAP password policy. However, the plug-in does not enforce that policy unless the LDAP schema has been extended.

If the SecretStore client is installed on your workstation, install and use the SecretStore plug-in (secretstore.npm) to iManager to administer SecretStore in LDAP mode. This file is found in the `\iManager\snapins` directory.

3.5 Configuration Issues

3.5.1 Using LDAP on eDirectory

All the functionality that is available in NMAS is also available on the LDAP Authentication client for SecureLogin. The LDAP client enables you to provide multilevel authentication (for example, a biometric device and a password).

When you use LDAP on eDirectory, the LDAP password can come from one of two places:

- The eDirectory password
- The NMAS Simple password

The eDirectory takes precedence. The simple password exists in case an eDirectory password does not exist.

If a user types a password that does not match the eDirectory password, LDAP attempts to match the simple password.

3.5.2 Using LDAP on Non-eDirectory Environments

This section contains the following information:

Configuring the Server

This section contains the following information:

Retrieving the Certificate

1. Ensure that certificate service is installed on the directory server.
2. Export a copy of the server certificate file to a temporary location for user deployment.

   When you export the certificate, ensure that the encoding format you select is DER encoded binary X.509 or Base-64 encoded X.509.
3. Manually change the certificate filename extension to `.der` or `.b64` (depending on the encoding format you select).

For details on certificate service, refer to the respective section of the documentation for the directory server you use.

Enabling Anonymous Queries

By default, anonymous queries are not enabled on some of the directory servers (including Active Directory).

If you use Active Directory, make sure that you have set the Anonymous Logon rights on the user container and that the settings have taken effect on all User objects within that container.

For more details, refer to AppNote:Configuring Active Directory to Allow Anonymous Queries for NSL LDAP Client (http://www.novell.com/coolsolutions/appnote/15120.html).

Following are the minimum permissions to be granted for Anonymous Logon:

Table 3-1 *Setting Permissions for Anonymous Logon*

User Object	Permissions	Inheritance	Permission Type
ANONYMOUS LOGON	List Contents	This object and all child objects	Object
ANONYMOUS LOGON	Read name	This object and all child objects	Property
ANONYMOUS LOGON	Read Name	This object and all child objects	Property
ANONYMOUS LOGON	Read objectClass	This object and all child objects	Property

Extending the Schema

- **Servers (except Active Directory):** Extend the LDAP directory schema for all directory servers other than Active Directory. While extending LDAP schema, ensure that you have

chosen the appropriate directory mode. For details, refer to “Extending the LDAP Directory Schema” on page 34.

NOTE: You have to extend the LDAP Schema on all servers if you want them to act as failover servers.

- **Active Directory:** Extend the Active Directory Schema. For details, refer to Section 4.4, “Extending the Active Directory Schema,” on page 50.

NOTE: Extending an LDAP directory schema on Active Directory can lead to improper configuration resulting in authentication failure.

Configuring the Workstation

1. Copy the server certificate file to your workstation.
2. Specify the certificate file path by adding the following registry key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP`
3. Under the above registry key, specify the following value:

   `CertFilePath REG_SZ full_path_of_cert_file`

   The certificate filename extension must be either `.der` or `.b64`, as in the following examples:

Name	Type	Data
CerttFilePath	REG_SZ	C:\ad_cert.der
CerttFilePath	REG_SZ	C:\ad_cert.b64

Using Contextless Login

If you configure a workstation to use the LDAP authentication, the LDAP module launches a login dialog box, which requires a user DN and password. The LDAP Authentication client provides a contextless login. This feature simplifies the login process by enabling you to type part of your username.

For example, Henri Dubois’ DN is cn=hdub, ou=rdev,o=vmp. Henri enters hdub in the login dialog box. The LDAP Authentication client finds and displays every user ID that begins with hdub. If just one user ID qualifies, the LDAP authentication client authenticates using Henri’s entire DN.

If multiple hdub IDs exist, the client lists all user IDs that begin with hdub. Henri then selects the DN for his user ID and logs in.

3.5.3 Setting Up Passphrase

A SecureLogin passphrase is a question and response combination used as an alternative form of identity verification. Passphrase functionality protects SecureLogin credentials from unauthorized access and enables users to access SecureLogin in offline mode. Passphrases can also be used as a substitute authentication mode if for example, a user forgets their password. Depending on the administrator’s preferences SecureLogin passphrase questions can be generated by the administrator and/or the user.

If a passphrase has previously been configured this dialog box will not display and the installation is complete.

On initial login to SecureLogin all users are requested to save a passphrase response. It is important that this response is easy to recall as it cannot be viewed by anyone.

As administrator, and therefore first user of SecureLogin, you must create a passphrase question for yourself.

1. Specify a question in the *Enter a question* field.
2. Specify an answer in the *Enter the answer* field.
3. Specify the answer again in the *Confirm the answer* field.
4. Click *OK*. Your passphrase is saved and SecureLogin is installed on the administration workstation.

Installing in Active Directory Environments

4

This section contains information on the following:

4.1 Prerequisites

- ❑ Have administrator level access to the server and administration workstation.
- ❑ Backup the existing directory.
- ❑ In multi-directory environments:
  - Identify the domain controller to determine which directory to install SecureLogin on first and the oder of replication.
  - Have access to the domain controller.

4.2 Installation Overview

1. Uninstall SecureLogin versions prior to 3.5.x.
2. Ensure Microsoft Management Console (MMC) Active Directory snap-ins are installed on the administration workstation.
3. Extend the directory schema for SecureLogin versions prior to 3.5.x.
4. Install Citrix or Terminal Services clients and Java Runtime Engine (JRE) on user workstations if the application types are to be single sign-on enabled.
5. Install SecureLogin on the administration workstation.
6. Create test users on the administration workstation.
7. Define and configure the SecureLogin user environment, including single sign-on enabling the required applications.
8. Copy test users configuration to relevant objects.
9. Deploy the SecureLogin application on user workstations.

NOTE: You must install Java Runtime Environment version 1.4 or later to enable single sign-on to Java applications or JavaScript logons on the Workstation.

4.3 Microsoft Active Directory

This section has the following information:

4.3.1 LDAP Mode

SecureLogin supports Microsoft Active Directory Operating in LDAP mode. There are no additional installation or configuration requirements. The only variation to the install is that you select LDAP and not Microsoft Active Directory as the installation platform.

To extend the Microsoft Active Directory Schema and assign user rights, see Section 4.4, "Extending the Active Directory Schema," on page 50

4.3.2 ADAM

SecureLogin supoorts deployment in an ADAM instance. For more information, see Chapter 5, "Installing in Microsoft ADAM Environments," on page 61.

4.4 Extending the Active Directory Schema

SecureLogin leverages the directory to store and manage SecureLogin data. SecureLogin extends the directory schema to add six SecureLogin schema attributes where SecureLogin data is stored. For more information on these six schema attributes refer to *Novell SecureLogin 6.0 Administration Guide*.

After you extend the Directory schema, you must give permission to objects including group policy, organizational units, and containers that will implement SecureLogin, in order to access the SecureLogin attributes. Authorizing Read and Write access to SecureLogin Directory schema attributes is referred to as 'Assigning user rights'.

Following are the six SecureLogin attributes added to the Directory schema:

- Protocom-SSO-Auth-Data
- Protocom-SSO-Entries
- Protocom-SSO-Entries-Checksum
- Protocom-SSO-Profile
- Protocom-SSO-SecurityPrefs
- Protocom-SSO-Security-Prefs-Checksum

The SecureLogin Microsoft Active Directory schema extension executable extends the schema on the server and enables you to assign user rights. You must determine which containers and organizational units need SecureLogin access and their distinguished name (DN) as you must assign rights to each container and organizational unit separately.

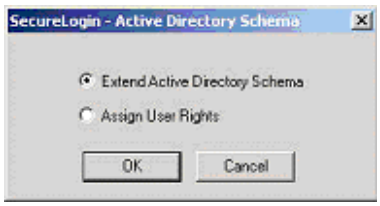
NOTE: You can also extend the Microsoft Active Directory schema to the root of the domain and assign rights to each container and organizational unit below.

IMPORTANT: •If SecureLogin version 3.5.x is installed, then you do not need to extend the directory schema since the attributes aer the same. However, any new directory objects for example organizational units, still require you to assign rights. For more information see, Section 4.5, "Assigning User Rights," on page 52.

- If you are using an earlier version of SecureLogin, see Chapter 7, "Upgrading from Earlier Versions," on page 91.
- If the Microsoft Active Directory instance is deployed using the `adsscheme.exe` file that has been copied from rather than run from the SecureLogin 6.0 installation CD, then administrators must copy the entire folder containing the Microsoft Active Directory Schema and Configuration files to their preferred location. The Microsoft Active Directory Schema and configuration files must be located in the same folder in order for the Active Directory instance to successfully deploy.

The following instructions apply to the cofiguration of the Microsoft Active Directory instance stored and administered on a separate server from the Active Direcotry server domain controller.

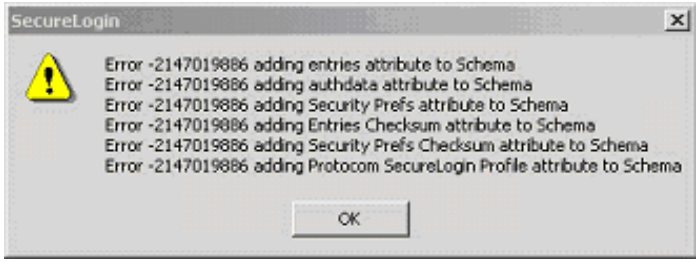
1. Log on to the server as an administrator.
2. Click *Schema Extension Tools* > *Active Directory Extension*, or run *adsschema.exe* found in the Tools folder of the install CD. The SecureLogin – Active Directory Schema dialog box is displayed.



3. Select the *Extend Active Directory Schema* option.
4. Click *OK*. A confirmation message box is displayed.
5. Click *OK* to return to the Active Directory Schema dialog box.

   Now that Directory schema has been extended access rights need to be assigned to the relevant containers and organizational units.

NOTE: If the schema has previously been extended, a message box listing the existing schema attributes is displayed.



6 Ignore this message and click *OK*.

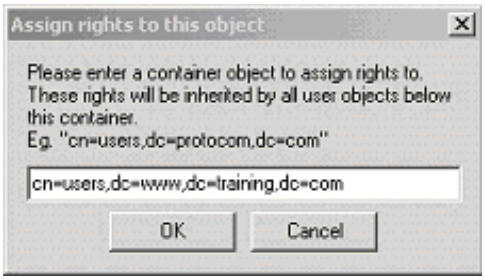
4.5 Assigning User Rights

You must assign permission to objects in the directory to strore data against the new SecureLogin schema attributes. Assign user rights to all objects that access SecureLogin, including user objects, containers, group policies, and organizational units.

When you assign rights to containers and organizational units, the rights filter down to all associated user objects. So unless you are required to do so, it is not necessary to assign rights at the individual user object level.

1 Run `adsschema.exe`, found in the `\securelogin\tools` directory.

2 Select *Assign User Rights*, then click *OK*. The Assign Rights to This Object dialog box is displayed.



NOTE: In the above figure, rights are assigned to the Users container.

The Users container definition is:

cn=users, dc=www, dc=training, dc=com

To assign rights to an organizational unit, for example Marketing, in the

domain www.company.com, the definition is:

ou=marketing, dc=www, dc=company, dc=com

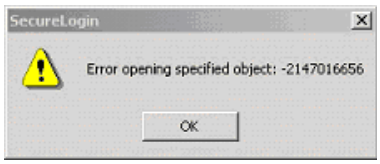
---

3 Specify your container or organizational unit definition in the Assign rights to this object field.

4 The confirmation dialog box appears.Click *OK* to return to the Active Directory Schema dialog box.

5 Repeat steps 4 and 5 to assign rights to all required user objects, containers and organizational units.

NOTE: If the above error message is displayed, rights have already been assigned to this object. This message box is for your information only.



NOTE: If the above error message is displayed, you have attempted to assign rights to an object that does not exist on this directory. Check your punctuation, syntax or spelling and repeat the procedure.

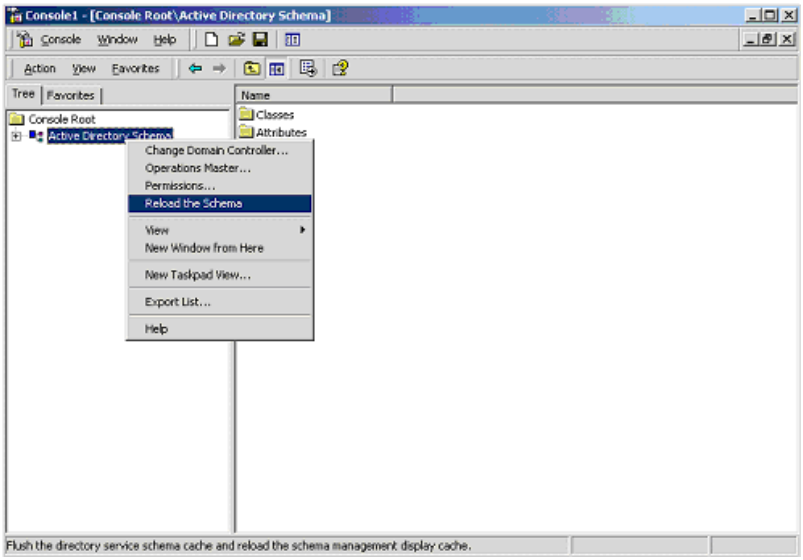
6 After you have assigned all required rights are successfully assigned, Click *OK* to return to the Active Directory Schema dialog box.

7 Click *Cancel.*

4.5.1 Refreshing the Directory Schema

To refresh the directory schema:

1 Run the Microsoft Management Console (MMC) and display the Active Directory Schema snap-in.



2 Right-click *Active Directory Schema*, then select *Reload the Schema*.

3 On the Console menu, click *Exit* to close the MMC.

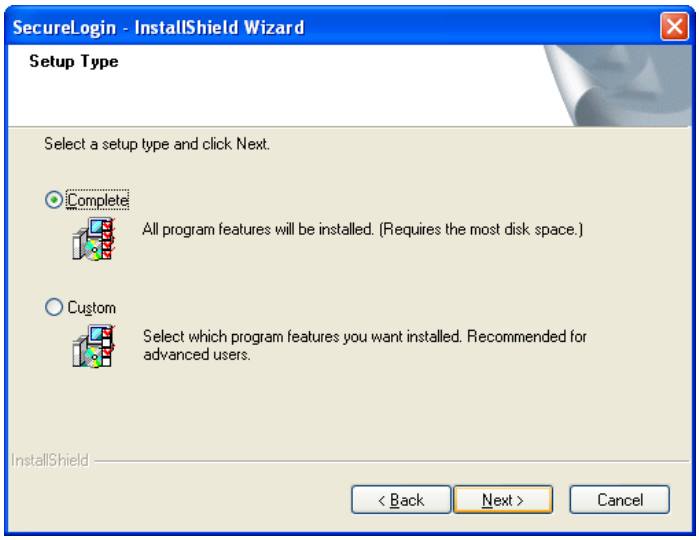
In a multiple-server environment, schema updates occur on server replication.

NOTE: You can extend rights to objects at any time after the schema is extended. If you add organizational units, then you need to rerun the *adschema.exe* tool and assign rights to the new object to permit SecureLogin data to write to the directory.

4.6 Installing SecureLogin: Active Directory

After you have finished extending the Active Directory schema and assigning permissions to the required directory objects, install the SecureLoginapplication on the administration and user workstations.

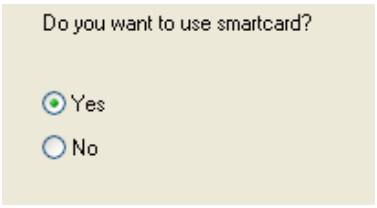
1. Log into the workstation as administrator.
2. Insert the installation CD, then click Install/upgrade or run `setup.exe`, found in the `securelogin\client` directory.
3. Select a language, click *Next*, then accept the license agreement.
4. Click *Next.*
5. Select *Complete*, then click *Next*.



The Complete option uses default values and installs SecureLogin in `c:\program files\novell\securelogin`.

6. Select Microsoft Active Directory as the platform where SecureLogin will store its data, then click *Next*.

7 The Do you want to use smartcard dialog box is displayed.



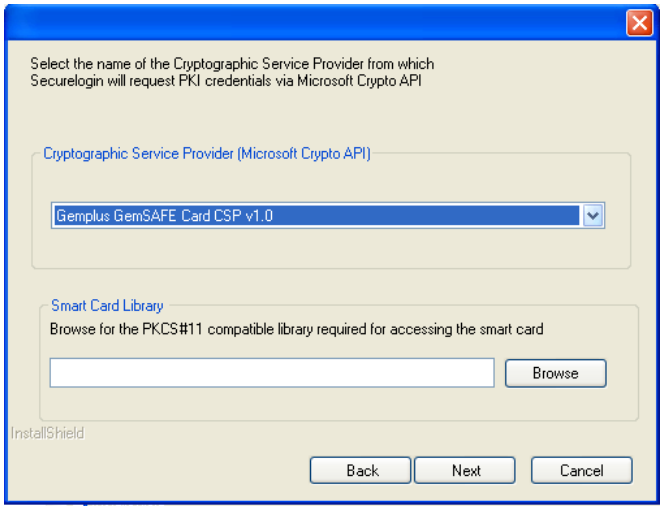
(Conditional) If you don't want to use smartcard, select *No,* click *Next,* then continue with Step 8.

8 (Conditional) If you want to use smartcard and if ActiveClient is detected in your system, select *Yes,*Click *Next,* then continue with Step 8.

9 (Conditional) If you want to use smartcard and if ActiveClient is not detected in your system:

9a Select *Yes,* click *Next.*

9b (Conditional) Select a cryptographic service provider from which SecureLogin will request PKI credentials via Microsoft Crypto API.



9c Click *Browse* and select a PKCS#11 compatible library required for accessing the smartcard, then click *Next*.

NOTE: This will speciy the location of the Cryptographic Token Interface installed as part of the smartcard vendor's software. These API files will be used by SecureLogin to communicate with the smartcard.

Manually configuring the third party smartcard PKCS library Assumes a high level of understanding the Cryptographic Service Provider's product.

For more information and instructions about smartcard settings and cryptographic tokens, see the *Novell SecureLogin 6.0 Administration Guide*.

---

10 Click *Next* > *Install*.

11 By default, the Launch Readme option is selected. Click *Next.*

12 By default, the Start SecureLogin at the Windows startup is selected. Deselect the option if you do not want SecureLogin to start at the Windows startup.

13 Click *Finish*.

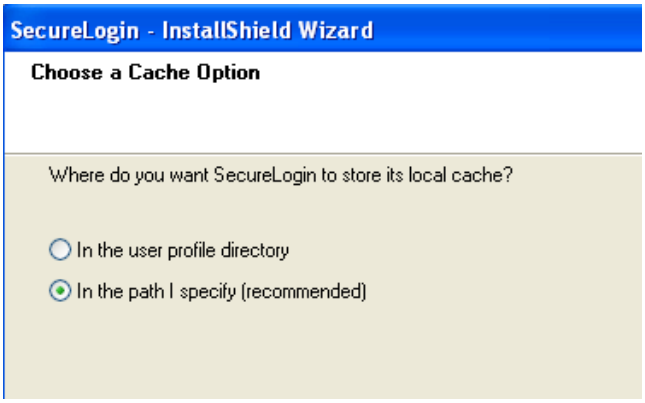
14 Specify when you want to restart the computer, then click *OK*.

15 After the workstation restarts, provide a passphrase question and passphrase answer, then click *OK*.

4.6.1 Using the Custom Option for Active Directory

The Custom option provides the same defaults as does the Complete option, but enables you to do the following:

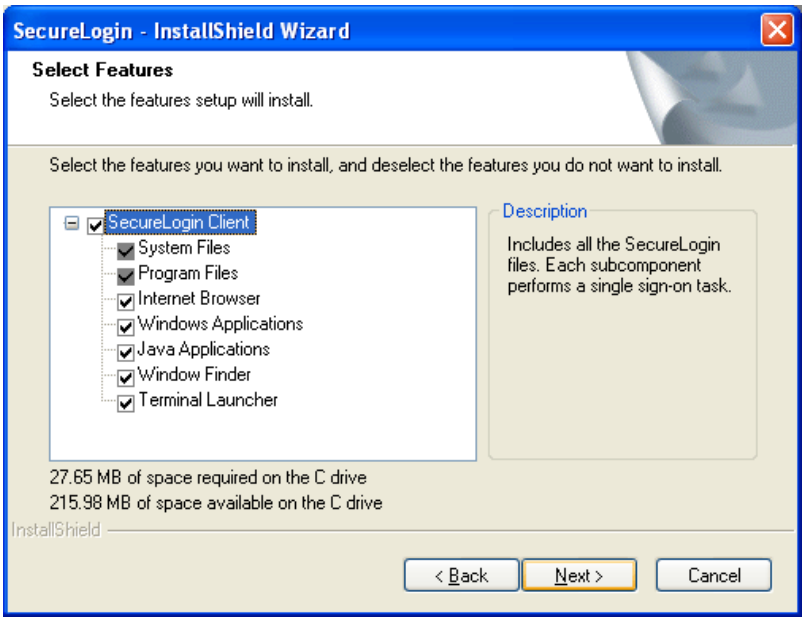
1 Specify a path for SecureLogin's local cache.



2 The user profile directory is the default path.

3 User profiles for Windows 2000 and Windows XP are stored in `Documents and Settings\username`.

4 Select SecureLogin components.



5 The Description panel provides information about a component that you select.

Select options for starting SecureLogin.

6 Specify when you want to restart the computer, then click *OK*.

4.7 Deploying

4.7.1 Deployment of Users

SecureLogin provides centralized management and deployment of user configuration by using the directory structure and administration tools. In the Active Directory, SecureLogin installs an additional tab to the Users and Computers, Properties dialog box. This dialog box provides SecureLogin administrative functionality in the same utility you currently use to manage your Active Directory users.

4.7.2 Configure User ’s Environment List

Configuring a user's SecureLogin environment includes:

- Setting preferences.
- Creating password policies (optional).
- Enabling single sign-on to applications.
- Creating passphrase questions for selection (optional).

NOTE: It is recommend that you configure SecureLogin on a test user account before deploying.

The following table shows options available for deploying and distributing user configurations:

User Configurations Options	Description
Copy Settings	Copies SecureLogin configuration from one object in the same directory to another object
Export and import	Distributes the configuration using an XML file.
Directory object inheritance	Inherits the configuration from a higher level directory object, for example a Group Policy.
Corporate Configuration redirection	Specifies a specific directory object from which the configuration is inherited.

NOTE: For more information about the selection and execution of the appropriate deployment and distribution methods for your organization, see the *Novell SecureLogin 6.0 Administration Guide*.

4.8 Setting Up a Passphrase

A SecureLogin passphrase is a question and response combination used as an alternative form of identity verification. Passphrase functionality protects SecureLogin credentials from unauthorized

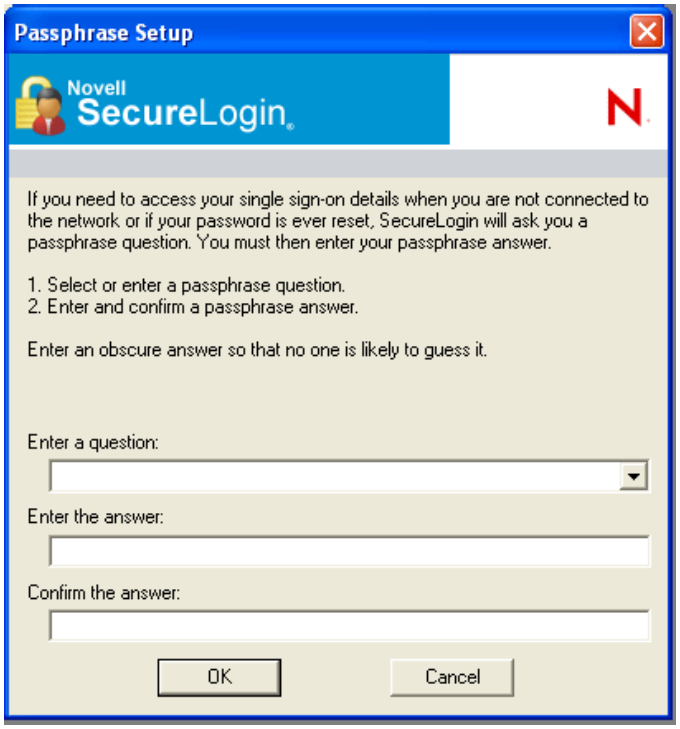
access and enables users to access SecureLogin in offline mode. Passphrases can also be used as a substitute authentication mode if for example, a user forgets their password. Depending on the administrator's preferences SecureLogin passphrase questions can be generated by the administrator and/or the user.

If a passphrase has previously been configured this dialog box will not display and the installation is complete.

Administrators can also set up SecureLogin passphrase questions for their users and enforce strict policies on answers. For more information, see *Novell SecureLogin 6.0 Administration Guide*.

NOTE: During installation, SecureLogin passphrase security is enabled to enforce passphrase setup during initial login. Administrators can disable the passphrase policy of SecureLogin by unchecking the Use Passphrase Policy check box in the Advanced Settings pane of the Administrative Management Utility.

IMPORTANT: System administrators must be aware of the possible implications for user's data security if passphrases are disabled.



On initial login to SecureLogin all users are requested to save a passphrase response. It is important that this response is easy to recall as it cannot be viewed by anyone.

As administrator, and therefore first user of SecureLogin, you must create a passphrase question for yourself.

1. Specify a question in the *Enter a question* field.
2. Specify an answer in the *Enter the answer* field.
3. Specify the answer again in the *Confirm the answer* field

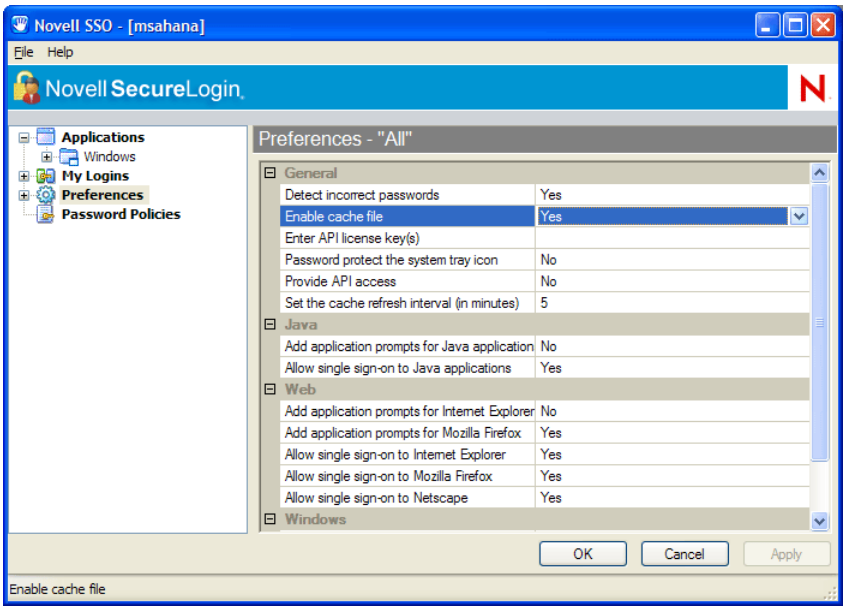
4 Click *OK*. Your passphrase is saved and SecureLogin is installed on the administration workstation.

NOTE: •When you upgrade, SecureLogin stores all user data, including the user's passphrase question and response, from the previous version. The creation of a new passphrase question or answer is not required.

- You can create passphrase questions for users to select from, in a directory environment. However, since you are the first SecureLogin user, you must create your own passphrase question. For more information about passphrases and instructions for creating passphrase questions for users, see *Novell SecureLogin 6.0 Administration Guide*.

4.9 Install SecureLogin for Mobile Users and Notebooks

Installing SecureLogin for mobile and remote users follows the same procedure as Section 4.6, "Installing SecureLogin: Active Directory," on page 54. However, it is important that you ensure the cache is saved locally, or users will be unable to access applications when they are disconnected from the network. The *Enable cache file* setting in the Preferences option is set to *Yes* by default. You can set this at either the Organization Unit level or on a per user basis.



Installing in Microsoft ADAM Environments

5

This section contains information on the following:

5.1 Prerequisites

- ❑ Windows* 2003 or Windows XP including Active Directory
- ❑ Assign permissions to a Network Service Account
- ❑ Create an ADAM instance
- ❑ Back-up the Active Directory server
- ❑ In multi-directory environments you need to identify the domain controller (to determine which directory to synchronize SecureLogin user data with and the order of replication)

NOTE: If the ADAM instance is deployed using the adamconfig.exe file that has been copied from rather than run from the SecureLogin 6.0 installation CD, then administrators will need to copy the entire folder containing the ADAM Schema and Configuration files to their preferred lcoation. The ADAM Schema and configuration files must all be located in the same folder, for ADAM instance to successfully deploy.

The following instructions apply to the configuration of the ADAM instance stored and administered on a separate server to the Active Directory server domain controller. If your configuration does not separate the Active Directory server and the ADAM instance server, follow the instructions for both.

5.2 Using Active Directory and ADAM

Novell® SecureLogin 6.0 supports deployment in an ADAM instance. Active Directory is responsible for the network authentication, while ADAM is responsible for storing and providing the SecureLogin configuration data, settings, policies and application definitions. For example, a user logs into the network, authenticates successfully to Active Directory then they are able to access ADAM for their SecureLogin data.

The ADAM application can be downloaded from (http://www.microsoft.com/downloads/details.aspx?FamilyId=9688F8B9-1034-4EF6-A3E5-2A2A57B5C8E4&displaylang=en)

5.3 Assign Permissions to a Network Service Account

A service account is a user account that is created explicitly to provide a security context for services running on Microsoft* Windows Server 2003. Application pools use service accounts to assign permissions to Web sites and applications running on Internet Information Services (IIS). Administrators can manage service accounts individually to determine the level of access for each application pool in a distributed environment.

Creating a Network Service Account enables the ADAM instance.

To create a Network Service Account:

1. Click *Start* > *All Programs* > *Administrative Tools* > *Active Directory Users and Computers*. Active Directory Users and Computers page is displayed.
2. Select *View* > *Advanced Features*. The *Advanced Features* option is enabled.
3. Select the *Domain Controllers* folder and locate the Domain Controller of your SSO-enabled domain.
4. Right-click the *Domain Controller* and select *Properties*. The [Domain] Properties page is displayed.
5. Select the *Security* tab. If the Network Service account is not on the list of Group or user names, add it.
6. Select the *Network Service* account.
7. In the *Permissions for Administrators* section, select *Allow to Create All Child Objects*.
8. In the *Permissions for Administrators* field, select *Allow to Delete All Child Objects*.

   NOTE: Selecting *Delete All Child Objects* has no effect for SecureLogin, but allows the ADAM instance to be cleaned properly when it is uninstalled.
9. Click *OK* to close the [Domain] Properties dialog box.

5.4 Configuring the ADAM Schema

SecureLogin leverages the directory to store and manage SecureLogin data. Six schema attributes are added to the directory schema. Once the ADAM schema has been extended with these attributes the relevant containers, organizational units (OUs) and user objects must be permitted to Read and Write SecureLogin data. The SecureLogin ADAM Configuration wizard automatically extends the ADAM instance schema and assigns directory access permissions to selected objects.

Following are the six SecureLogin Single Sign-On attributes added to the directory schema:

- Protocom-SSO-Auth-Data
- Protocom-SSO-Entries
- Protocom-SSO-SecurityPrefs
- Protocom-SSO-Profile
- Protocom-SSO-Entries-Checksum

- Protocom-SSO-Security-Prefs-Checksum

For more information about the SecureLogin schema attributes, see the *Novell SecureLogin 6.0 Administration Guide*.

5.5 Overview of the Install Procedure

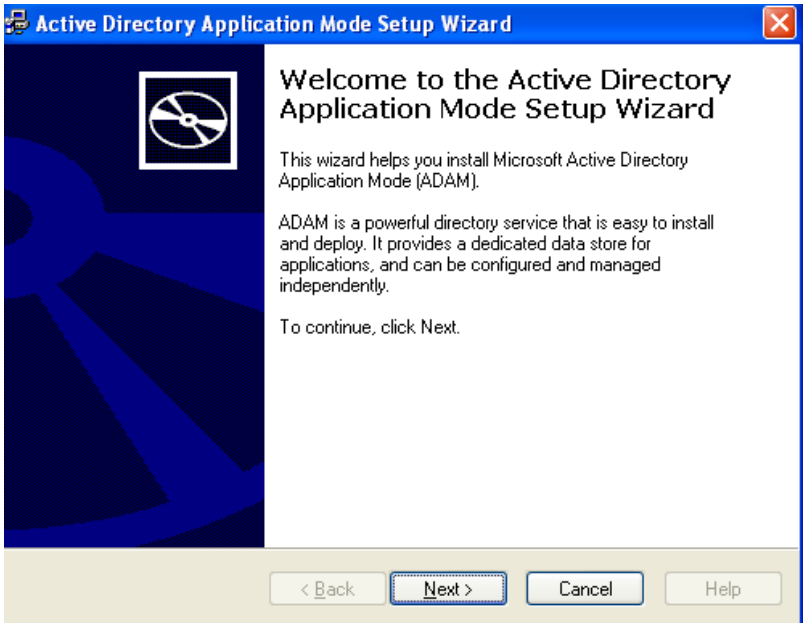
This section contains information on the following:

5.5.1 Create the ADAM Instance

The ADAM setup files are provided in the `Tools` folder of the SecureLogin Distribution CD.

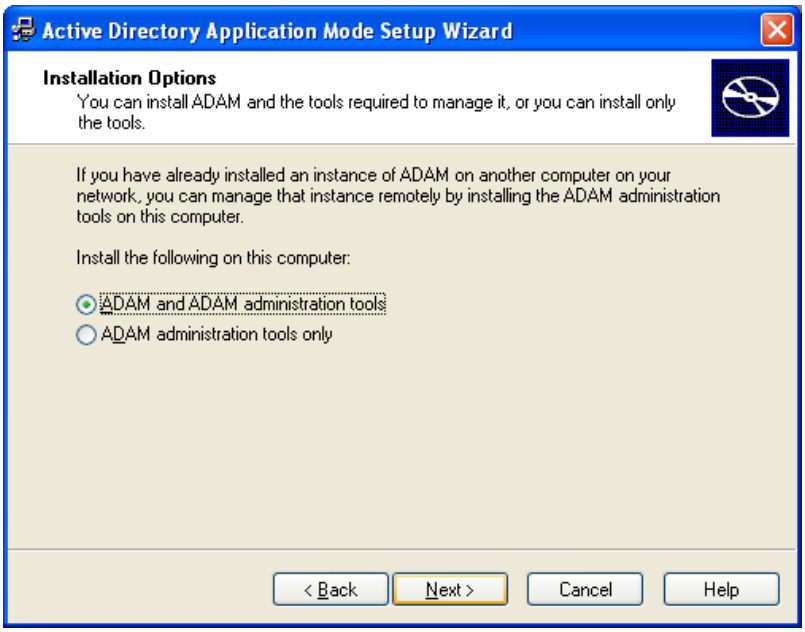
To create an ADAM instance for SecureLogin 6.0:

1. Double-click the `adamsetup.exe` file. The Active Directory Application Mode Setup Wizard is displayed.



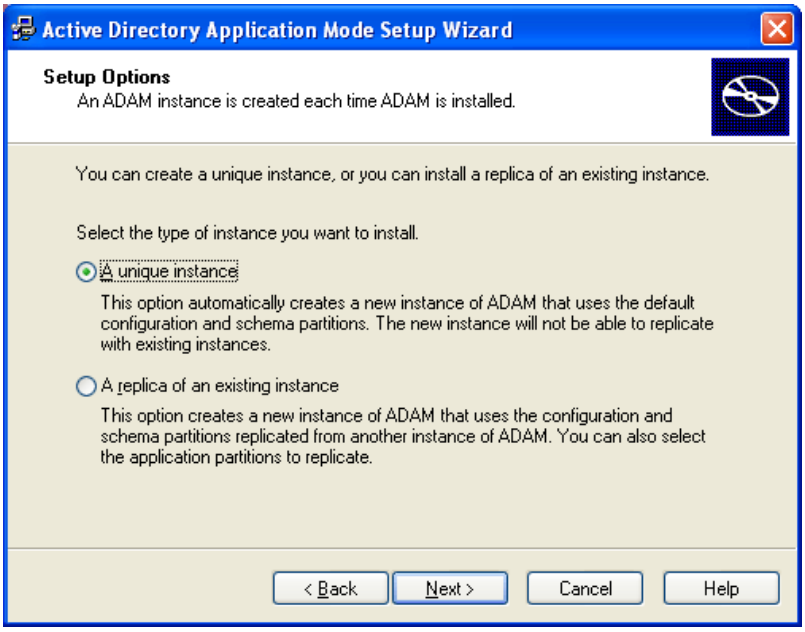
2. Click the *Next* button. The License Agreement dialog box is displayed.
3. Accept the license agreement, then click *Next*.

The Installation Options dialog box is displayed.



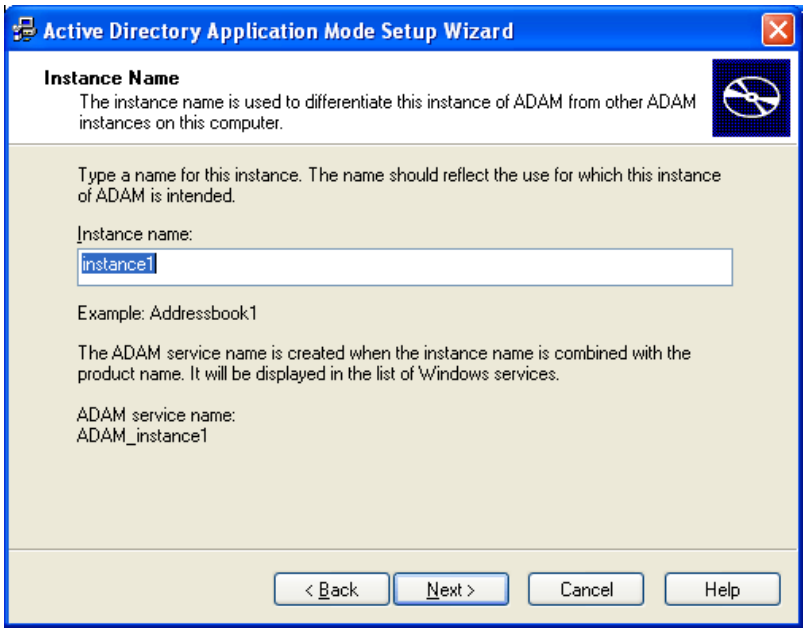
4 Select the *ADAM and ADAM administration tools* option.

5 Click *Next*.The Setup Options dialog box is displayed.



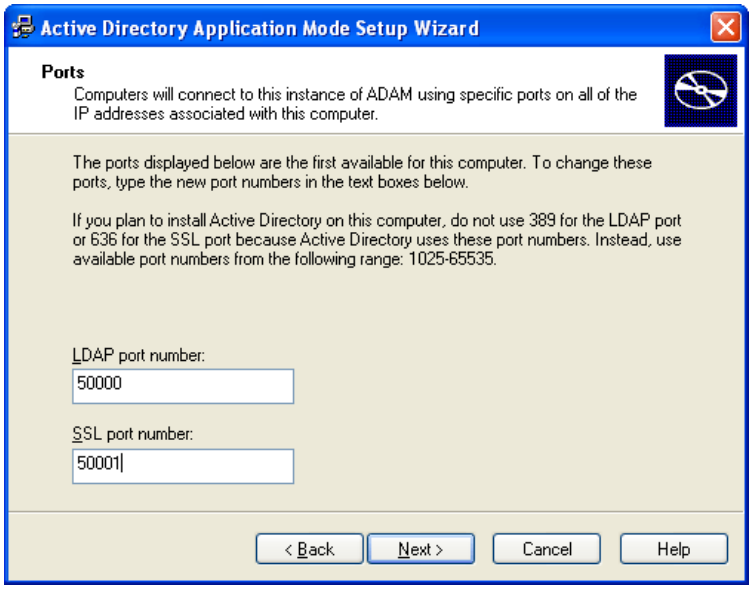
6 Select the *A unique instance* option.

7 Click *Next* . The Instance Name page is displayed.



8 Speify a name for the ADAM instance in the *Instance name* field.

9 Click *Next*. The Ports page is displayed.

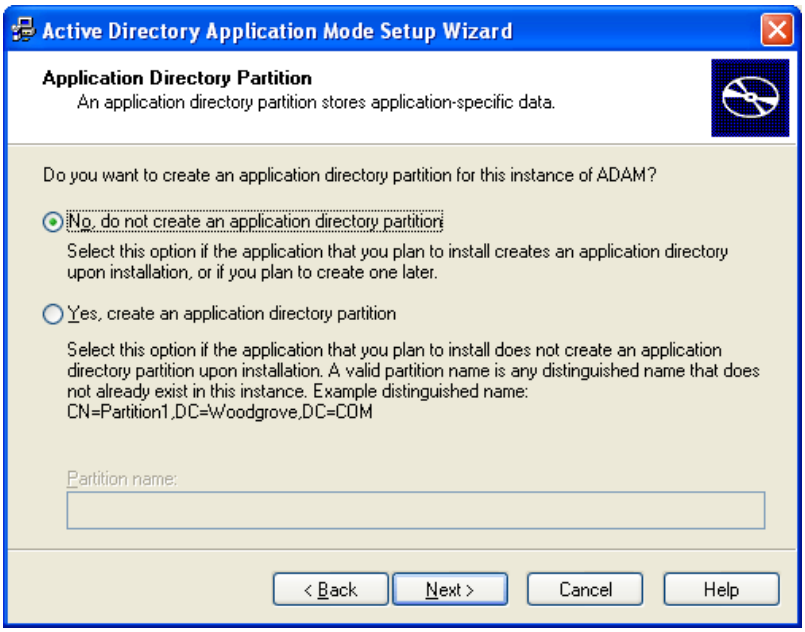


10 Enter the ADAM instance port number in the LDAP port number field and enter the ADAM instance SSL port number in the SSL port number field. The default LDAP port number is 50000 and the SSL port number 500001. If Active Directory is not installed on the computer, the default will be LDAP port number 389 and SSL port number 636. The default values are recommended, however if required, the port numbers can be manually configured.

NOTE: Make a note of the LDAP port number and SSL port number as this information is required for SecureLogin ADAM configuration.

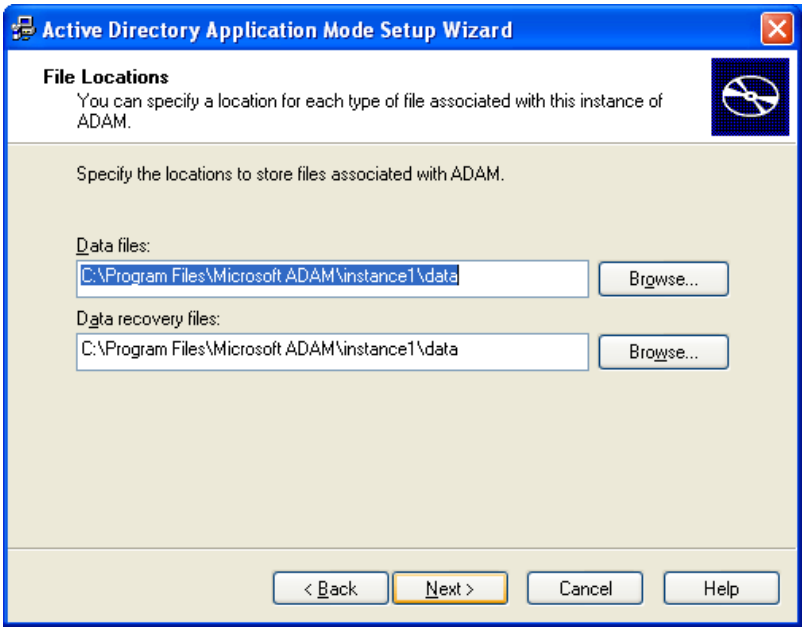
---

11 Click *Next*. The Application Directory Partition page is displayed.



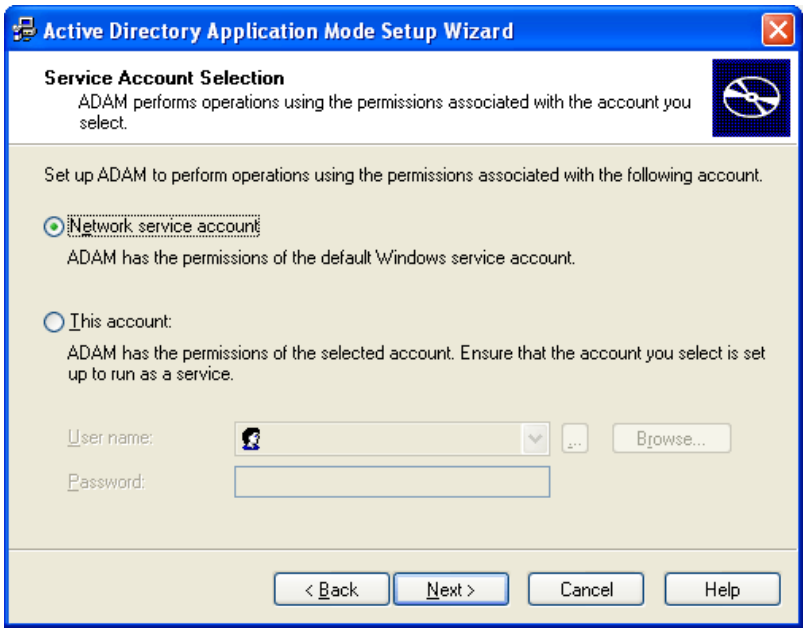
12 Select *No, do not create an application directory partition*.

13 Click *Next*. The File Locations page is displayed.



14 Specify alternative locations for ADAM files in the *Data files* and *Data recovery files* fields or accept default values.

15 Click *Next*. The Service Account Selection page is displayed.



16 Select the *Network service account* option or the Select the *This account* option and type the credentials for the selected service account.

NOTE: The service account selected must have permissions to register a Service Connection Point (SCP) and permission to install and execute SecureLogin. Selecting the Network service account opton is recommended; however, an account with a static password can also be specified.

---

17 Click *Next*. The ADAM Administrators page is displayed.

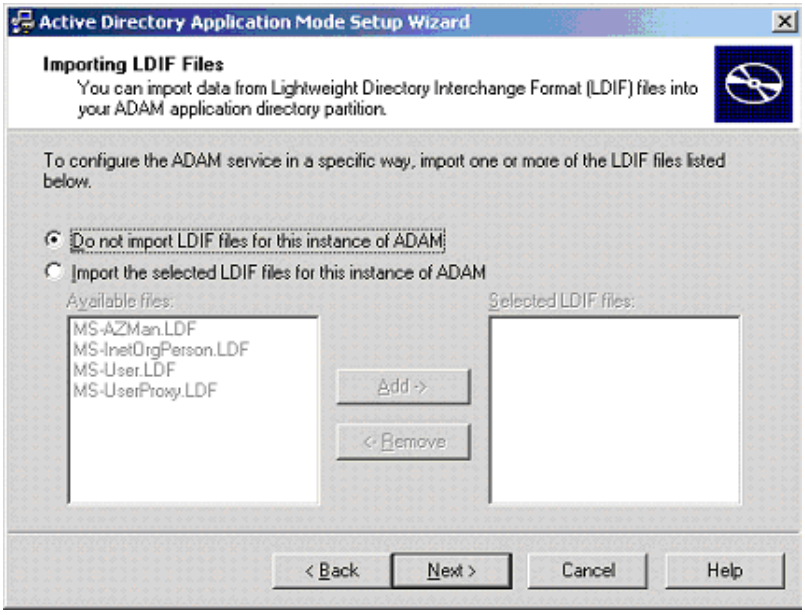
18 Select the *Currently logged on user: SECURELOGIN\Administrator* option or select *This account* and specify the account or group name in the *Account name* field, if required.

NOTE: The account selected needs administrator level permissions for the ADAM instance. In this example, the default is selected as the current user, the Administrator will administer this ADAM instance.

If an alternative account or group is preferred, select This Account and enter the account or group name and credentials.

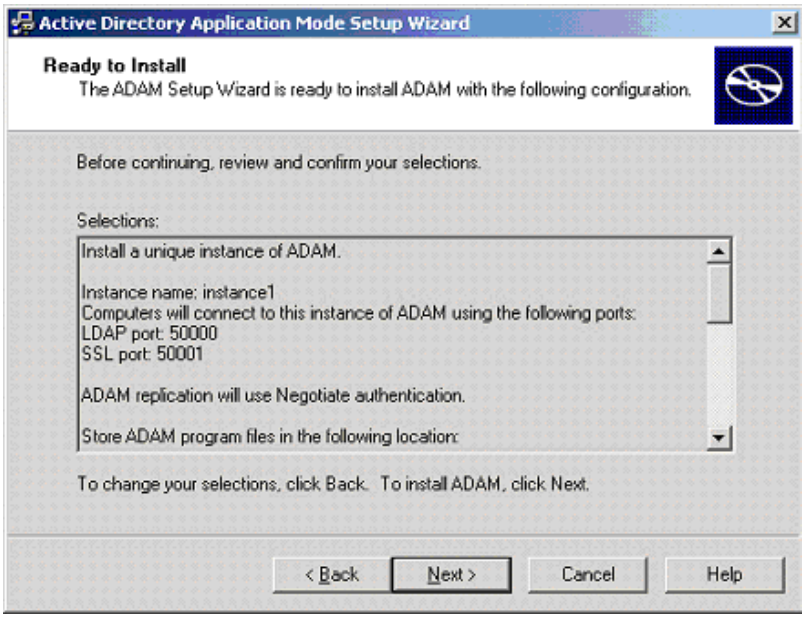
---

19 Click the *Next* button. The Importing LDIF Files page is displayed.



20 Select the *Do not import LDIF files for the instance of ADAM* option is selected.

21 Click *Next*. The Ready to Install page is displayed.



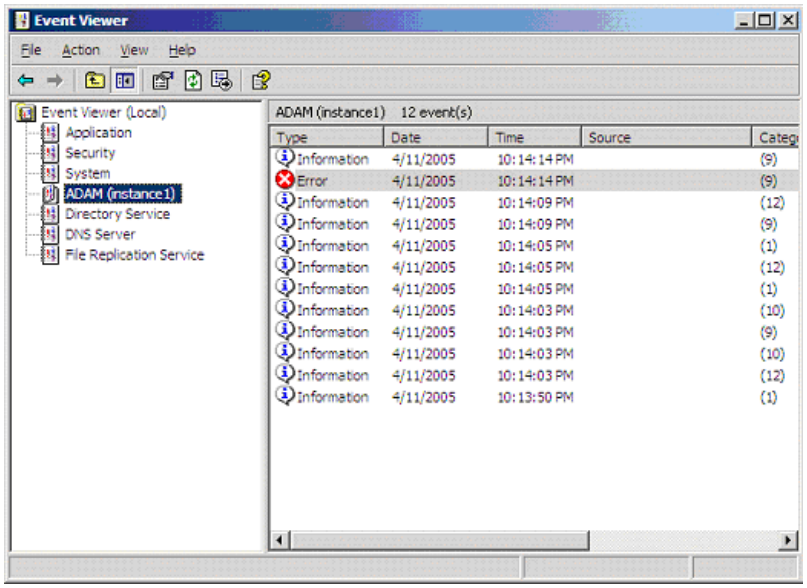
22 Review the setup options in the Selections window to confirm the required options are selected.

23 Click *Next* to continue or *Back* to change selected options.

24 Click *Next* when ADAM instance creation settings are confirmed.

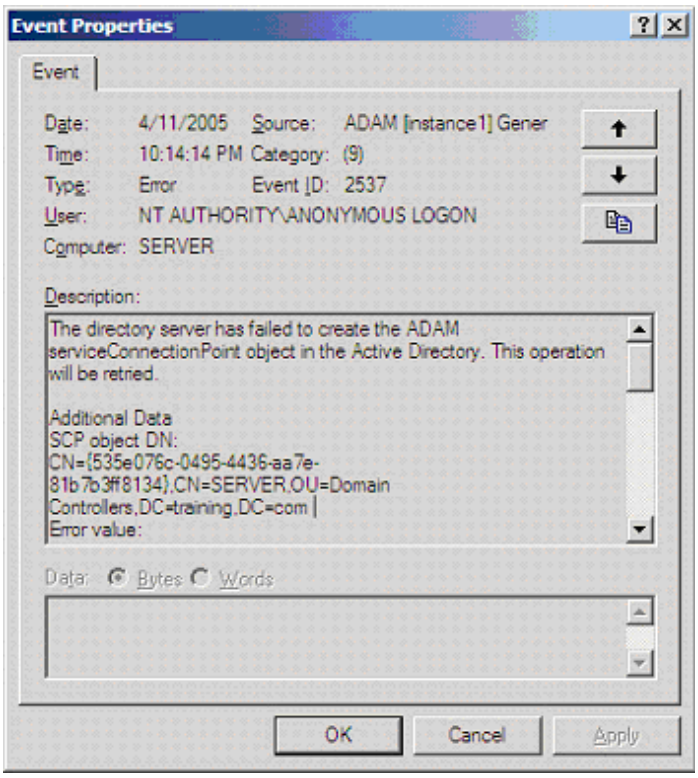
25 Click *Finish* to create the ADAM instance. Review the Windows Event log to ensure the ADAM instance is created without errors.

26 From the Windows Start menu select, *Programs* > *Administrative Tools* > *Event Viewer*. The Windows Event Viewer displays with the ADAM (Instance#) displayed in the Event Viewer hierarchy.



27 Double-click *ADAM (Instance#)* to view the Event log.

28 If an error icon is displayed double-click to view the error details.



When the ADAM instance is successfully created execute the SecureLogin ADAM Configuration wizard to automatically extend the ADAM instance schema and assign Read and Write Rights to directory user objects.

5.5.2 Using the ADAM Configuration Wizard

Before executing the SecureLogin ADAM Configuration wizard:

1 Navigate to the Tools folder on the CD

2 Copy the `ADAMconfig` folder to your local drive

The SecureLogin ADAM Configuration wizard extends the ADAM Directory Schema with SecureLogin Single Sign-On attributes, creates ADAM partitions and assigns selected directory objects Read and Write permissions to the SecureLogin attributes. The Wizard creates corresponding user Proxy objects for users objects in Active Directory, including the directory hierarchy to the ADAM instance and can be used to synchronize user object structure after initial SecureLogin Configuration.

To run the SecureLogin ADAM Configuration wizard:

1 Log on to the ADAM instance/server (or administration workstation if separate) as Administrator (or a user with Administrator level access).

2 Double-click the *AdamConfig.exe* file.

The Welcome to the SecureLogin ADAM Configuration wizard page is displayed. Ensure you have all the required Active Directory and ADAM Administrator account details selected during ADAM instance creation.

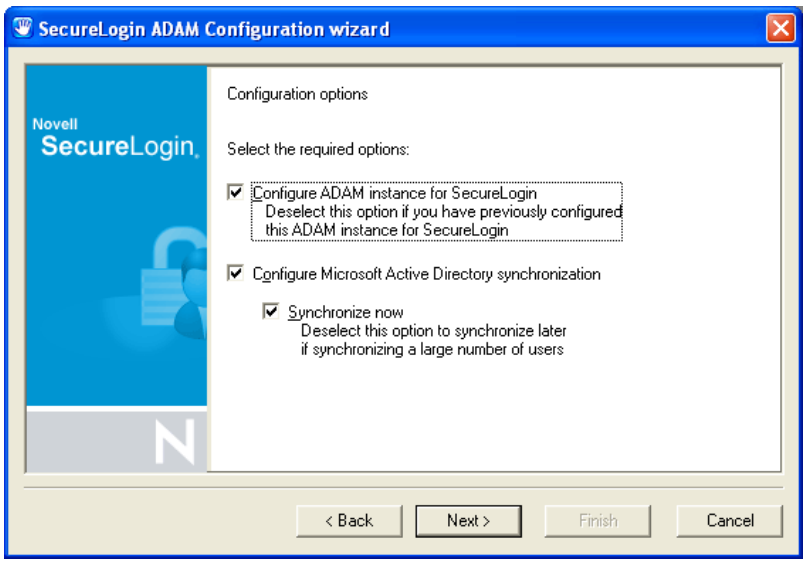
3 Click *Next*.

NOTE: The ADAM schema can be extended manually at the command line using the `MS-UserProxy.LDF` and `sso-adam-schema.LDF` files. These files are located in the `Tools` folder of the SecureLogin distribution CD. We recommend that this procedure is only performed with the assistance of our consultants.

---

4 Select the Configure ADAM instance for SecureLogin option on first execution of the SecureLogin ADAM Configuration wizard.

Although configuration is required only once, selection of this option on subsequent executions has no adverse affects.



The SecureLogin ADAM Configuration wizard copies across selected Active Directory user data to the ADAM instance, including the directory hierarchy.

NOTE: Directory synchronization of a large number of users may adversely affect network performance. The SecureLogin ADAM Configuration wizard can be executed and directory synchronization delayed to a convenient time.

The SecureLogin ADAM Configuration wizard can be executed at any time to synchronize updated Active Directory user data. A command file, `SyncAdam.cmd` is located in the AdamConfig folder copied to the local drive. The `SyncAdam.cmd` cannot be executed prior to running the AdamConfig wizard.

---

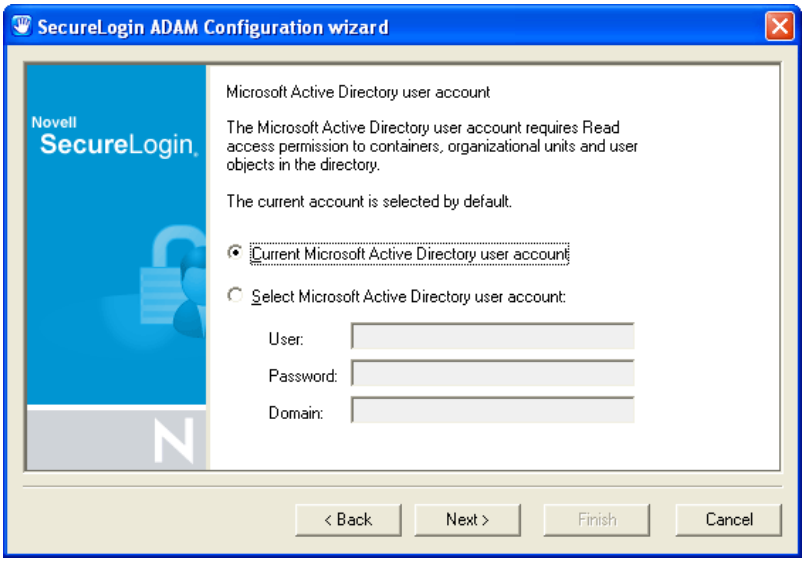
5 Select the *Configure Microsoft Active Directory synchronization* option.

6 Check the *Synchronize now* check box if required.

NOTE: Each time a new organizational unit is created in Active Directory the SecureLogin ADAM Configuration wizard, or the `SyncAdam.cmd` command file, must be executed to synchronize with the ADAM Instance and assign Read and Write permissions. For more information refer to section Section 5.5.4, "Synchronize Data from Active Directory to an ADAM Instance," on page 78.

---

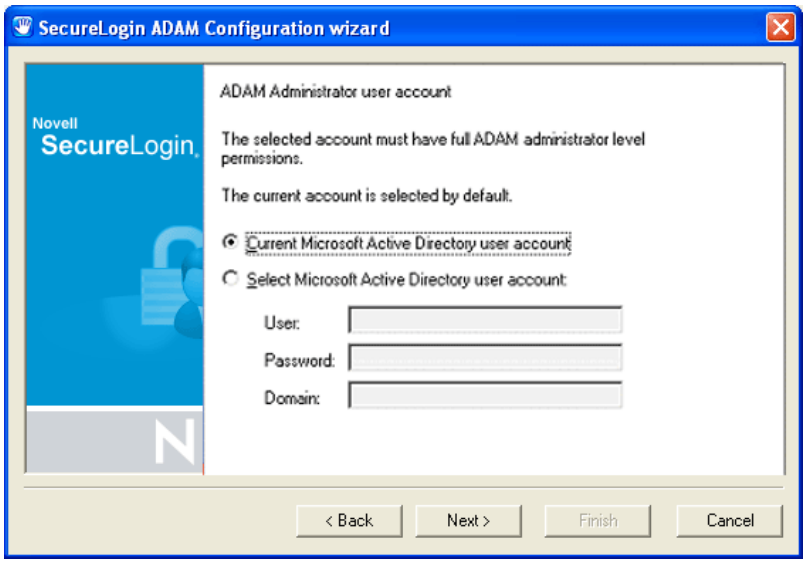
7 Click *Next*. The Microsoft Active Directory user account page is displayed.



The account selected in this page is used to access and copy the Active Directory object data for synchronization with the ADAM instance, so it must have Read permission. This account muct not have Write permission.

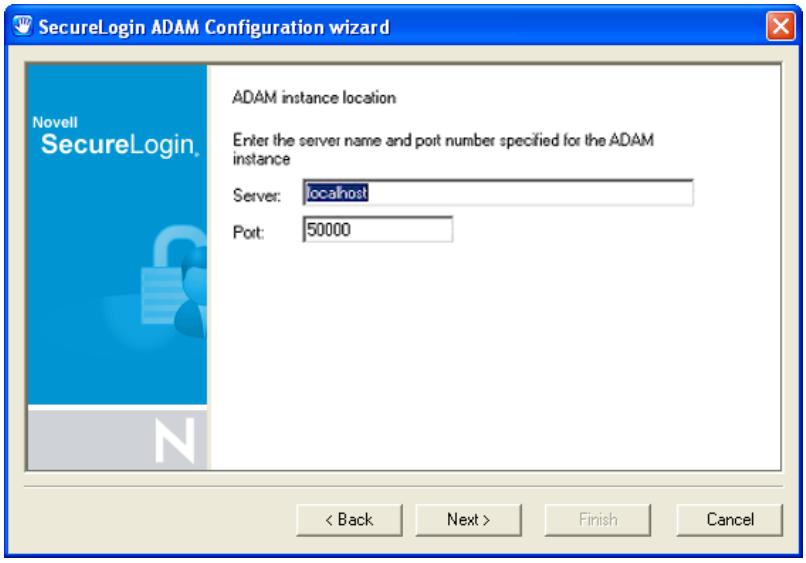
8 Select *Current Microsoft Active Directory User Account* or select the *Select Microsoft Active Directory user account* option and enter the account details in the *User*, *Password* and *Domain fields* and click *Next.*

The ADAM Administrator user account page is displayed.



The account selected in this dialog box is used to manage SecureLogin in this ADAM instance and therefore requires Administrator level access. By default the current account (the one you have logged on with) is selected. However, any user account that has Administrator level access to the ADAM instance is valid.

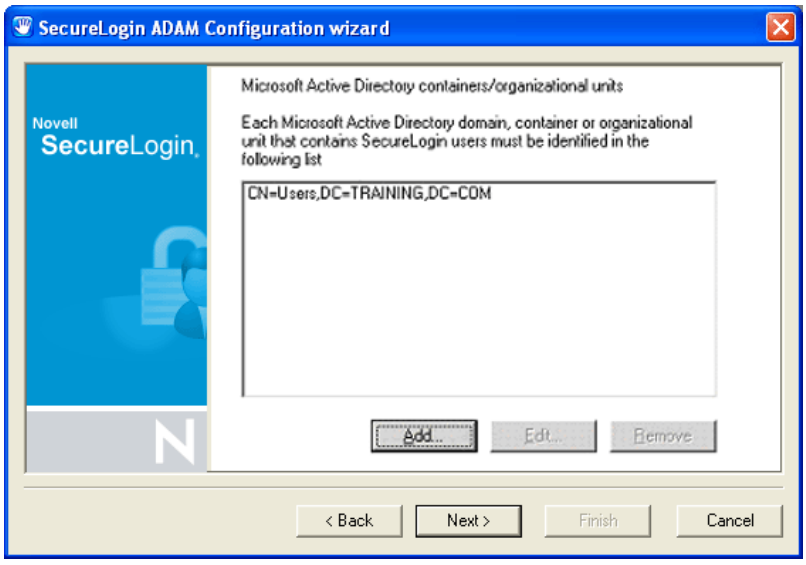
9 Select the *Current Microsoft Active Directory user account* option or the *Select Microsoft Active Directory user account* option and enter the account details in the *User*, *Password* and *Domain* fields and click the *Next* button. The ADAM instance location page is displayed.



10 The default server value is localhost. Choose an alternative server if you are hosting your ADAM instance on another computer.

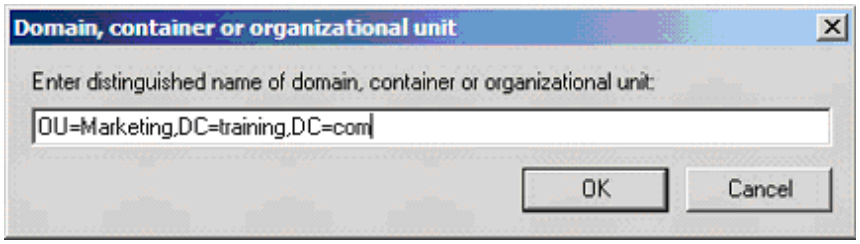
The default port is 50000. Enter an alternative port number if this is not the ADAM instance server port.

Accept the default values or specify the alternative Server and Port values as required and click *Next*. The Microsoft Active Directory containers/organizational units dialog box is displayed.



All containers and organizational units that include SecureLogin users are specified in this dialog box, to assign SecureLogin rights and select for Microsoft Active Directory synchronization.

11 Click the *Add* Button.The Domain, Container or Organizational unit dialog box is displayed.

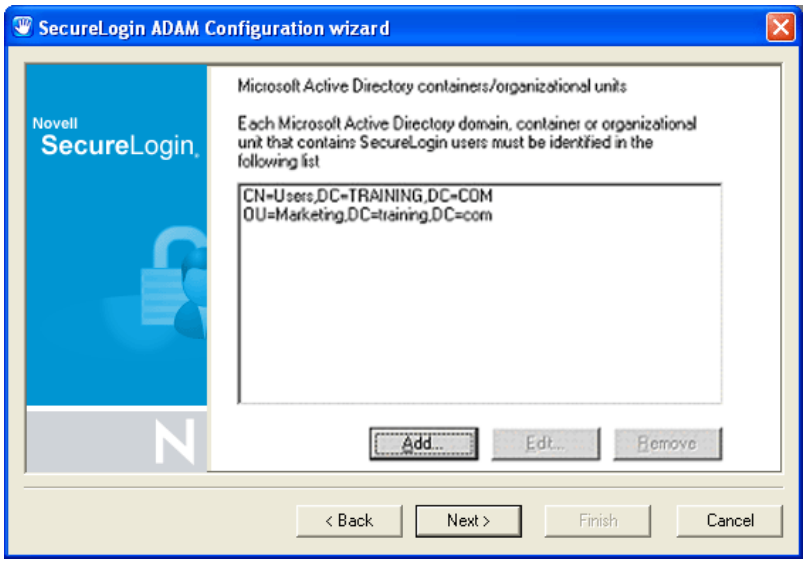


12 Specify the full distinguished name in the *Enter distinguished name of domain, container or organizational unit* field.

13 Click *OK*. The ADAM Configuration error message box will be displayed if the distinguished name of the domain, container or organizational unit specified is invalid.

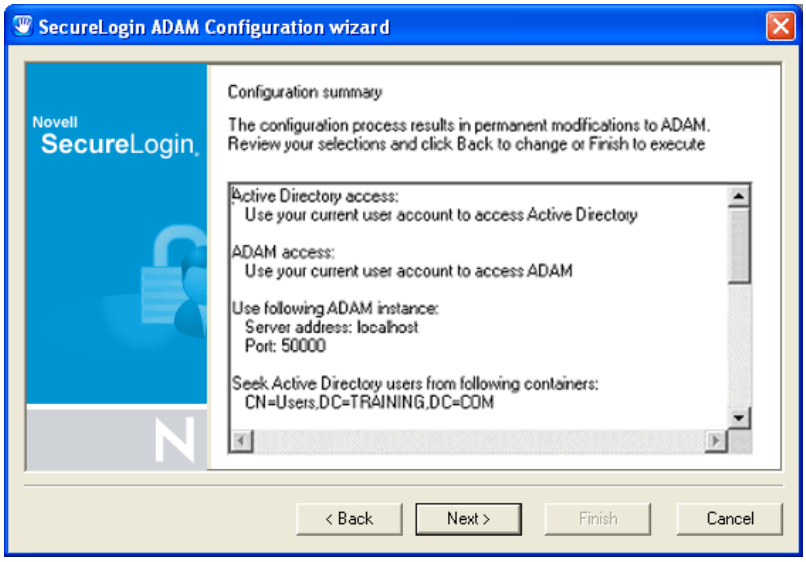
If this occurs, click the *OK* button. Re-enter the correct name in the Enter distinguished name of domain, container or organizational unit field and click *OK*.

14 Click *Next* when all required objects are added to the list.



The Configuration summary dialog box is displayed

15 Click *Back* to change details or *Finish* to execute.



The SecureLogin ADAM Configuration - Termination dialog box is displayed if the configuration was not able to complete successfully.

If this occurs, review the text box to investigate cause of termination. If a solution to the problem is determined, click *Close* and repeat execution of the SecureLogin ADAM Configuration wizard.

The SecureLogin ADAM configuration - Finished dialog box is displayed.

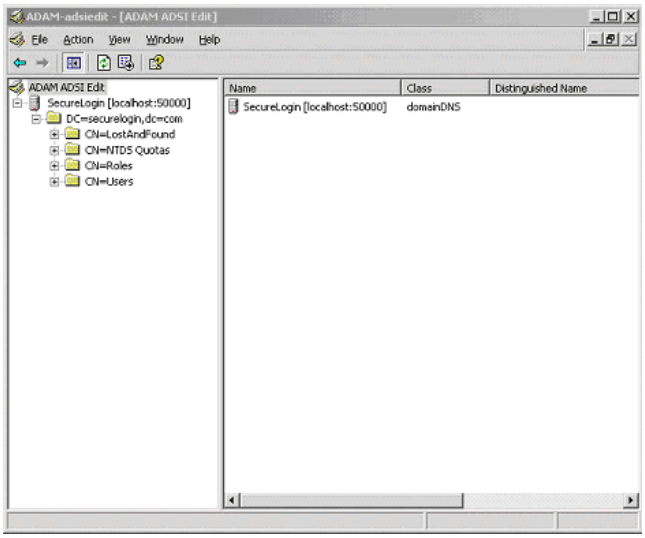
16 Click *Close*.

5.5.3 Using the ADAM ADSI Edit Tool

The ADSI Edit tool is a MMC snap-in used to view all objects in the directory (including schema and configuration information), modify objects and set access control lists on objects.

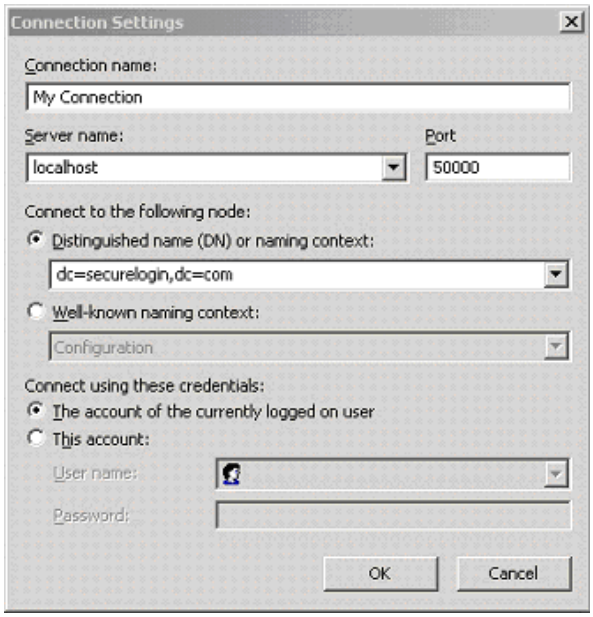
To check and review SecureLogin ADAM configuration start the ADSI Edit tool:

1 Select from the *Start* > *Programs* > *ADAM* > A*DAM ADSI Edit*. The ADAM ADSI Edit tool is displayed.



2 Select A*DAM ADSI Edit* in the hierarchy pane, to view the ADAM Instance details.

3 Select *Connect to* from the Action menu. The Connection Settings dialog box is displayed.



4 Specify a name for the connection in the *Connection name* field.

5 Specify the ADAM instance server name in the *Server name* field.

6 Specify the ADAM instance port name in the *Port name* field.

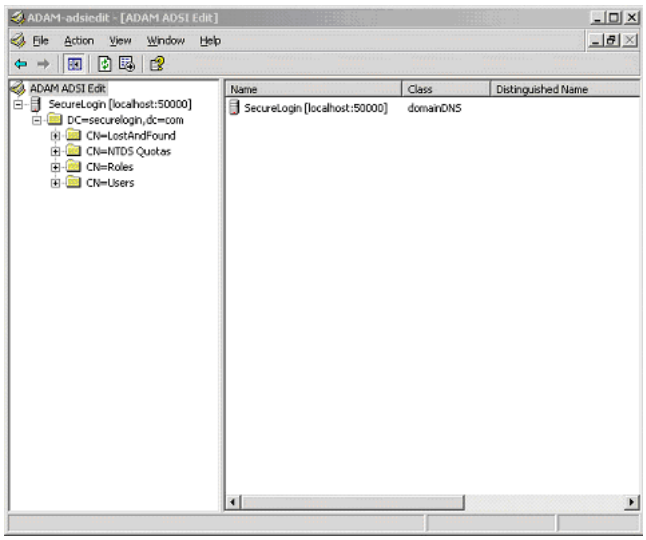
7 Select the *Distinguished name (DN) or naming context* option.

8 Specify the *Distinguished Name in the Distinguished name (DN) or naming context* field.

9 Select a *Connect using these credentials*, account option to connect to the ADAM instance.

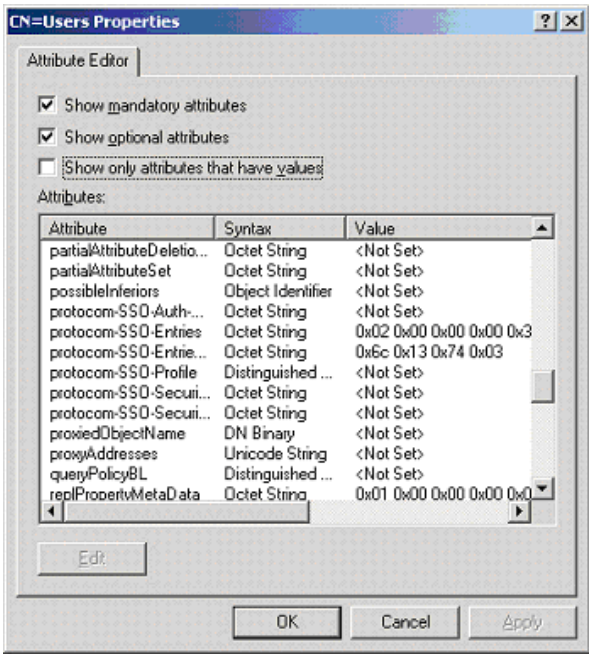
The account of the currently logged on user option is selected in this example.

10 Click *OK*. The ADSI Edit tool displays the selected ADAM instance.



Right-click on the Users container to display the context menu.

11 Select the *Properties* option. The CN=Users Properties dialog box is displayed.



12 To confirm the schema attributes have been added successfully, scroll down the Attributes table window to display the six SSO attributes.

Repeat for each container and/or organizational unit containing SecureLogin users to ensure rights have been successfully assigned.

If the SecureLogin attributes do not display, execute the ADAM Configuration wizard and ensure you have specified the required container, organizational unit and/or user object.

Contact Novell Technical Support for assistance if required.

5.5.4 Synchronize Data from Active Directory to an ADAM Instance

Active Directory to ADAM Synchronizer is a command-line tool that synchronizes data from an Active Directory forest to a configuration set of an ADAM instance. This is used to ensure that new users added to Active Directory have objects representing their SecureLogin data created in the ADAM instance.

To synchronize data from Active Directory to an ADAM instance, open the folder where you copied the ADAM files to and double-click the `syncadam.cmd` file.

It is advisable to run the synchronization method on a regular basis, or when Active Directory users are changed. A way to manage this would be to add the process to the Windows Scheduled Tasks.

Once the synchronization is complete, check the log file, `SyncAdam.log` to make sure that the process was successful.

Automatically Synchronized

The following processes are automatically synchronized:

- A new container or organizational unit in Active Directory will be created as a corresponding container in ADAM.
- A new user in Active Directory will be created as ADAM user proxy.
- a renamed user object in Active Directory will cause corresponding user proxy to be renamed in ADAM.
- A moved user object in Active Directory will cause corresponding user proxy to be moved in ADAM. This requires both user object source container and destination container in synchronization scope.

Not Synchronized Automatically

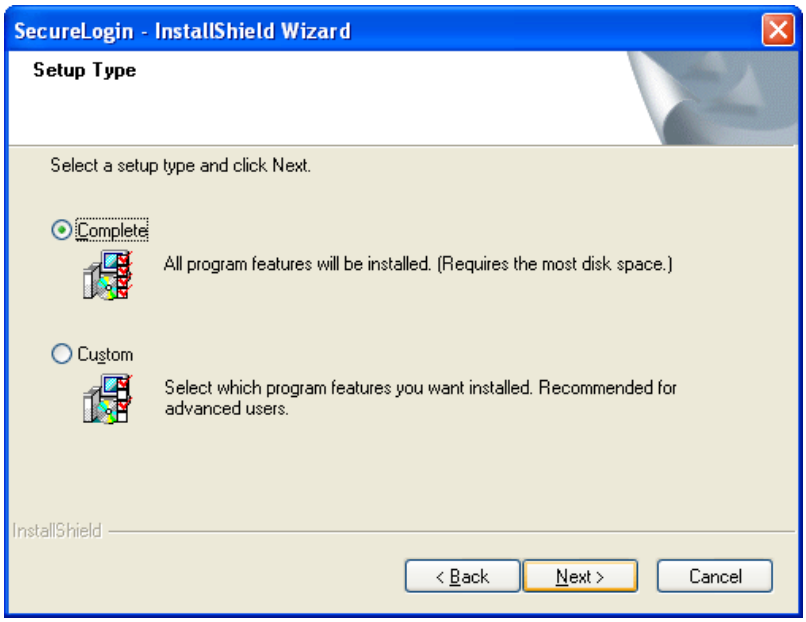
The following processes are not automatically synchronized:

- Deleted user objects in Active Directory are not deleted in ADAM by default. This is due to safety reasons. You can override this by manually editing `SyncAdam.config`. However this is not recommended unless there is a good reason to as the user name may conflict with 'zombie' user or performance issues.
- Deleted, moved or renamed containers and organizational units in Active Directory will not be reflected to ADAM. Changes to existing container or OU objects in Active Directory must be manually reflected to ADAM using the ADSI Edit tool or any other directory editor. For example, if an OU is renamed in Active Directory, it must be renamed in ADAM. Due to safety reasons, synchronization will not run if existing containers and OU's do not match with Active Directory and ADAM.

5.6 Installing SecureLogin in the ADAM Environment

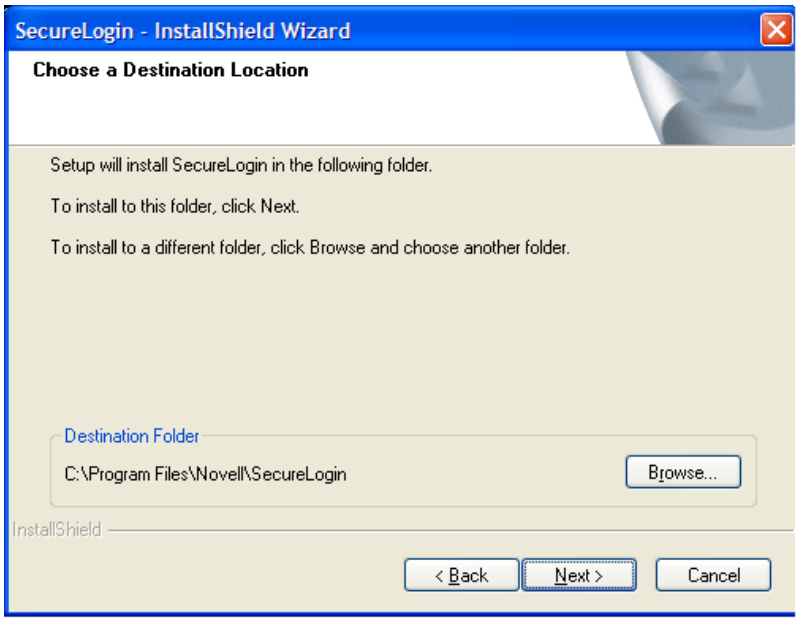
1. Run `setup.exe`, found in the `\securelogin\client` directory.
2. Select a language, click *Next* twice, then accept the license agreement.

3 Select setup type, then click *Next*.



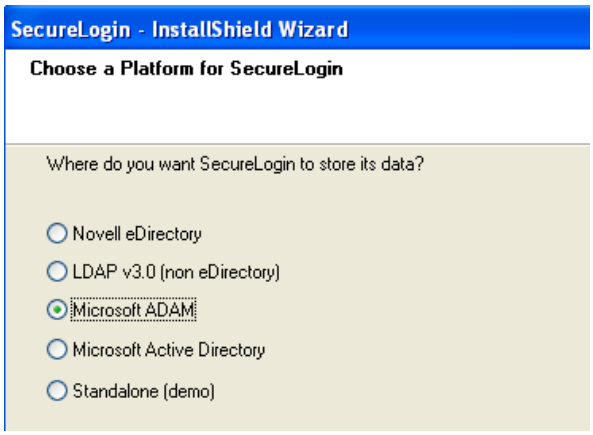
If you select the Complete setup option, the default values are used.

4 (Conditional) If you select the Custom setup option, the Choose a destination folder dialog box appears.

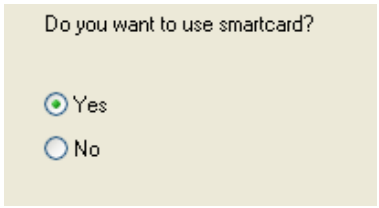


5 (Conditional) Click *Next*, to install SecureLogin to the default folder or click *Browse* and choose another folder to install.

6 Click *Microsoft ADAM* > *Next*.



7 In the Do you want to use smartcard dialog box, select No, if you do not want to use smartcard, then continue with Step.

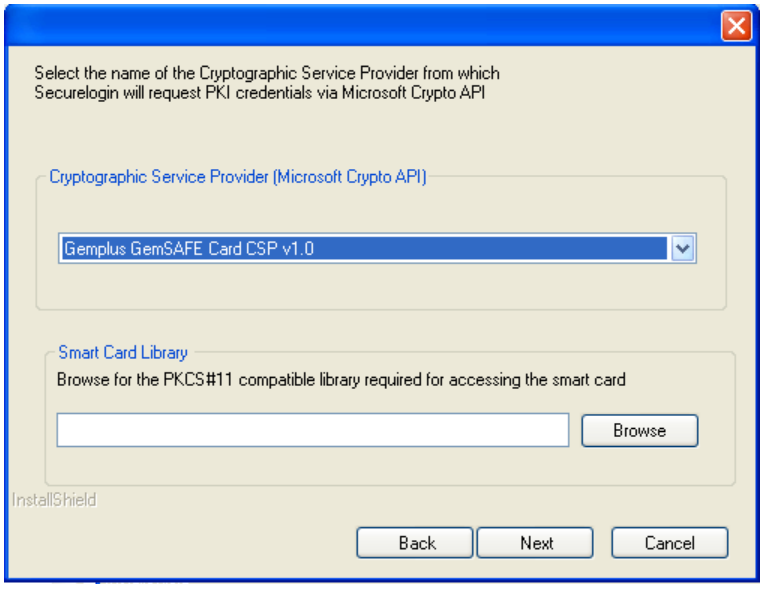


8 (Conditional) If you want to use smartcard and if ActiveClient is detected in your system, select *Yes*, *Click* , then continue with Step 8.

9 (Conditional) If you want to use smartcard and if ActiveClient is not detected in your system:

9a Select *Yes*, Click *Next*.

9b (Conditional) Select a cryptographic service provider from which SecureLogin will request PKI credentials via Microsoft Crypto API.



9c Click *Browse* and select a PKCS#11 compatible library required for accessing the smartcard, then click *Next*.

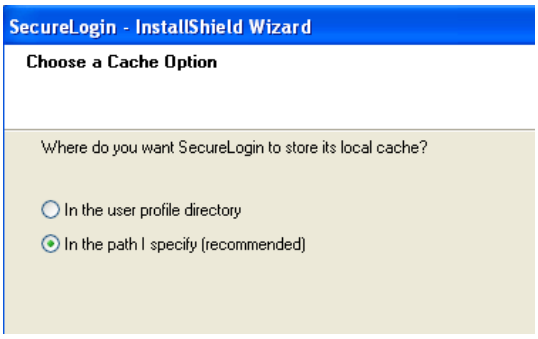
NOTE: This will speciy the location of the Cryptographic Token Interface installed as part of the smartcard vendor's software. These API files will be used by SecureLogin to communicate with the smartcard.

Manually configuring the third party smartcard PKCS library Assumes a high level of understanding the Cryptographic Service Provider's product.

For more information and instructions about smartcard settings and cryptographic tokens, see the *Novell SecureLogin 6.0 Administration Guide*.

---

10 (Conditional) The Installation options dialog box is displayed if you have selected the custom setup option.



Specify where you want SecureLogin to store its local cache.

11 (Conditional) Click *Next*, after the directory location is defined to continue to the next dialog box.

If Citrix or terminal services applications are detected, the Citrix/remote client options dialog box is displayed.

12 (Conditional) Select features that you want to install at the Select Features dialog box, then click *Next*.

13 At the Ready to Install SecureLogin dialog box, click *Install.*

14 By default, the Launch Readme option is selected. Click *Next.*

15 By default, the Start SecureLogin at the Windows startup is selected. Deselect the option if you do not want SecureLogin to start at the Windows startup.

16 Click *Finish*.

17 Specify when you want to restart the computer, then click *OK*.

5.7 Setting Up Passphrase

A SecureLogin passphrase is a question and response combination used as an alternative form of identity verification. Passphrase functionality protects SecureLogin credentials from unauthorized access and enables users to access SecureLogin in offline mode. Passphrases can also be used as a substitute authentication mode if for example, a user forgets their password. Depending on the administrator's preferences SecureLogin passphrase questions can be generated by the administrator and/or the user.

If a passphrase has previously been configured this dialog box will not display and the installation is complete.

On initial login to SecureLogin all users are requested to save a passphrase response. It is important that this response is easy to recall as it cannot be viewed by anyone.

As administrator, and therefore first user of SecureLogin, you must create a passphrase question for yourself.

1. Specify a question in the *Enter a Question* field.
2. Specify an answer in the *Enter the Answer* field.
3. Re-enter the answer in the *Confirm the Answer* field.
4. Click *OK* to save the passphrase.

NOTE: When you upgrade SecureLogin, all user data including the users' passphrase question and response from the previous version are stored. Therefore, creation of new passphrase is not required after upgrading SecureLogin from a previous version.

5.8 Deploying

SecureLogin provides centralized management and deployment of user configuration via efficient leveraging of the directory structure and administration tools. In Microsoft ADAM, administrators manage users via the Administrative Management Utility accessed from the Windows Start menu.

5.8.1 Configuring User's Environment

Configuring a user's SecureLogin environment includes:

- Setting Preferences
- Creating Password Policies (Optional)
- Enabling required applications on SecureLogin
- Creating of Passsphrase questions for user selection (optional)

It is recommended that SecureLogin configuration is trailled on test user accounts prior to deployment. Comprehensive information on user configuration is provided in the administration guide.

SecureLogin provides a range of options for deployment and distribution of user configurations.

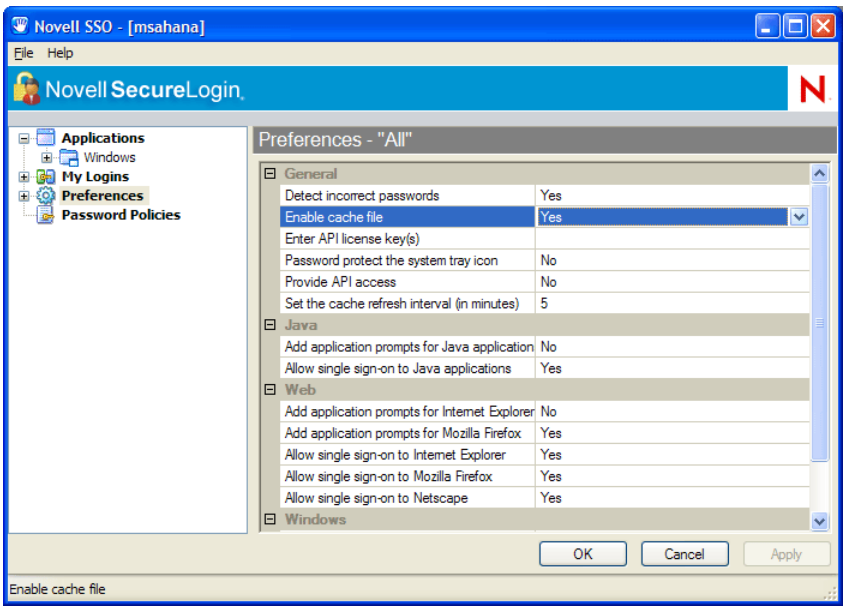
5.8.2 Managing SecureLogin in an ADAM Instance

SecureLogin users are managed in the Administrative Management Utility. For more information on SecureLogin administration, refer to the *Novell SecureLogin 6.0 Administration Guide*. The Administrative Management Utility is accessed via the Start menu. The Administrative Management Utility manages users at the container, organizational unit and user object levels.

1. Access SLManager.
2. Specify the distinguished name of the required object. For example, CN=users, dc=SecureLogin, dc=com.
3. The Administrative Management Utility is displayed.

5.8.3 Installing SecureLogin for Mobile Users and Notebooks

To install SecureLogin for mobile and remote users, follows the procedure found in Section 5.6, "Installing SecureLogin in the ADAM Environment," on page 79. However, it is importatn that you ensure the cache is saved locally, or users will be uinable to access the aplications when they are disconnected from the network. The Enable Cache file setting in the Preferences options of the SecureLogin is set to Yes by default. This option can be set either at the organizational unit level or on a per user basis.


Novell SSO - [msahana]
File Help
Novell SecureLogin
Applications
Windows
My Logins
Preferences
Password Policies
Preferences - "All"
General
Detect incorrect passwords Yes
Enable cache file Yes
Enter API license key(s)
Password protect the system tray icon No
Provide API access No
Set the cache refresh interval (in minutes) 5
Java
Add application prompts for Java application No
Allow single sign-on to Java applications Yes
Web
Add application prompts for Internet Explorer No
Add application prompts for Mozilla Firefox Yes
Allow single sign-on to Internet Explorer Yes
Allow single sign-on to Mozilla Firefox Yes
Allow single sign-on to Netscape Yes
Windows
OK
Cancel
Apply
Enable cache file

SecureLogin on a Standalone Workstation

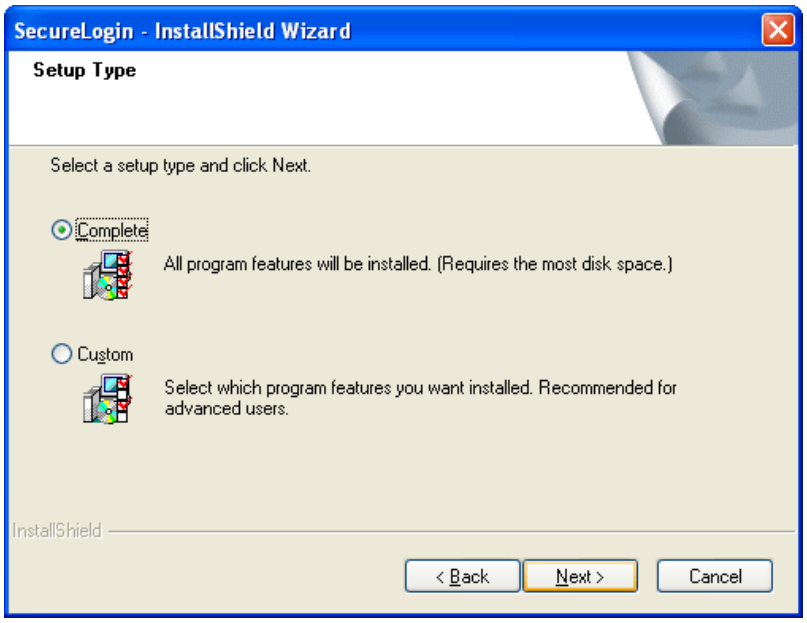
6

The standalone option runs without directory synchronization and uses only local cache files. Select this option to demonstrate or evaluate SecureLogin.

This section contains the following information:

6.1 Installing SecureLogin: Standalone Workstations

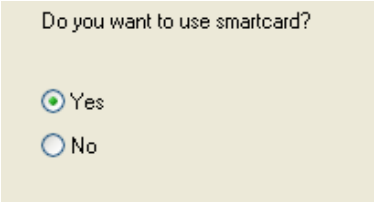
1. Run `setup.exe`, found in the `\securelogin\client` directory.
2. Select a language, click *Next*, and accept the license agreement.
3. Click *Complete* > *Next*.



The Complete option uses default values and installs SecureLogin in *c:\program files\novell\securelogin*. For options available through the Custom option, see “Using the Custom Option for Standalone Workstations” on page 58.

4. Select *Standalone* as the platform where SecureLogin will store its data, then click *Next*. The Do you want to use smartcard dialog box is displayed.

5 (Conditional) If you don't want to use smartcard, select *No,* click *Next,* then continue with Step 8.

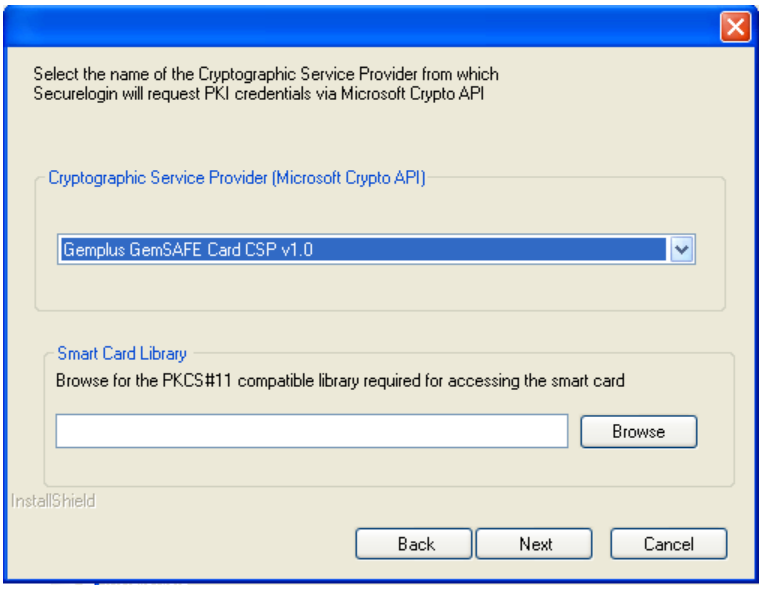


6 (Conditional) If you want to use smartcard and if ActiveClient is detected in your system, select *Yes,*Click *Next,* then continue with Step 8.

7 (Conditional) If you want to use smartcard and if ActiveClient is not detected in your system:

7a Select *Yes,* click *Next.*

7b (Conditional) Select a cryptographic service provider from which SecureLogin will request PKI credentials via Microsoft Crypto API.



7c Click *Browse* and select a PKCS#11 compatible library required for accessing the smartcard, then click *Next*.

NOTE: This will speciy the location of the Cryptographic Token Interface installed as part of the smartcard vendor's software. These API files will be used by SecureLogin to communicate with the smart card.

Manually configuring the third party smartcard PKCS library Assumes a high level of understanding the Cryptographic Service Provider's product.

For more information and instructions about smartcard settings and cryptographic tokens, see the *Novell SecureLogin 6.0 Administration Guide*.

---

8 Click *Next* > *Install*.

9 By default, the Launch Readme option is selected. Click *Next.*

10 By default, the Start SecureLogin at the Windows startup is selected. Deselect the option if you do not want SecureLogin to start at the Windows startup.

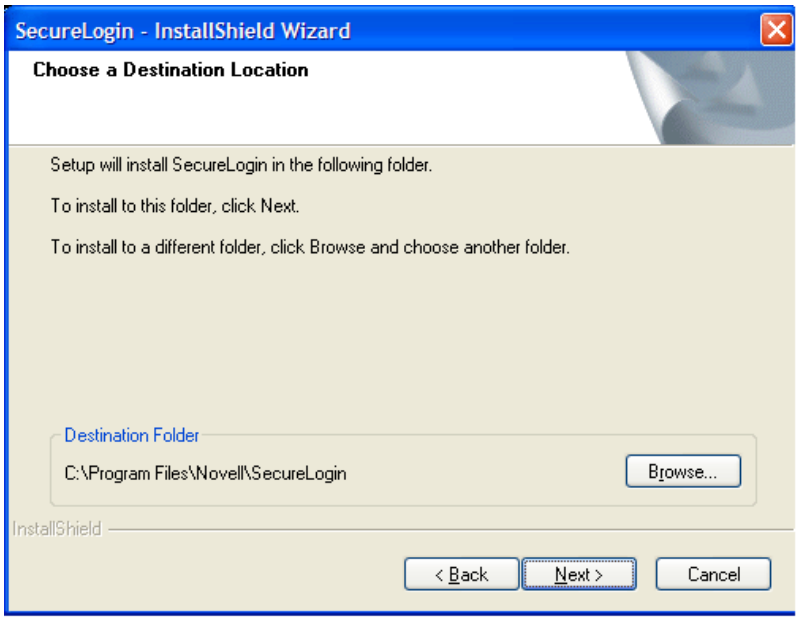
11 Click *Finish*.

12 Specify when you want to restart the computer, then click *OK*.

6.2 Using the Custom Option for Standalone Workstations

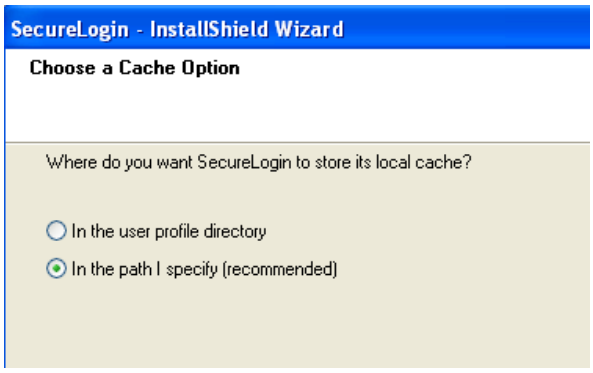
The Custom option provides the same defaults as does the Complete option, but enables you to do the following:

- Specify where SecureLogin files will be stored.

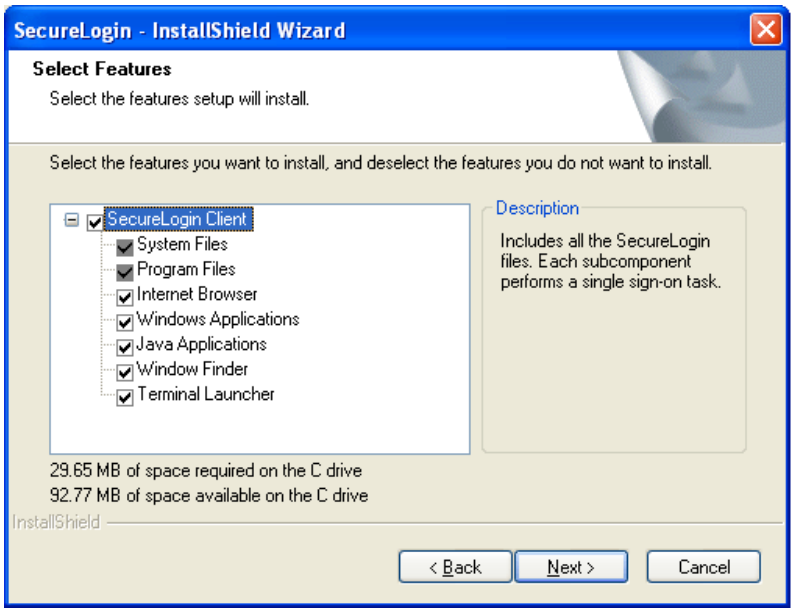


You can use the default path or specify a different one.

- Specify a path for to store the SecureLogin local cache.



- Select SecureLogin components.



The Description panel provides information about a component that you select.

If the Java Runtime Environment (JRE) is not installed on your workstation, the Java component doesn't appear among the option. To use the Java component, you need JRE 1.4 or later.

Upgrading from Earlier Versions 7

This section provides information on the following:

7.1 Upgrading Entirely to SecureLogin 6.0

If you plan to upgrade all previous versions to SecureLogin 6.0, use information in this section. If you plan to have a mixed environment, where some workstation are running SecureLogin 6.0 but other workstations are running earlier versions, see Running SecureLogin 6.0 in Mixed Environments.

Before upgrading from SecureLogin 3.0.x. to SecureLogin 6.0, close SecureLogin. The installation program can normally handle locked files.

7.2 Upgrading from Novell SecureLogin 3.5

Even if SecureLogin 3.5 was deployed to work with eDirecoty, a cache most likely exists on the workstation, unless the administrator turned that capability off. After you upgrade, the later version of SecureLogin recognizes the cache left by SecureLogin 3.5 and automatically works with it.

If all SecureLogin 3.5 data was stored in eDirectory, and if SecureLogin 6.0 is installed to work with Novell SecretStore®, SecureLogin 6.0 still uses the Prot:* attributes in the directory, even if it is deployed to use SecretStore.

7.2.1 Upgrading in Standalone Mode

When you upgrade SecureLogin in the standalone mode, you will be prompted whether to run SecureLogin in the Seamless mode or not.

If you select yes, SecureLogin 6.0 will automatically take your NDS username and password and login.

7.3 Upgrading from Novell SecureLogin 3.0.x

To upgrade from SecureLogin 3.0.x versions:

1. Uninstall SecureLogin 3.0.x from your workstation.
2. Run `setup.exe` found in the `\securelogin\client` directory on the Novell SecureLogin 6.0 image or CD.

7.4 Running SecureLogin 6.0 in Mixed Environments

You can run SecureLogin 6.0 and SecureLogin 3.0.x in the same environment.

When SecureLogin 6.0 runs in the same environment as SecureLogin 3.0.x, SecureLogin 6.0 does the following:

- Versions the SecureLogin data store.
- Saves SecureLogin 6.0 data in the SecureLogin 3.0 data format.

This mixed mode enables you to gradually deploy SecureLogin 6.0 in a SecureLogin 3.0 environment while still allowing you to perform most administration tasks during the transition.

Deploying SecureLogin 6.0 in a mixed environment has the following limitations:

- Limited administrative functionality

  When you run SecureLogin 6.0 in mixed mode, new features such as shadow variables will not work. Also, some SecureLogin 6.0 settings and changing script descriptions aren't supported in mixed mode.
- Warning messages

  To inform you that you are running in mixed mode, a warning message is displayed when data is saved in the SecureLogin 3.0 format.

7.4.1 Upgrading to SecureLogin 6.0

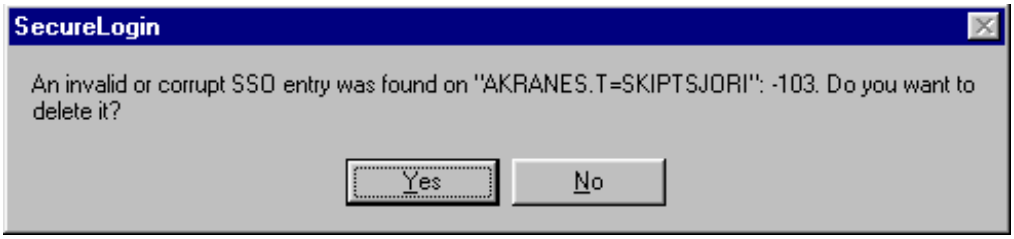
The single sign-on functionality of SecureLogin uses the directory schema to determine which version of the data store to write out. If this functionality finds the new directory attributes that are added by the SecureLogin 6.0 schema tool, SecureLogin uses the new data format.

In mixed environments, SecureLogin 6.0 reads and writes data in the SecureLogin 3.0 format and functions as usual. No administrative intervention is required.

When workstations are upgraded to SecureLogin 6.0, they continue to use the SecureLogin 3.0 data format on the User objects. This functionality allows users to move between SecureLogin 3.0 and SecureLogin 6.0 workstations.

After all users in the tree have been upgraded to SecureLogin 6.0, you can run the schema extension tool and upgrade the directory schema. All SecureLogin clients will then upgrade their data stores to the SecureLogin 6.0 format.

If any SecureLogin clients remain in the tree after the schema has been updated to include the SecureLogin 6.0 attributes, the SecureLogin 3.0 clients will receive the "corrupt data" error message.



After the directory schema has been extend for SecureLogin 6.0, it is not possible to revert to the SecureLogin 3.0 data format.

7.4.2 Managing Mixed Environments

While SecureLogin is running in mixed mode, you will be able to modify most of the corporate and user configuration settings. However, if you attempt to set a new setting, SecureLogin displays the following warning message:

```
SecureLogin was unable to save some of your data because it is not
supported by the currently selected data format version. This
incompatible data has not been saved.
```

The incompatible data is any new setting that appears in SecureLogin 6.0 but was not present in SecureLogin 3.0. Incompatible data could come from the following:

- Dialog position information
- New settings
- Shadow variables

7.5 Phased Upgrades

In large organizations it is often not feasible to fully deploy an application to all users simultaneously. SecureLogin provides full support for phased or staggered upgrades. This allows you to upgrade users without downtime and within an unrestricted time frame.

This flexibility is due to the Cache Synchronization functionality of SecureLogin. Each time a user logs on to the network, the SecureLogin workstation cache is compared and synchronized with the user's SecureLogin data on the directory. During an upgrade the directory and workstation versions will differ for a brief period.

The following table shows scenarios for deploying SecureLogin phased upgrades.

Upgrade	Followed by
Directory Schema first	All workstations upgraded or; Workstations upgraded by object (group policy,container, OU or user).

Upgrade	Followed by
Workstations first	Directory schema updated, with either: • All workstations upgraded, or; • Workstations upgraded by object (group policy, container, OU or user).

NOTE: When upgrading SecureLogin from a previous version, the version running on the administrative workstation (the workstation used to administer SecureLogin) must be the same as the data being administered.

7.6 Hot Desk and Mobile Users

Hot desk users do not work from a fixed workstation and their user data is stored on the directory. For example, in a hospital environment staff may be stationed in a different ward each shift and are able to access their applications and data from any workstation.

When users logs on to SecureLogin, their details are downloaded from the directory to the local workstation cache. All workstations accessed by kiosk mode users must run the same version of SecureLogin. If users log on to an upgraded workstation, they will be unable to access their SecureLogin data on workstations running a previous version of the software.

7.7 Stop Tree Walking

Checking for inherited values from higher level objects is referred to as “tree walking.” Each time the SecureLogin user cache synchronizes with the directory, SecureLogin checks for changed configuration data including preference values, password policies, preconfigured applications, and application definitions.

SecureLogin data not manually configured at the user object level is automatically inherited from higher level directory objects. To ensure higher level object settings are not inadvertently inherited by lower level objects, set Stop walking here to Yes before upgrading.

You can also use Stop walking here to limit directory traffic in organizations where the network is congested or geographically dispersed. Set his function at the organizational unit, or container level to stop SecureLogin from traversing the directory hierarchy past the specified level.

To set Stop walking here at the Users container:

1. Access iManager, then select *Manage SecureLogin SSO* from the left pane. For more information see Section 2.4.2, “Installing Plug-Ins for iManager,” on page 30.
2. Select *Preferences* from the drop-down list.
3. Select the *Stop walking here* option and change the value to *Yes*.
4. Click *apply*.

All user objects in the Users container will now inherit their SecureLogin configuration from the Users container level and below.

7.8 Change the Directory Database Version

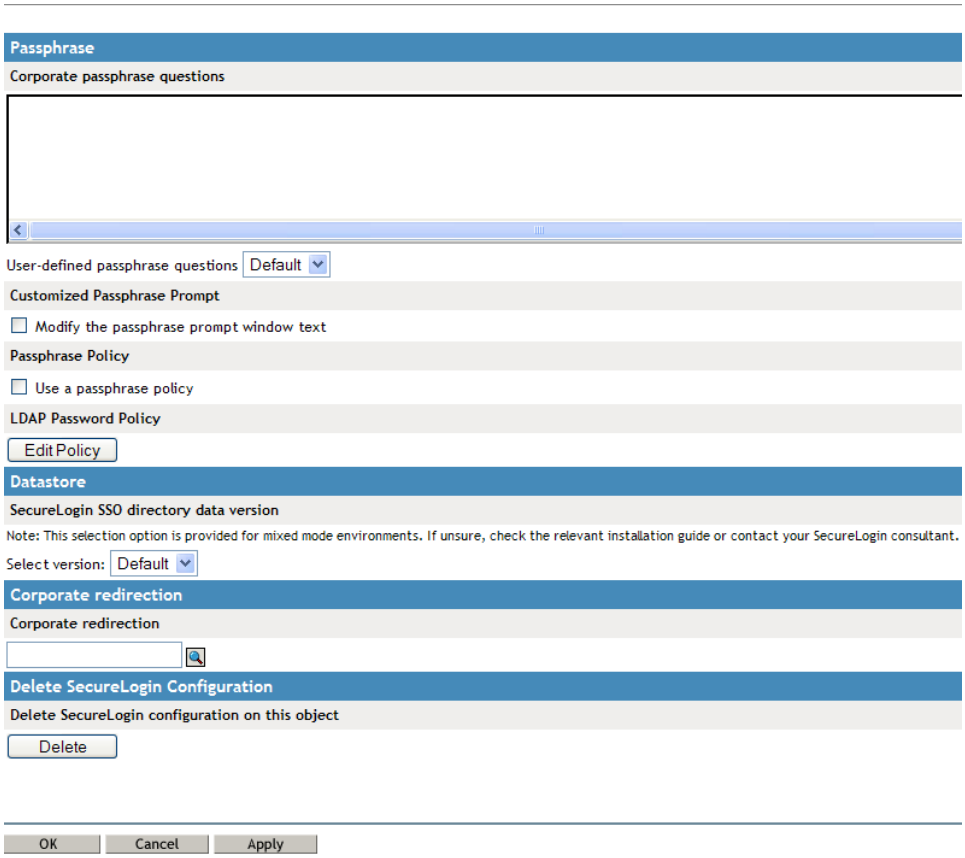
SecureLogin is backward compatible, therefore all workstations running previous versions will continue to operate successfully after the directory is upgraded to the new version. Although the directory is upgraded, the SecureLogin client on the workstation will continue to function as the old version of SecureLogin until you have upgraded all users to the new version and manually set the directory database version to the new version.

You can configure directory database versions at user object, container and organizational unit levels. We recommend you set the database version at the container and organizational unit levels. This should help you manage the database and minimize the possibility of conflicting versions.

NOTE: Manually setting the directory database version is only required for SecureLogin versions prior to 3.5.x.

To set the directory database version at the organizational unit level:

1. Access iManager, then select *Manage SecureLogin SSO* from the left pane. For more information see Section 2.4.2, “Installing Plug-Ins for iManager,” on page 30
2. Select *Advanced Settings* from the drop-down list.
3. From the *Select Version* drop-down list, select the required version.



NOTE: You cannot select a version lesser than your current version.

4 Click *Apply*. When the upgrade is installed on all the workstations, follow the above procedure to change the directory database version. The next time the directory server and the workstation caches are synchronized, SecureLogin will operate in the new version mode.

7.9 Upgrade Deployment Checklist

Before you upgrade:

- Identify mobile and kiosk workstation users.
- Complete your migration plan.
- Back up your SecureLogin data by exporting to an XML file.
- Close SecureLogin. You cannot run the application during an upgrade.

7.10 Develop a Migration Plan

To ensure a smooth transition, it is recommend that you develop a migration plan. When you develop your plan, you need accurate information identifying the following:

- Version of SecureLogin :
  - Set to run on the directory.
  - Installed on the administration workstation.
  - Installed on each user workstation.
- Timeframe within which you must complete the full upgrade.
- Deployment method (automated or manual?)
- Total number of users.
- Which containers/organizational units each user belongs to.
- Kiosk mode users.
- Laptop users.
- Which users, if any, you need to upgrade first.
- Applications required to be SecureLogin enabled.

This information is the basis of the migration plan. You can develop and document migration plans in a variety of ways, the following is an example of one method.

7.11 Example of a Migration Plan

- Section 7.11.1, “The Organization,” on page 96
- Section 7.11.2, “Summary Order of Upgrade,” on page 97

7.11.1 The Organization

Acme is an organization with a total of 30,000 users. 16,000 are allocated a fixed workstation, 3,000 are laptop users, and 11,000 access applications in kiosk mode. The network environment is Microsoft Active Directory and SecureLogin version 3.5 is currently implemented. All users are managed from one administration workstation. ZenWorks is used for application distribution and deployment generally occurs overnight.

Sales OU users have laptops for mobile access to the network. The Central Administration OUs contain a combination of static workstations and laptop users.

Manufacturing and Purchasing OU users are mobile; workstations are accessed in kiosk mode. Users in the remaining OUs are each allocated a workstation for their sole use.

The Java functionality provided by the new version of SecureLogin is eagerly awaited by users in the Sales group, so they have volunteered to trial the upgrade. Once the upgrade is successfully deployed to the Sales group, SecureLogin Single is deployed in stages to the rest of Acme.

7.11.2 Summary Order of Upgrade

1. Directory and test user
2. Sales
3. Central Administration and Human Resources
4. Accounting and Marketing
5. Manufacturing and Purchasing
6. Administration Workstation

Week 1, Day 1

Upgrade the server directory; extend the schema and assign rights to the organizational units. Ensure that all containers and organizational units have the:

- Directory Database Version value 3.0.
- Stop tree walking here preference option value set to Yes.

Create a test user in the Sales OU and change the setting for the user object to Directory Database Version value 3.5 Test single sign-on enabling of required applications.

Week 1, Day 2

On successful deployment of the upgrade on the test user, manually set the Directory Database Version value to 3.5 on the Sales OU to enable full upgrade functionality.

Deploy the SecureLogin upgrade on all Sales OU workstations/laptops. Assist Sales users with single sign-on enabling Java applications.

Ensure all laptop users have the SecureLogin Cache setting enabled to ensure the cache is stored locally.

Week 1, Day 3

Monitor any upgrade issues for the upgraded Sales OU users. If all issues have been resolved successfully install the SecureLogin upgrade on all laptops and workstations associated with the Central Administration and Human Resources OUs.

Set the Directory Database Version value 3.5 on the Central Administration and Human Resources OUs to enable full upgrade functionality.

Week 1, Day 4

Install the SecureLogin upgrade on workstations associated with the following OUs:

- Accounting
- Marketing

Week 1, Day 5

Review and resolve any issues.

Week 1, Day 6

Install the SecureLogin upgrade on workstations associated with the following OUs:

- Manufacturing
- Purchasing

Review any upgrade issues encountered by Central Administration OU users. If all OK, change the Directory Database Version value to 3.5 setting for the following OUs:

- Accounting
- Marketing

Week 2, Day 7

All users now have the SecureLogin upgrade application installed.

Review and resolve any issues.

Upgrade the administration workstation.

Week 2, Day 8

If all issues resolved successfully, change the Directory Database Version value to 3.5 setting for all remaining OUs.

Ensure the following OUs are enabled simultaneously to cater for mobile/kiosk users:

- Manufacturing
- Purchasing

The changeover is planned to occur at midnight and all users have been requested to logout prior to or at this time and wait until 12.10 AM before logging back in.

Week 2, Day 8

Migration completed, review of migration plan commences.

IMPORTANT: Contact Novell Technical Support engineer for help.

Installing and Configuring Secure Workstation

8

This section provides information on the following

8.1 Overview

Secure Workstation locks a workstation when it isn’t being used. You can configure Secure Workstation to execute an administrator-specified lock action after a user-inactivity timeout or after an authentication device such as a smart card is removed.

Scenario: Inactivity Timeout. Secure Workstation is installed on Markus’ workstation. The timeout period is set for 10 minutes. Markus leaves his workstation to attend a department meeting. After 10 minutes, Secure Workstation locks Markus’ workstation. No one can access information on or through that workstation until Markus returns and unlocks it.

Scenario: An Authentication Device Is Removed. Claire is a nurse. Secure Workstation is installed on all the workstations that Claire uses. She logged in to the nursing station’s workstation by using a proximity card. Claire completes a report and then leaves to assist a patient. She removes the proximity card from the workstation. Secure Workstation shuts down the applications that Claire was using and logs Claire off.

Secure Workstation consists of the following components:

- The Novell® Secure Workstation Service
- The Quick Login/Logout Interface
- The Local Policy Editor
- The Secure Workstation Post-Login Method for NMAS™

Secure Workstation is a post-login method. It is similar in some ways to the Workstation Access post-login method that shipped with NMAS 2.0. However, Secure Workstation is more secure than Workstation Access, and does not use a screen saver. Secure Workstation provides more features than Workstation Access.

Secure Workstation supports only Windows 2000 and later versions. Windows 98, Windows ME, Windows NT, and other platforms are not supported.

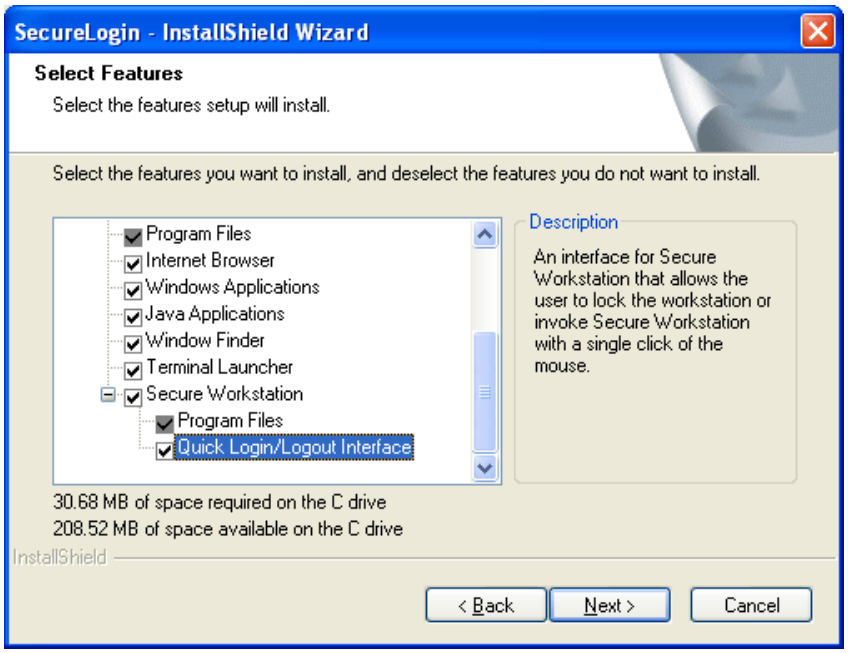
8.2 Setting Up Secure Workstation

This section provides information on the following:

- Section 8.2.1, “Installing Secure Workstation,” on page 100
- Section 8.2.2, “Installing iManager Plug-In to Secure Workstation,” on page 101

8.2.1 Installing Secure Workstation

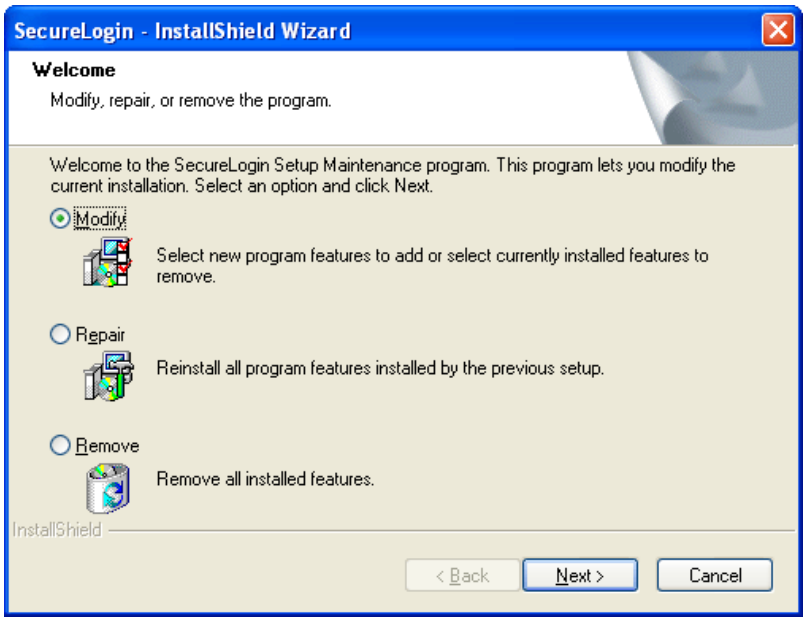
By default, Secure Workstation program files are installed with the Complete option, if the Novell NMAS Client option is selected during a SecureLogin 6.0 client installation. As the following figure illustrates, however, the Quick Login/Logout Interface isn’t installed by default.



If you selected the Custom option and deselected the Secure Workstation component, you can quickly add it

1 Run `setup.exe`, found in the \client directory on the SecureLogin 6.0 image.

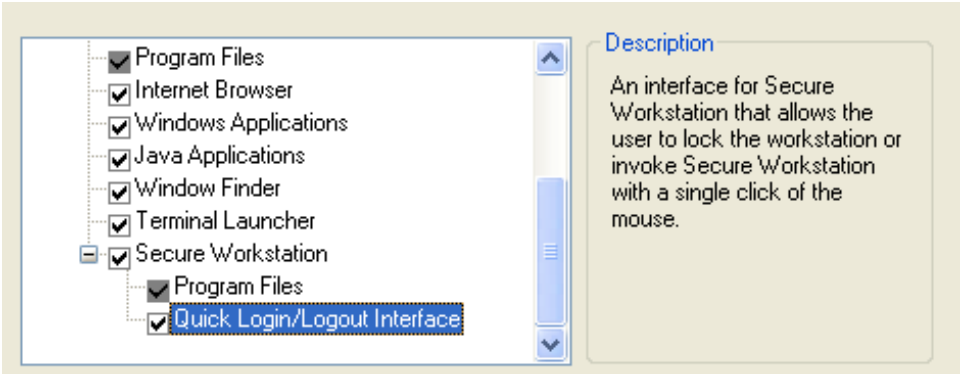
If SecureLogin is already installed, InstallShield launches the Modify, Repair, or Remove dialog box.



2 Select *Modify*, then click *Next.*

3 Check the *Secure Workstation* check box and the desired subcomponents.

Figure 8-1 *Components of Secure Workstation Component*



4 Click *Next*, then click *Finish*.

8.2.2 Installing iManager Plug-In to Secure Workstation

You administer Secure Workstation by using iManger™ and by configuring Secure Workstation settings on the workstation. For more information on installing the iManager plug-in to Secure Workstation, see Section 2.4.2, “Installing Plug-Ins for iManager,” on page 30.

8.3 Understanding Secure Workstation Policies

Three Secure Workstation policies specify how Secure Workstation behaves:

- The Local policy
- The Network policy
- The Effective policy

The Local policy is stored under an ACL-protected registry key on the workstation. The Network policy is stored in eDirectory™ and delivered to the workstation using the NMAS™ Post-Login Method. (For more information, see Section 8.6, “The Secure Workstation Post-Login Method for NMAS,” on page 112. The Effective policy is created by combining the Local policy with the Network policy.

All three policies contain the same elements. Secure Workstation always enforces the Effective policy.

Secure Workstation reads the Local policy each time a user logs in to Windows. As long as the Novell Secure Workstation Service is running, the Local policy will be in effect during each user's Windows’ session.

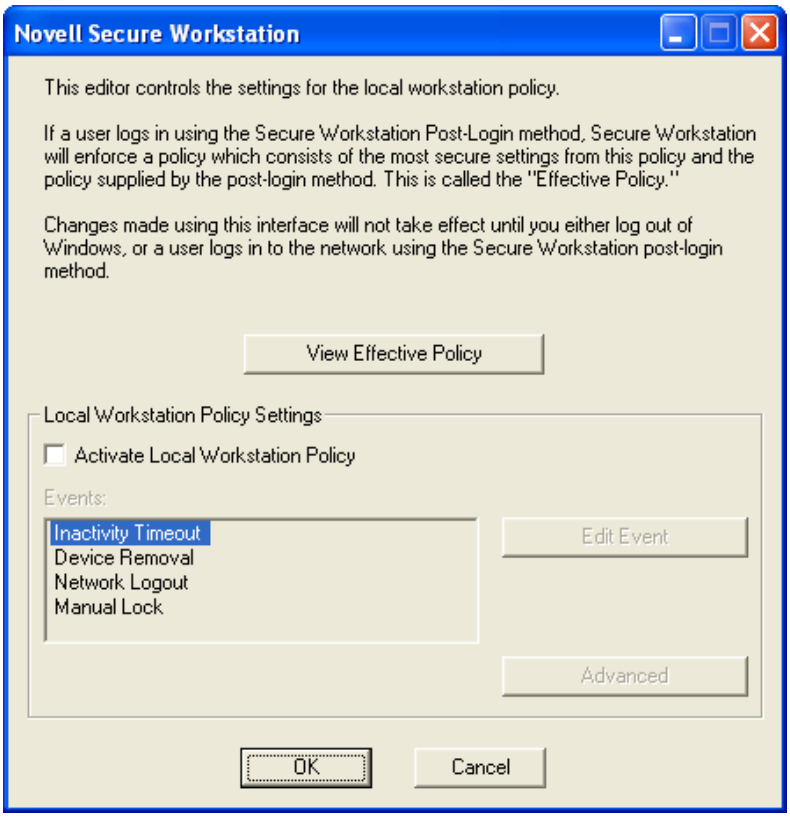
When a user logs in to the network using the Secure Workstation Post-Login Method for NMAS, the post-login method sends the Network policy to the Novell Secure Workstation Service. The service reads the Local policy and combines it with the Network policy to create the Effective policy. The Effective policy consists of the most secure settings from the Local policy and the Network policy.

If a user logs in to Windows but does not use the post-login method, the service creates the Effective policy by making a copy of the Local policy.

8.4 Local Policy Editor

The Local Policy Editor provides an easy way to edit the Local policy. To access the Editor, click *Start* > *Programs* > *Novell SecureLogin* > *Secure Workstation Policy Editor*.

The following figure illustrates the Local Policy Editor's main dialog box:



By default the Local policy is inactive, and most of the controls on the dialog box are inactive. To activate the Local policy (and all of the controls on the dialog box), check the *Activate Local Workstation Policy* check box.

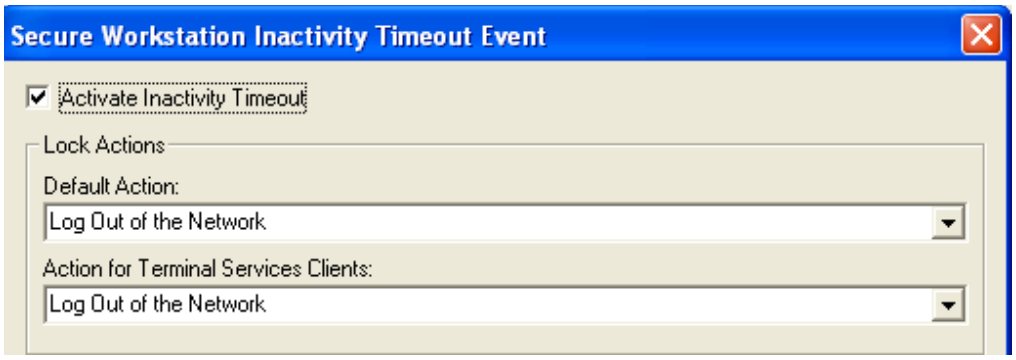
The Secure Workstation Policy enables you to specify the lock events that Secure Workstation should watch for, and what action should be taken when an event occurs. The Events list box displays a list of lock events.

You can edit settings for a specific event by selecting the event in the list box and clicking Edit Event. A dialog box is displayed with settings for the event you select. As the following figure illustrates for the Inactivity Timeout event, the dialog box for each event contains an Activate check box.

Secure Workstation ignores the event unless this box is checked.

As the following figure illustrates, the Lock Actions group box for each event contains the following:

- A drop-down list for selecting a Default Action
- A drop-down list for selecting an Action for Terminal Services Clients



The Default Action list contains the following items:

- Log Out of the Workstation

  Logs the user out of Windows.
- Log Out of the Network

  Logs the user out of either Client32™ or the LDAP Authentication Client, depending on which one has been installed.
- Close All Programs

  Closes a set of programs specified in the Advanced section of the policy.
- Close All Programs and Log Out of the Network
- Lock the Workstation

  Causes the same result as pressing Ctrl+Alt+Del, then selecting Lock Workstation.

The Action for Terminal Services Clients list contains the following items

- Log Out of the Workstation
- Log Out of the Network
- Close All Programs
- Close All Programs and Log Out of the Network
- Disconnect the Session

  Disconnects a remote terminal services session.

When a lock event is triggered, Secure Workstation takes the action associated with that event. Secure Workstation uses the default action unless the user's session is being served to a remote workstation using either Citrix* or Windows Terminal Services. Secure Workstation refers to these as Remote Sessions.

NOTE: For SecureLogin 6.0, detection of removed devices for remote sessions hasn't been implemented. Detection of removed devices works from the console but not for Citrix or Terminal Services client.

To see details about the policy that Secure Workstation is currently enforcing, click *View Effective Policy*, found on Secure Workstation's main dialog box. For information about the Effective policy, see Section 8.3, "Understanding Secure Workstation Policies," on page 102.

If you have recently started the Novell Secure Workstation service, it might not have an Effective policy yet. If so, you will get an error message when you click View Effective Policy. The service creates an Effective policy only when the user logs in to Windows, or when a user logs in using the Post-Login Method for NMAS.

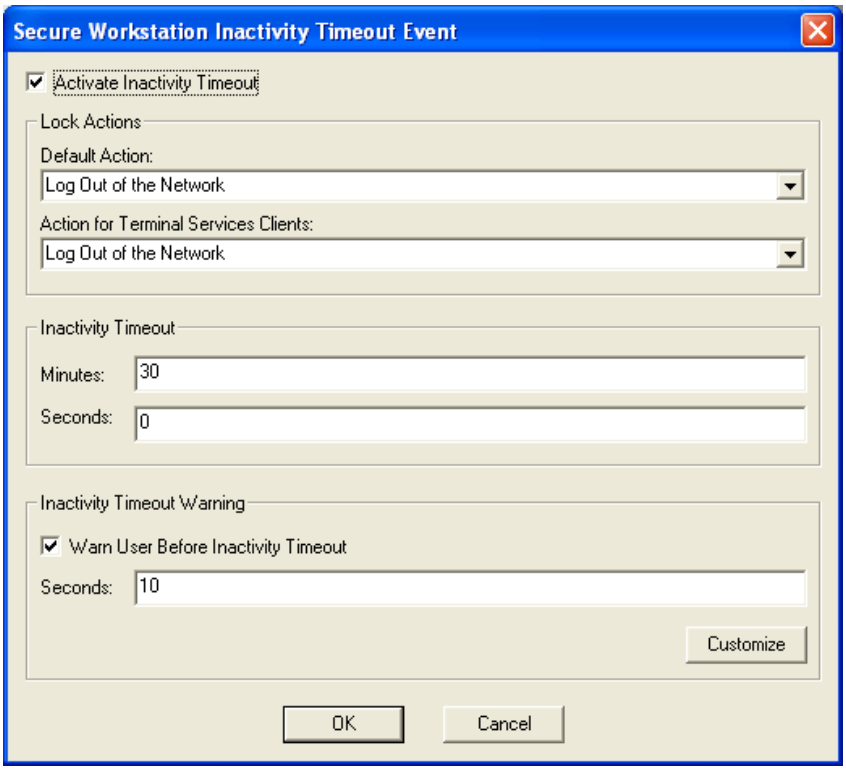
NOTE: If you are running the Local Policy Editor on a Terminal Server, the policy editor shows the Effective policy for the session that it is running in.

8.5 Configuring Secure Workstation Events

This section provides information on the following:

8.5.1 Configuring an Inactivity Timeout Event

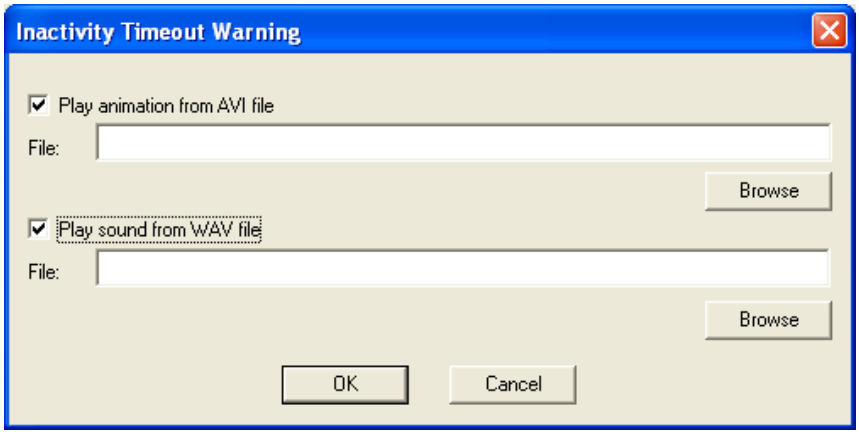
The following figure illustrates the dialog box for configuring Inactivity Timeout events:



This dialog box enables you to specify the inactivity timeout and configure a warning that is displayed just before the inactivity timeout is reached.

You can configure a .wav file that will be played when the warning is shown. You can also specify an .avi file to be played for the warning. To configure these features:

1. Click *Customize*.
2. Select an option.



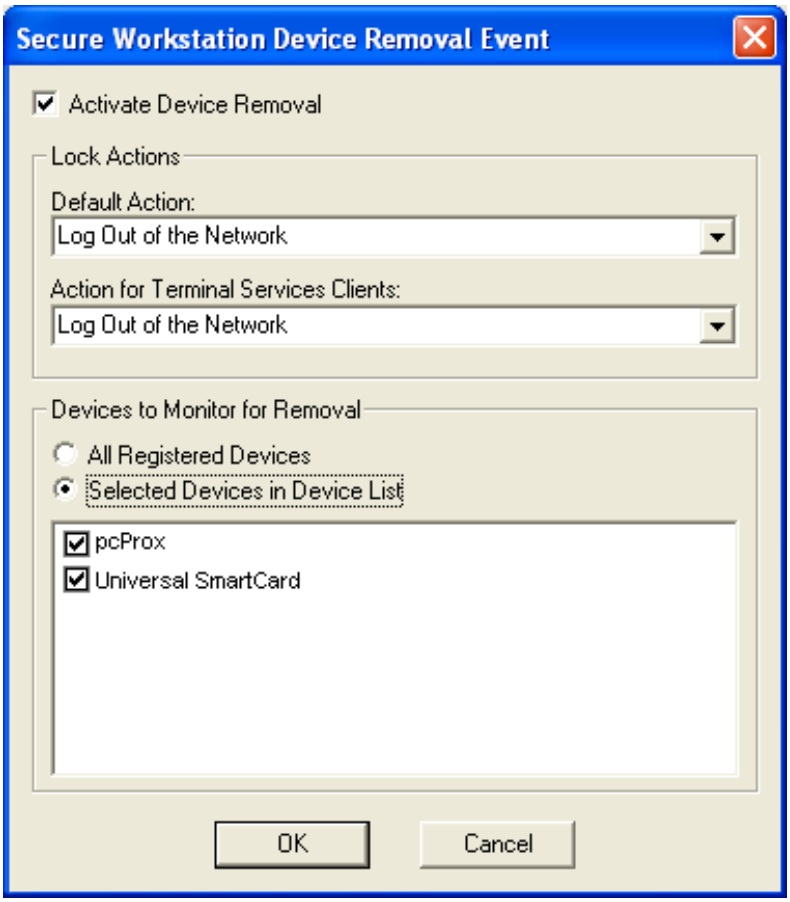
3. Browse to and select `.avi` or `.wav` files.
4. Click *OK*.

The warning message can accommodate `.avi` files that display images of any size.

The warning dialog box is displayed for the last few seconds of the inactivity timeout. You can specify the number of seconds that the warning dialog box is displayed. For example, if you set an inactivity timeout of thirty seconds and configure the warning dialog box to display for ten seconds, Secure Workstation displays the warning dialog box after twenty seconds of inactivity.

8.5.2 Configuring a Device Removal Event

The following figure illustrates the dialog box for configuring a Device Removal event.



The Devices to Monitor for Removal section contains a list of devices that are registered with the Secure Workstation.

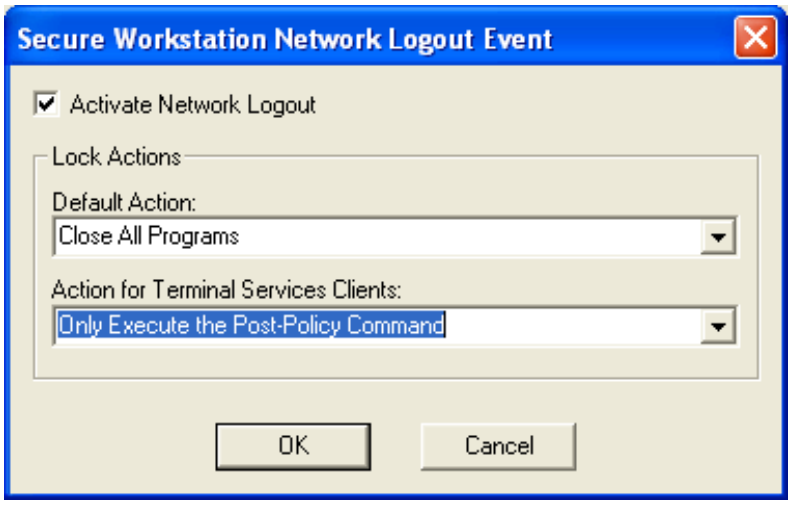
This dialog box enables you to specify which devices are included in the policy. If a device is included in the policy, it must be present during the user's session. If a device in the list is not present, Secure Workstation executes the lock action.

For SecureLogin 6.0, both the Universal Smart Card and pcProx Methods for NMAS can report device removal events to Secure Workstation.

Other NMAS partners have also implemented devices that can report device removal events to Secure Workstation. If you want to use a device that does not show up in the list, make sure that you have installed the NMAS Login Client Method for the device. If the device still doesn’t show up, check with the vendor of the device to ensure that it will work with Secure Workstation.

8.5.3 Configuring a Network Logout Event

The following figure illustrates a Network Logout event:



A Network Logout event is triggered when a user logs out of the network. This event could be triggered by either Client32 or the LDAP Authentication Client, depending on which client is present.

One of the intended uses of the Network Logout event is to close programs that the user might have used for single sign-on through Novell SecureLogin. This event might also be used to display a login dialog box or run a script when the user logs out. For more information, see Section 8.5.6, “The Post-Policy Command,” on page 112.

This event has a different set of lock actions than the other events. The Default Action list contains the following actions:

- Log Out of the Workstation
- Close all programs
- Only Execute the Post-Policy Command

The Action for Terminal Services Clients list contains the following actions:

- Log Out of the Workstation
- Close All Programs
- Disconnect the Session
- Only Execute the Post-Policy Command

The Default Action list doesn’t include the following actions:

- Lock the Workstation

  This action has been omitted because of the behavior of the GINA. If a network connection isn’t present when the workstation is locked, the Client32 GINA won’t allow the workstation to be unlocked with an eDirectory authentication.
- Log Out of the Network

This action has been omitted because it doesn't make sense to log out of the network in response to a network logout event.

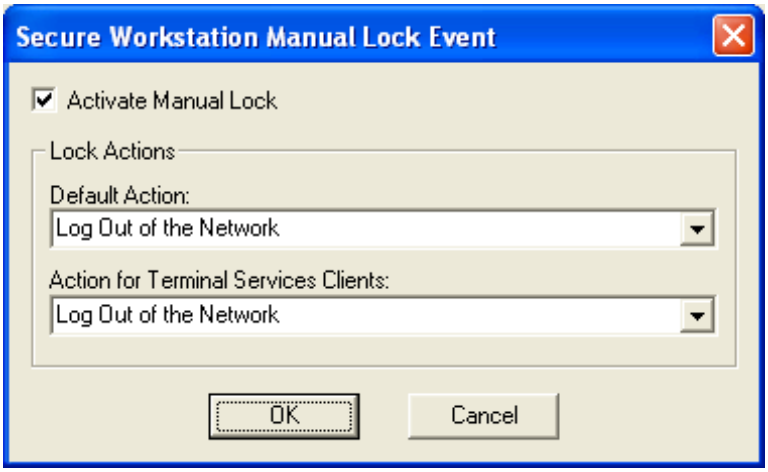
The Network Logout event is the only event that includes the Only Execute the Post-Policy Command action. This action is actually a substitute for the Log Out of the Network action that is available with other events. If you want to execute a Post-Policy Command on network logout, but not do anything else, use this action.

You can use the Post-Policy Command to display a login dialog box or run a script. For more information, see Section 8.5.6, "The Post-Policy Command," on page 112.

8.5.4 Configuring the Manual Lock Event

The Manual Lock event gives users the ability to manually trigger Secure Workstation. A user can manually trigger Secure Workstation either by clicking the Logoff button on the Quick Logon/ Logoff Interface or by executing `SWLock.exe` in the System32 directory.

The following figure illustrates the Manual Lock dialog box.



To configure Manual Lock:

1. Select *Manual Lock* from the main page, then click *Edit Event*.
2. Check the *Activate Manual Lock* check box.

3 (Optional) Select an option from the *Default Action* drop-down list.

4 (Optional) Select an option from the *Action for Terminal Services Clients*.

8.5.5 Advanced Settings

The following figure illustrates the Advanced Settings dialog box.

To configure advanced settings, click *Advanced* on Secure Workstation's main dialog box.

Terminating Applications

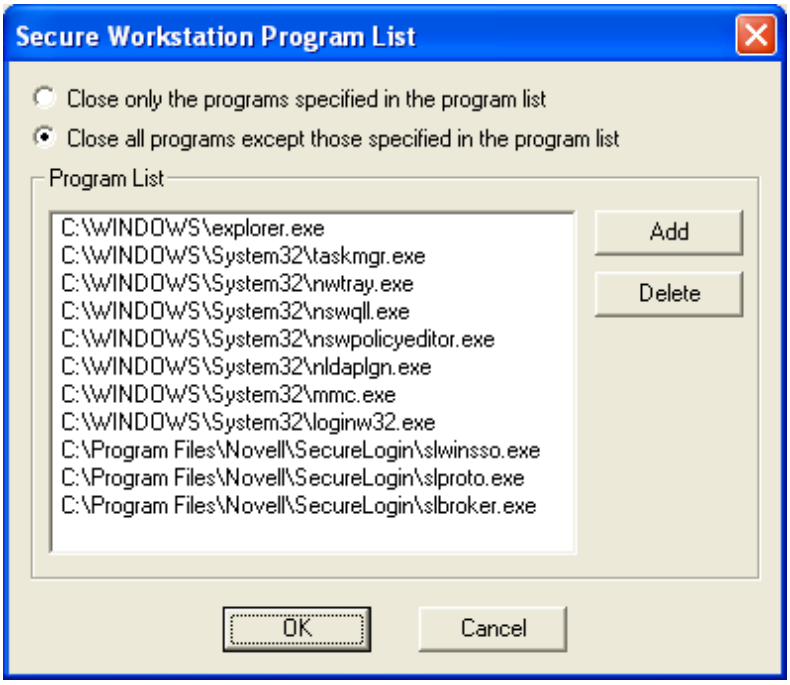
The Force Termination of Non-Responding Applications When Logging Out of Windows check box affects the way that programs will be shut down when Secure Workstation logs a user out of Windows. If this box is checked, Windows terminates programs that don't respond to a "close" message in a timely manner. This setting logs the user out of Windows more quickly, but some programs might not get an opportunity to save their data before being terminated.

The Wait Before Starting to Terminate Applications When Closing All Programs check box is similar, except that it controls the behavior of the Close All Programs action. When Secure Workstation closes programs, it always sends a Close message to each program to tell it to shut down. If the Wait Before Starting to Terminate Applications When Closing All Programs check box isn't checked, Secure Workstation does nothing else to close the programs. The result is that some programs might not shut down.

For example, if Microsoft Word* has an unsaved document, Secure Workstation might display a *Save As* dialog box.

On the other hand, if the W*ait Before Starting to Terminate Applications When Closing All Programs* check box is checked, Secure Workstation checks to see if the programs are still running after the specified timeout. Any programs that are still running at this point are terminated and might not have a chance to save their data.

The following figure illustrates the dialog box that displays when Secure Workstation closes programs:



You can use the Program List to specify which programs should be closed when Secure Workstation executes a Close All Programs action. If you select *Close Only the Programs Specified in the Program List*, Secure Workstation closes only the programs listed.

If you select *Close All Programs Except Those Specified in the Program List*, Secure Workstation closes all programs except those specifically listed.

NOTE: If you select *Close All Programs Except Those Specified in the Program List*, SecureLogin closes every program in the user's sessions except those listed. This closing includes `explorer.exe`, the process associated with the user's desktop.

Secure Workstation closes only the programs that the currently logged in Windows user has sufficient rights to close on his own. Programs that the user does not have rights to (such as a service running as the LocalSystem account) aren't closed.

When Secure Workstation is running on a Terminal Server, only the programs in the current user's session are closed. Programs running in other users' sessions aren't affected.

You don't need to specify the full path and name of each program in the program list. For example, instead of adding `c:\winnt\system32\notepad.exe` to the list, you could just add `Notepad.exe`.

However, if you don't specify the full path, the entry will correspond to all programs with that name, regardless of their path. For instance, listing Notepad.exe in the list without the path would match both `c:\winnt\system32\notepad.exe`, and `c:\documents and settings\user\notepad.exe`.

You can also use environment variables in the program list. For example, you could specify `%systemroot%\System32\notepad.exe` instead of `c:\winnt\system32\notepad.exe`.

8.5.6 The Post-Policy Command

The Post-Policy Command is a command that is executed after Secure Workstation executes the lock action. This feature was designed to display a login dialog box after a Close All Programs or Log Out of the Network action has been executed. However, you can use this feature to run any program or script. You must provide the full path and name of the program to run.

To display the login dialog box, use `loginw32.exe` for Client32. Use `nldaplgn.exe` for the LDAP Authentication Client. Both programs are located in the system32 directory.

If you have configured the Network Logout event, Secure Workstation restarts the program specified in the Post-Policy Command if it terminates before a user is logged in. This allows the login dialog box to be displayed again if a user clicks *Cancel*.

8.6 The Secure Workstation Post-Login Method for NMAS

You can use the Secure Workstation Post-Login Method for NMAS to deliver a Network policy to Secure Workstation. The Network policy is stored in eDirectory. You can use iManager to configure the policy. The Network policy contains the same items as the Local policy

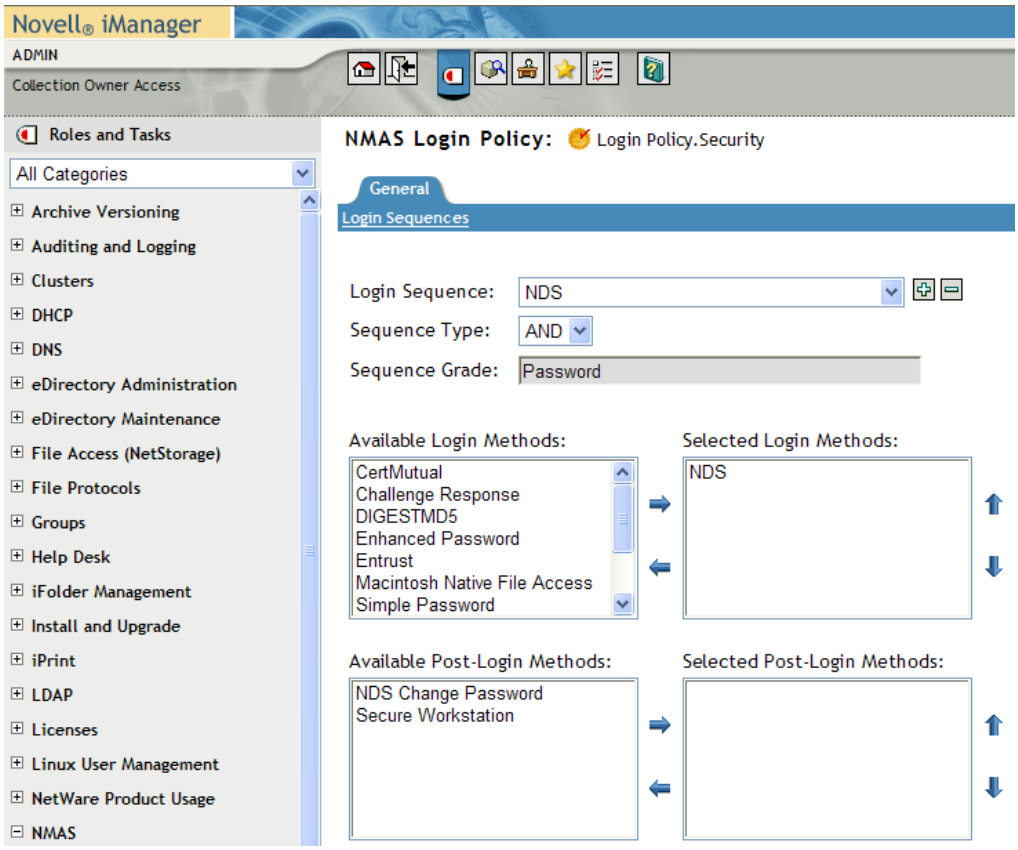
1. Install the Post-Login Method by using iManager or the NMAS Method Installer.

   To use the NMAS Method Installer, run *methodinstaller.exe*, found in the *nmas\nmasmethods* directory on the Novell SecureLogin 6.0 software image or CD.

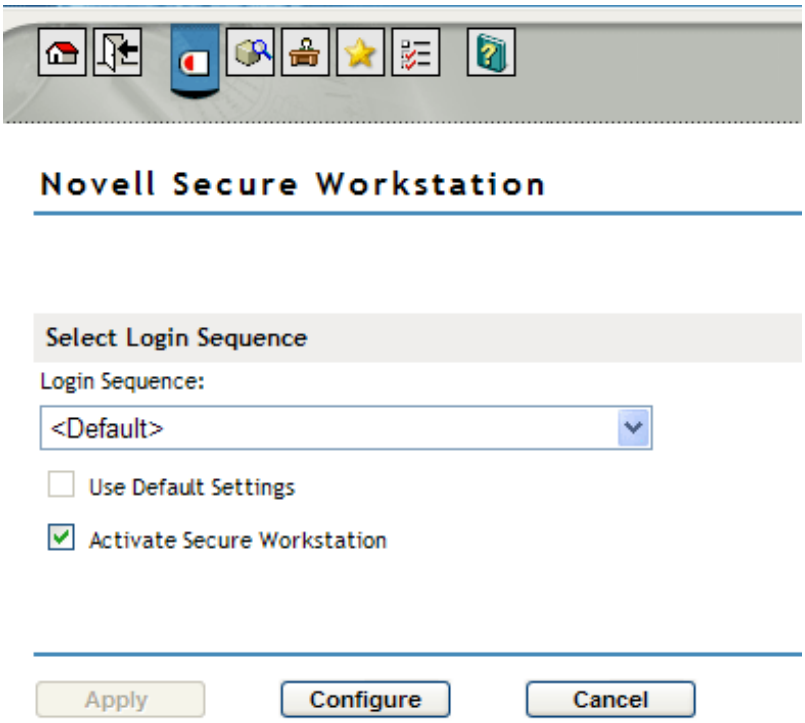
   You must have at least one NMAS Server, and you must have the NMAS Client installed on your system with Secure Workstation. The Post-Login Method will run on NetWare, Windows, Linux, Solaris, and AIX servers.

   The Post-Login Method is located on the SecureLogin 6.0 image or CD in the *\securelogin\nmas\nmasmethods* directory. For instructions on installing a login method, refer to the NMAS documentation.
2. Create at least one NMAS Login Sequence that includes Secure Workstation.

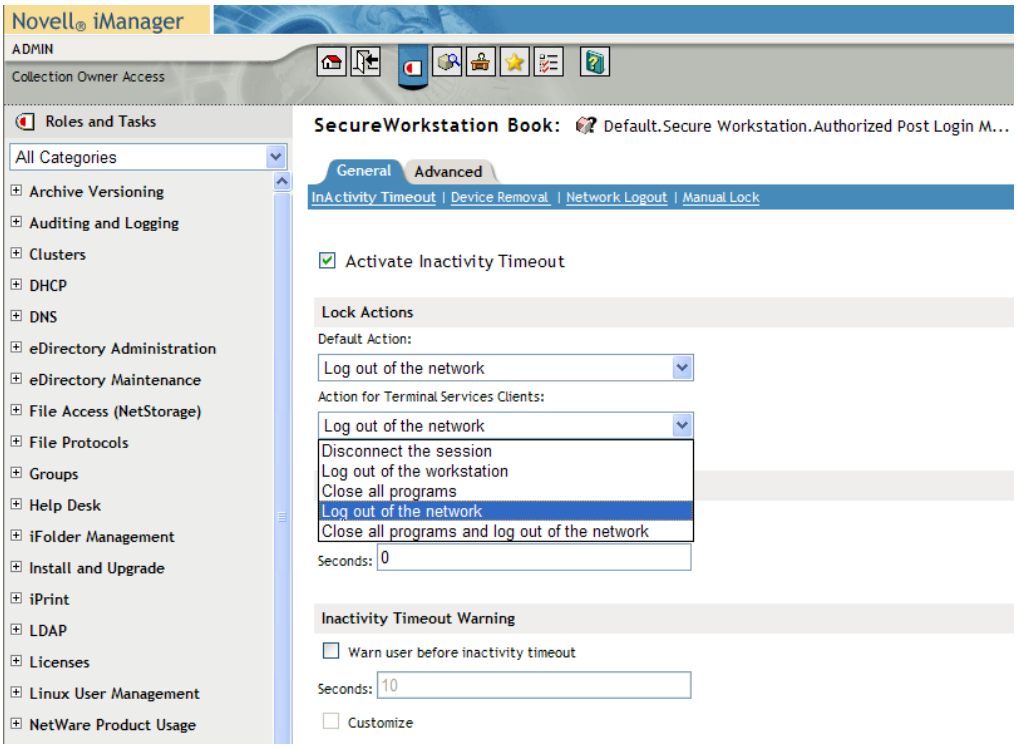
Using iManager, select *NMAS* > *NMAS Login Sequences*. The following page will be displayed:



3 Using iManager, select *Novell Secure Workstation* > *Select Sequence*.The Novell Secure Workstation page will be displayed.



4 You can either select Use Default Settings and click Apply or select Activate Secure Workstation and click Configure. The following dialog box is displayed:



For information on the pcProx and other post-login methods, see User Identification Plug-ins in the Novell Modular Authentication Services Administration Guide (http://www.novell.com/documentation/nmas23/index.html)

The Login Sequence list will be populated with each login sequence that contains the Secure Workstation method. You can configure a different policy for each sequence that contains the Secure Workstation method. The policy associated with the [Default] sequence will be applied to any sequence that contains the Secure Workstation method but does not yet have a Network policy configured.

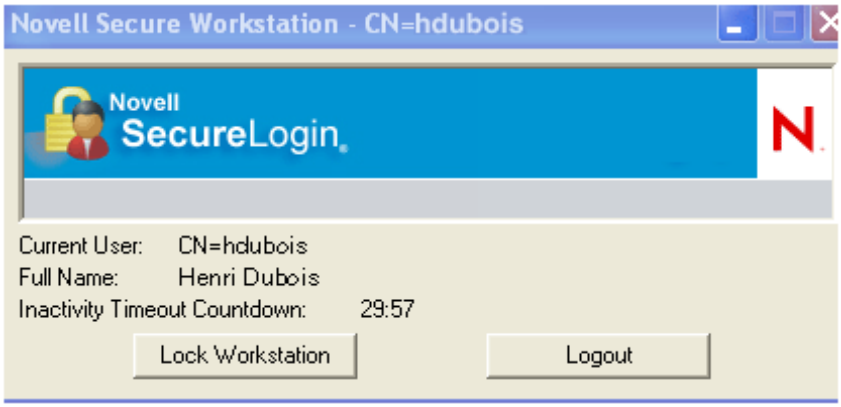
NOTE: You can create as many login sequences that contain the Secure Workstation method as you need. Also, you can associate a different policy with each sequence and then associate each sequence with a different set of users. For information on configuring login sequence restrictions and configuring a user's default login sequence, see the NMAS Administration Guide (http://www.novell.com/documentation/nmas23/index.html).

The iManager interface for configuring the Network policy is similar to the Local Policy Editor. For more information on the options available when configuring a Secure Workstation Policy, see Section 8.4, “Local Policy Editor,” on page 102.

8.7 Quick Login/Logout

Quick Login/Logout provides an easy way for users to see who is logged in to a workstation. It also provides a convenient way for a user to lock or log out of the workstation when leaving a work area. QuickLogin/Logout is probably most useful for kiosks or shared workstations.

The following figure illustrates Quick Login/Logout’s dialog box



By default, Quick Login/Logout shows the following:

- The user ID of the currently logged in user
- The user's full name
- The amount of time remaining before a Secure Workstation inactivity timeout

8.7.1 Using the Lock Workstation Button

To lock the workstation, click Lock Workstation. Clicking this button does the same thing as pressing Ctrl+Alt+Del, then selecting Lock Workstation.

This feature is most useful when used with the LDAP Authentication Client. A user who plans to leave a public workstation for only a few minutes can elect to lock the workstation so that the user's programs continue running. However, this prevents other users from using the workstation.

For this reason, a feature has been implemented in the LDAP Authentication Client that allows a different user to unlock the workstation. If a different user logs in, the following happens:

- The previous user is logged out.
- Secure Workstation receives a Network Logout Event and takes the action associated with that event in the policy

If the action associated with the Network Logout Event is Close All Programs, the previous user's programs are closed when the workstation is unlocked.

By default the LDAP Authentication Client allows only the user who is currently logged in to unlock the workstation. For information on how to change this behavior, see the LDAP Authentication Client documentation.

NOTE: Quick Login/Logout is visible even when the workstation is locked, but the Lock Workstation and Logout buttons aren't visible.

Scenario: Locking the Workstation. Sandy is a network administrator and Gudrun is a nurse at the VMPClinic. Nurses at a nursing station frequently need to interrupt their data entry to check on patients.

Gudrun logs in to the shared workstation, opens DataQuick to view patient data, then opens RediLog to update a report. Before she has completed her tasks, however, she is summoned to a patient's room. Planning to be gone from the workstation for just two minutes, Gudrun doesn't want to log out. Instead, she clicks Lock Workstation and leaves to check on a patient. Returning, Gudrun unlocks the workstation and continues using DataQuick and RediLog.

Only Gudrun or a network administrator is able to unlock the workstation.

Scenario: Unlocking a Locked Workstation. Sandy changes a registry setting in the LDAP Authentication Client so that a workstation in the General Services section doesn't remain locked for long periods of time. The setting enables other users to use the locked workstation. Sandy also selects the Network Logout event, then selects Close All Programs from the Default Action drop-down list.

Peter had been using the workstation but has been gone for some time. The workstation is locked. Sofia needs to use it. She logs in, a process that logs Peter out of the network. Secure Workstation detects the logout event and closes all programs. Sofia authenticates to the network and uses the workstation.

8.7.2 Using the Logout Button

When you click Logout, the Quick Login/Logout Interface sends a Manual Lock signal to Secure Workstation. Secure Workstation executes the action associated with the Manual Lock Event in the policy, then executes the Post-Policy Command.

The following figure illustrates actions that you can set from the Default Actions drop-down list:

If the action for the Manual Lock Event is Close All Programs and Log Out of the Network, and the Post-Policy Command has been configured to launch the login dialog (either *loginw32.exe* or *nldaplgn.exe*), Secure Workstation does the following, all within a matter of seconds:

- Closes the current user's programs.
- Logs the user out of the network.
- Displays a login dialog for the next user.

NOTE: The speed at which Secure Workstation closes programs depends on several factors. For more information, see "Terminating Applications" on page 110.

Scenario: Sharing a Workstation. Nurses at VMP Clinic share a workstation at a nursing station. As administrator, Sandy wants one nurse to be able to log off quickly and another nurse to be able to log in quickly. Sandy selects Close all Programs and Log Out of the Network as the default Manual Lock action. In addition, Sandy configures the Post-Policy command to launch the login dialog box.

Gudrun logs in to the workstation, opens DataQuick to check patient data, opens RediLog to update a report, completes her tasks, then clicks *Logout*. Secure Workstation closes DataQuick and RediLog, logs Gudrun out of the network, then displays the login dialog box. The workstation is ready for the next nurse.

8.7.3 Details about Policy Enforcement

The behavior of Secure Workstation depends on the settings in the Effective policy. The policy includes the following:

- A set of events that Secure Workstation listens for
- A set of actions that will be taken when one of those events occurs.

After Secure Workstation detects an event, the user is considered to be out of compliance with the policy. This means that the user has, for example, exceeded an inactivity time limit or removed an authentication device, such as a smart card. Unless one of the actions is Log Out of the Workstation or Lock the Workstation, Secure Workstation continues to execute the action associated with the events in the policy that are out of compliance.

Scenario: Removing a Proximity Card. The Effective policy contains a Device Removal Event that requires a pcProx proximity card. The action associated with this event is Close All Programs. Secure Workstation is set up to close all programs specified in the policy when the card is removed.

Claire attempts to restart one of those programs without replacing the proximity card. Secure Workstation immediately closes the program. Secure Workstation continues to execute the action associated with the Device Removal Event until the user is in compliance with the event.

This behavior is the same for all of the Secure Workstation events. If you don't want users to have the ability to run certain programs without being authenticated to the network, configure a Network Logout Event that closes those programs.

You can use the Post-Login Method to provide Secure Workstation with a new effective policy.

Scenario: A New Effective Policy. Claire leaves and takes her proximity card. Secure Workstation closes her programs and continues closing them until her proximity card has been replaced. Markus approaches the workstation and presents his proximity card. Secure Workstation continues to close the programs specified in the policy.

The programs are closed because Secure Workstation requires Claire’s proximity card to be present, because Secure Workstation detected Claire’s card when Secure Workstation generated the Effective policy that it is currently enforcing. However, Markus can log in using the Post-Login Method, which causes Secure Workstation to refresh its policy. Secure Workstation now requires Markus’ proximity card to be present instead of Claire’s card.

You can use the Post-Login Method to provide Secure Workstation with a new effective policy.