

Novell Nsure™ SecureLogin

3.51.2

www.novell.com

INSTALLATION GUIDE

April 08, 2005



Novell®

Legal Notices

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

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

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

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

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

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

www.novell.com

Nsure SecureLogin 3.51.2 Installation Guide

April 08, 2005

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

Novell Trademarks

Client32 is a trademark of Novell, Inc.

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

eDirectory is a trademark of Novell, Inc.

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

NMAS (Novell Modular Authentication Services) is a trademark of Novell, Inc.

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

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

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

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

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

Nsure is a 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** **7**

- 1 Overview** **9**
 - Supported Platforms 9
 - Servers 9
 - Browsers 10
 - Workstations 10
 - Deploying SecureLogin 10
 - Installing Java 10
 - Selecting Modify, Repair, or Remove 11
 - Using a Silent Install 12
 - Automating the Installation 13
 - Installing SecureLogin on Servers 15
 - SecureLogin on Windows and NT Servers 15
 - SecureLogin and SecretStore in NetWare Environments 15
 - Some Tips Concerning Workstations 15

- 2 Installing in Novell eDirectory Environments** **17**
 - Extending the eDirectory Schema 17
 - If You Plan to Use the SecretStore Client 18
 - Installing SecureLogin: eDirectory 19
 - Using the Custom Option for Novell eDirectory 22
 - Installing Administrative Tools for eDirectory 22
 - Installing ConsoleOne 23
 - Installing the SecureLogin Snap-In to ConsoleOne 23

- 3 Installing in LDAP Environments** **25**
 - LDAP with eDirectory 25
 - Preparing for an LDAP Directory 25
 - Installing SecureLogin: LDAP with eDirectory 27
 - LDAP without eDirectory 32
 - Using the Custom Option for LDAP without eDirectory 34
 - Granting Rights 36
 - Installing Administrative Tools for LDAP 36
 - Configuration Issues 37
 - Using LDAP on eDirectory 37
 - Using LDAP on Non-eDirectory Environments 37
 - Using Contextless Login 39

- 4 Installing in Active Directory Environments** **41**
 - Preparing Active Directory 41
 - Prerequisites 41
 - Preparing to Extend the Active Directory Schema 41
 - Extending the Active Directory Management Schema 42
 - Assigning User Rights 44
 - Replicating Six Attributes 46

Installing SecureLogin: Active Directory	47
Using the Custom Option for Active Directory	48
Setting the Default Domain Policy	50
Installing Management Tools for Active Directory	51
5 Installing in Windows NT/2000 Domains	53
Installing SecureLogin: Microsoft NT/2000 Domains	53
Using the Custom Option: SecureLogin in NT/2000 Domains	54
Using Administrative Tools	55
6 SecureLogin on a Standalone Workstation	57
Installing SecureLogin: Standalone Workstations	57
Using the Custom Option for Standalone Workstations	58
7 Upgrading from Earlier Versions	59
Upgrading Entirely to SecureLogin 3.51.2	59
Upgrading from Novell SecureLogin 2.5	59
Upgrading from Novell SecureLogin 3.0.x	59
Running SecureLogin 3.51.2 in Mixed Environments	60
Upgrading to SecureLogin 3.51.2	60
Managing Mixed Environments	61
8 Installing and Configuring Secure Workstation	63
Overview	63
Setting Up Secure Workstation	64
Installing Secure Workstation	64
Installing the ConsoleOne Snap-In to Secure Workstation	65
Understanding Secure Workstation Policies	65
The Local Policy Editor	66
Configuring Secure Workstation Events	68
Configuring an Inactivity Timeout Event	68
Configuring a Device Removal Event	70
Configuring a Network Logout Event	70
Configuring the Manual Lock Event	72
Advanced Settings	72
Terminating Applications	73
The Post-Policy Command	75
The Secure Workstation Post-Login Method for NMAS	75
Quick Login/Logout	77
Using the Lock Workstation Button	78
Using the Logout Button	79
Details about Policy Enforcement	80
9 Troubleshooting	81
Can't Find a Server	81
Verifying the eDirectory Schema	81
Verifying the LDAP Directory Schema	84
Verifying the Active Directory Schema	87
If ?sysuser(system) and ?syspassword(system) Are Unavailable	90
Useful TIDs	90
A Lotus Notes	93
Migrating Lotus Notes	93

About This Guide

The *SecureLogin Installation Guide* is for network administrators. It provides information on the following:

- ◆ Chapter 1, “Overview,” on page 9
- ◆ Chapter 2, “Installing in Novell eDirectory Environments,” on page 17
- ◆ Chapter 3, “Installing in LDAP Environments,” on page 25
- ◆ Chapter 4, “Installing in Active Directory Environments,” on page 41
- ◆ Chapter 5, “Installing in Windows NT/2000 Domains,” on page 53
- ◆ Chapter 6, “SecureLogin on a Standalone Workstation,” on page 57
- ◆ Chapter 7, “Upgrading from Earlier Versions,” on page 59
- ◆ Chapter 8, “Installing and Configuring Secure Workstation,” on page 63
- ◆ Chapter 9, “Troubleshooting,” on page 81

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.

User Comments

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

Documentation Updates

For the most recent version of this document, see Novell SecureLogin 3.51.2 on the [Novell documentation Web site](http://www.novell.com/documentation) (<http://www.novell.com/documentation>).

Additional Documentation

This *Guide* is part of a documentation set for SecureLogin 3.51.2. Other documents include the following:

- ◆ The Help systems in SecureLogin on the desktop as well as SecureLogin snap-ins to ConsoleOne[®] or Microsoft* Management Console.
- ◆ The **Nsure SecureLogin 3.51.2 Administration Guide** (tools and tasks to manage SecureLogin and configure terminal emulators)
- ◆ The **Nsure SecureLogin 3.51.2 Scripting Guide** (concepts concerning scripting, scripting commands, and example scripts for applications)
- ◆ The **Nsure SecureLogin 3.51.2 Terminal Services Guide** (configuring Citrix servers)
- ◆ The **Nsure SecureLogin 3.51.2 Configuration Guide for Terminal Emulation** (how to configure Terminal Launcher for selected terminal emulators)
- ◆ The **Nsure SecureLogin 3.51.2 User Guide** (using SecureLogin to enable applications for single sign-on)

If you are running Novell[®] SecretStore[®] in your environment, make sure that you upgrade SecretStore on your server before installing SecureLogin. For documentation on SecretStore, see the *SecretStore 3.3.3 Administration Guide* (<http://www.novell.com/documentation/secretstore33/index.html>).

1

Overview

This section provides information on the following:

- ◆ “Supported Platforms” on page 9
- ◆ “Deploying SecureLogin” on page 10
- ◆ “Installing SecureLogin on Servers” on page 15
- ◆ “Some Tips Concerning Workstations” on page 15

Supported Platforms

Novell[®] SecureLogin 3.51.2 supports the following platforms. The latest support packs are recommended for all platforms.

Servers

- ◆ NetWare[®] 5.1 or later with Novell eDirectory[™] 8.6.2 or later
- ◆ Novell eDirectory on NetWare, Windows* NT*, Windows 2000, or Linux*

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

eDirectory Version Running on Linux	Version of SecretStore to Use
eDirectory 8.6.2	SecretStore 3.0.5
eDirectory 8.7.0	Not supported. Upgrade to eDirectory 8.7.1.
eDirectory 8.7.1 or later	SecretStore 3.3.3 or later

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

SecureLogin 3.51.2 for eDirectory supports only ConsoleOne[®] 1.3.2 or later.

- ◆ Microsoft* Windows 2000 Server, Terminal Server, or Advanced Server with Active Directory*
- ◆ Microsoft Windows NT4 Domains
- ◆ Microsoft Windows NT4 Terminal Server
- ◆ Microsoft Windows 2003 Server or Terminal Server with Active Directory
- ◆ Servers running LDAP-compliant directories

Browsers

- ◆ Internet Explorer 5.5 or later
- ◆ Netscape* 4.7.x

SecureLogin 3.51.2 provides legacy support, but with less functionality than provided for Internet Explorer.

Depending on workstation configurations, the browsers might behave differently.

Workstations

- ◆ Windows 98 SE

If SecureLogin is to access eDirectory over NetWare Core Protocols™, Windows 98 workstations should have Novell Client™ 3.33 or later. If you use LDAP, the Novell client isn't required.

- ◆ Windows NT 4.0 with SP6
- ◆ Windows 2000 Professional

Windows 2000 workstations using NetWare Core Protocols must have Novell Client 4.83 or later.

- ◆ Windows XP

SecureLogin supports the default Windows shell, explorer.exe.

The SecureLogin snap-in to ConsoleOne requires ConsoleOne 1.3.2 or later.

Deploying SecureLogin

WARNING: The SecureLogin installation program overwrites the tlaunch.ini file. If you have enabled any terminal emulator applications for single sign-on, copy tlaunch.ini from the active directory (for example, Program Files\novell\securelogin) to a safe directory before upgrading or reinstalling SecureLogin. After upgrading or installing, copy the saved tlaunch.ini file back to the original file.

This section provides information on the following:

- ◆ “Installing Java” on page 10
- ◆ “Using a Silent Install” on page 12
- ◆ “Automating the Installation” on page 13

If you want to enable Java applications for single sign-on, refer to this section. Otherwise, skip it.

Installing Java

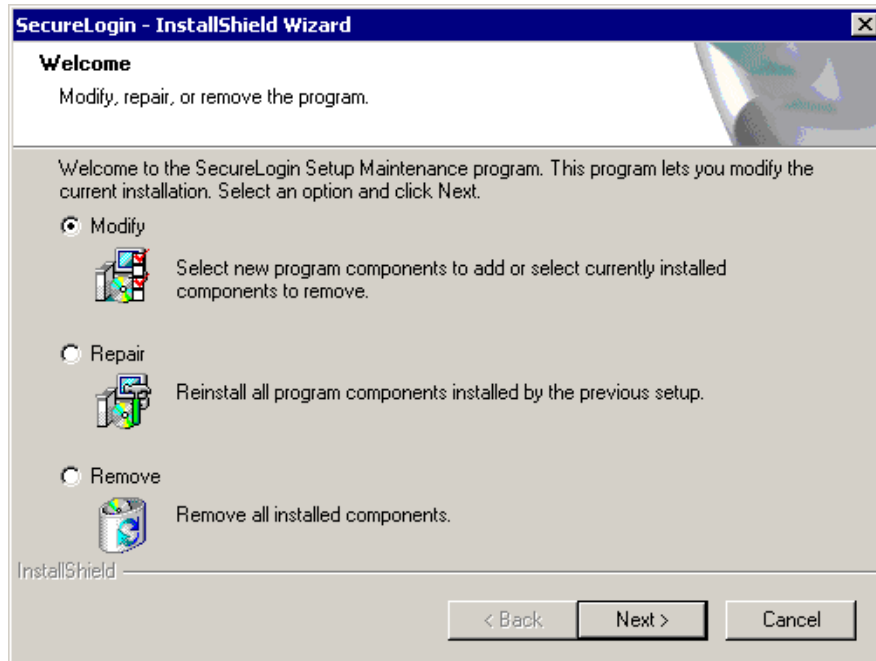
SecureLogin 3.51.2 supports Java applications. However, during installation the Java Applications component is displayed and available only if Java is installed on your workstation. If the Java Runtime Environment is not installed on your workstation, download and install it. To find out whether the Java Runtime Environment is installed on a workstation, use Add/Remove Programs in the Control Panel.

- 1** Go to the [Java download Web page \(http://www.java.com/en/index.jsp\)](http://www.java.com/en/index.jsp).
- 2** Click Free Download, then click Yes to install and run the Java plug-in.

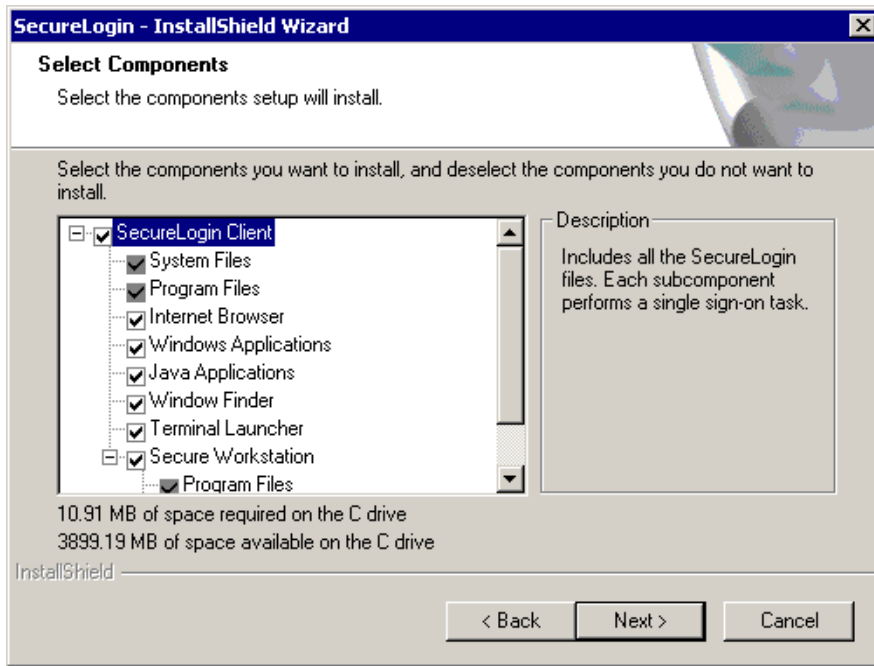
- 3 Click Yes to install and run jinstallerx.exe.
- 4 Accept the license agreement, select a setup type, then click Next.
- 5 Click Finish, then restart your workstation.

Selecting Modify, Repair, or Remove

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



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.

To reinstall components, you select Repair. The installation program detects previously installed components and reinstalls them.

Using a Silent Install

A silent install provides InstallShield* with instructions for installing SecureLogin. To use a silent install, 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 same environment that the silent installation will run.

Do this before you create a response file. You need to be familiar with the installation process and options, so that you don't capture unnecessary data or missteps in the response 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 98 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.

- 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 `-fl` 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.

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

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

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.

- 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 -s -fl"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 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`.

Also, you can 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.

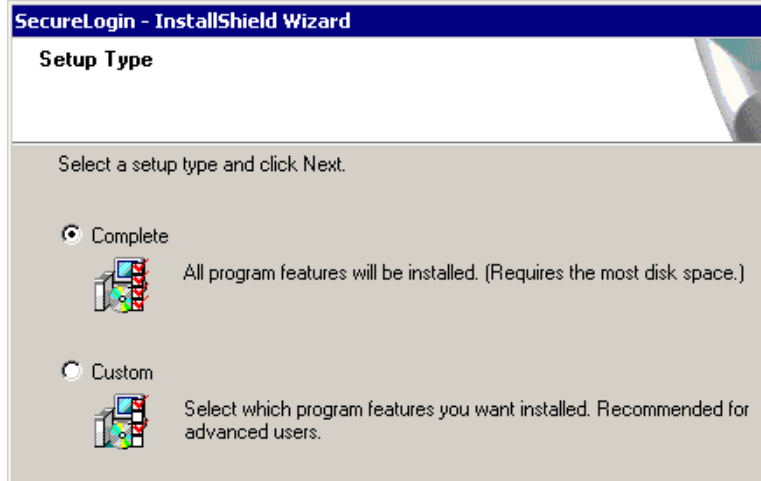
Automating the Installation

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

3 Make changes.

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

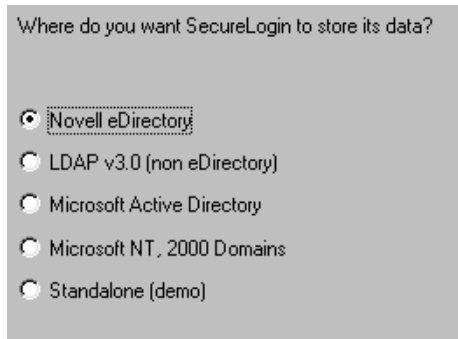


The [SetupType] section in automate.ini determines whether the dialog box appears:

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

By default, the dialog box displays. If you uncomment the ShowDialog line, the dialog box doesn't 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:



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

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

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

- 4 Save and exit.

Installing SecureLogin on Servers

SecureLogin on Windows and NT Servers

You can install SecureLogin on a Windows NT or Windows 2000 server.

In fact, to administer SecureLogin in an Active Directory or NT Domain environment, you must install SecureLogin on an NT or 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.

SecureLogin and SecretStore in NetWare Environments

You don't install SecureLogin on a NetWare server. Instead, you install SecureLogin and snap-ins to ConsoleOne on workstations. To administer SecureLogin, you use an administrative tool on the desktop, ConsoleOne in eDirectory environments, or the Microsoft Management Console in Active Directory 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 install SecretStore server components on a NetWare server and then install the SecretStore client on workstations.

You install SecretStore server components before installing SecureLogin on a workstation. You install the SecretStore client while installing SecureLogin on a workstation. Also, make sure that the current primary tree and server connections are set to the tree where the SecretStore service has been installed. For information on installing SecretStore, see "Installing SecretStore" in the *SecretStore 3.3.3 Administration Guide* (<http://www.novell.com/documentation/secretstore33/index.html>).

Some Tips Concerning Workstations

SecureLogin does not support workstations running Windows 95 or 98 in Active Directory and NT Domain environments.

For Windows 95/98 and Windows XP Pro workstations using NetWare Core Protocols, install the latest Novell client.

NICI

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

- ♦ eDirectory LDAP platform

- ◆ A non-eDirectory LDAP platform
- ◆ The SecretStore Client feature
- ◆ The NMAS™ Client feature

You don't need to install NICI separately. If NICI isn't already installed on your workstation, the installation program automatically installs it. If you have an earlier version of NICI, the installation program detects it and then updates to the later version.

The path to the NICI installation is in the automate.ini file. You can turn off the NICI autolaunch by commenting out the paths for NICI.

NMAS

When you install SecureLogin, the Novell Modular Authentication Service (NMAS) can be installed as well. After NMAS is installed, the Novell Client changes. The password field disappears.

If you uninstall SecureLogin, NMAS isn't uninstalled.

To turn off the NMAS autolaunch, comment out the paths for NMAS in the automate.ini file.

NOTE: You do not have the option to install NMAS in a silent install of SecureLogin.

2

Installing in Novell eDirectory Environments

This section provides information on the following:

- ◆ “Extending the eDirectory Schema” on page 17
- ◆ “Installing SecureLogin: eDirectory” on page 19
- ◆ “Installing Administrative Tools for eDirectory” on page 23

WARNING: If you are upgrading and are using SecretStore, upgrade SecretStore on your server to version 3.3.2 before installing SecureLogin 3.51.2. Otherwise, secrets might be lost.

Extending the eDirectory Schema

So that SecureLogin can save users’ single sign-on information, the Novell® eDirectory™ schema must be extended. Ndsschema.exe extends the eDirectory schema and grants rights to existing users so that they can use SecureLogin.

The SecureLogin snap-in to ConsoleOne® automatically grants rights to objects that you create after you run ndsschema.exe. Therefore, you don’t need to run ndsschema.exe again. You only extend the eDirectory tree schema once for SecureLogin.

IMPORTANT: If you create objects by using ConsoleOne on a workstation that doesn’t have the SecureLogin snap-in, those objects won’t receive rights.

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

IMPORTANT: Don’t run ndsschema.exe from a Windows 98 workstation. SecureLogin doesn’t support doing this.

1 Run ndsschema.exe.

This file is available on your workstation after you run nsl351.exe from the CD or download. Typically, this file is in the c:\securelogin\tools directory. However, if you unzipped 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

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:

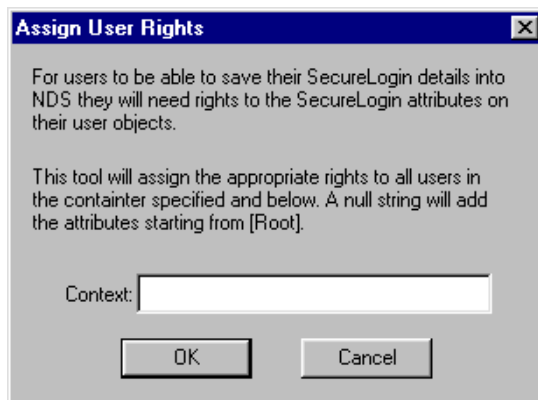
- ◆ Prot:SSO Auth
- ◆ Prot:SSO Entry
- ◆ Prot:SSO Entry Checksum
- ◆ Prot:SSO Profile
- ◆ Prot:SSO Security Prefs

- ◆ Prot:SSO Security Prefs Checksum

For information on these attributes, see “[Extending the Active Directory Schema](#)” on page 44.

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

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.

Rights on Container objects are inherited. These rights flow to subdirectories, 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 NT, 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:\program files\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).

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 on workstations.

To find out 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 3.3.0 Novell SecretStore`).

You can also use ConsoleOne. If SecretStore is installed, the SecretStore object displays in the Security container.

If SecretStore isn't 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.

If you are upgrading and are using SecretStore, upgrade SecretStore on your server to version 3.3.2 or later.

WARNING: If you don't upgrade SecretStore on your server, secrets might be lost.

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

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.

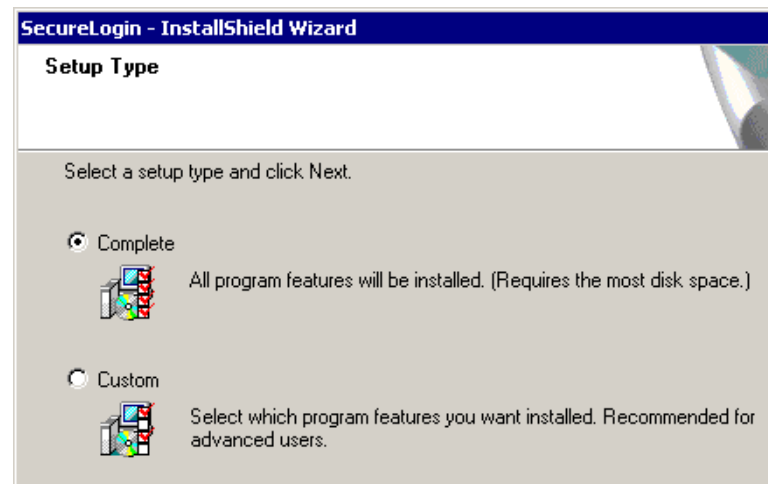
- 1 Make sure that you are authenticated to an eDirectory tree.

In Step 5 below, you select an installation option. If you are authenticated to an eDirectory tree and select to install SecureLogin along with SecretStore, installation proceeds as expected. If you are not authenticated, the following scenario occurs.

Scenario: Unusable Login Prompt. You are not authenticated to an eDirectory tree. You select to install the SecureLogin client along with SecretStore. During the installation, you select default settings. The installation program prompts you for a username and password. However, the username field cannot be edited, and no password has been set.

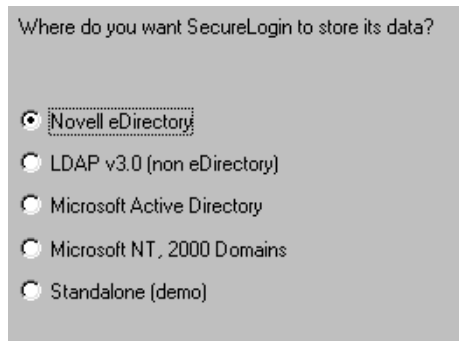
Until you authenticate to eDirectory and set a passphrase or password, SecureLogin continues to display this "unusable" prompt each time that SecureLogin is started.

- 2 Run setup.exe, found in the securelogin\client directory.
- 3 Select a language, click Next twice, then accept the license agreement.
- 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, see “Using the Custom Option for Novell eDirectory” on page 22.

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



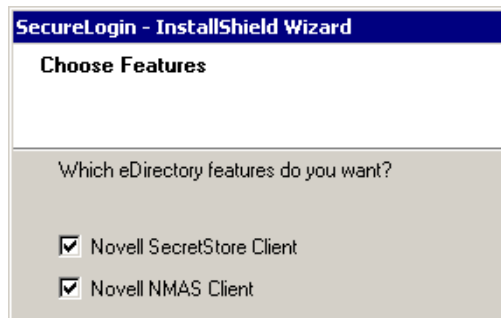
- 6 Select Novell Client for Windows or LDAP, then click Next.



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



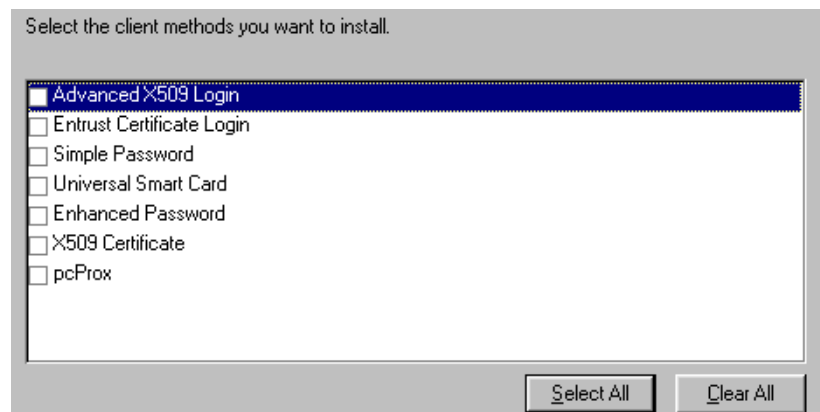
IMPORTANT: Select Novell SecretStore only if SecretStore is installed on a server. For information on SecretStore, see the [SecretStore 3.3.3 Administration Guide \(http://www.novell.com/documentation/secretstore33/index.html\)](http://www.novell.com/documentation/secretstore33/index.html).

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

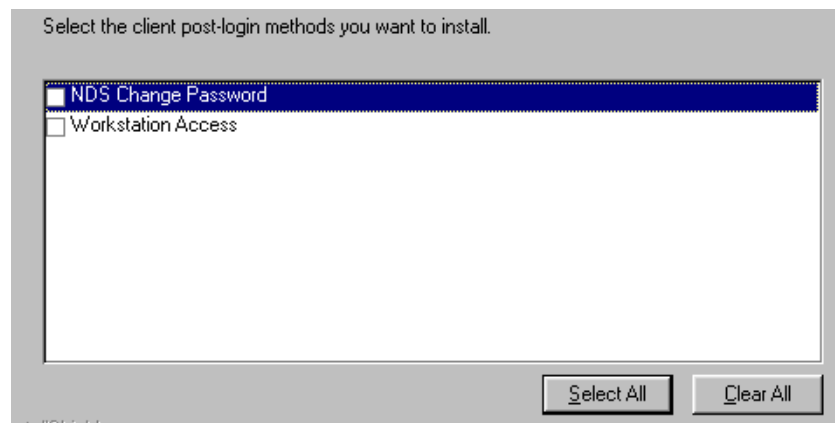
However, if you install the SecretStore client and then later run the install program and deselect the SecretStore client, you will cause problems to the directory cache. All the credential sets that are stored in SecretStore will be unavailable to the eDirectory client. Nevertheless, as long as the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

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

- 8** Click Install.
- 9** (Conditional) If you selected the NMAS client, select one or more NMAS login methods, then click Next.



- 10** (Conditional) If you selected the NMAS client (for example, for a Windows 98 installation), select post-login methods, then click Next.



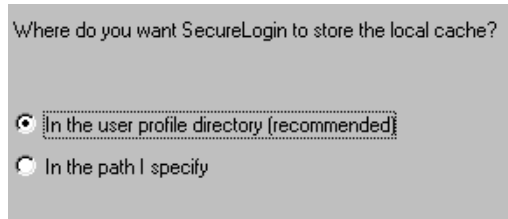
The NDS Change Password option enables you to change your eDirectory password during a login session without using the eDirectory password to log in.

- 11** Click Finish, click Yes, then click OK to restart your workstation.

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 are in the following locations:

Platform	The User Profile Directory
Windows 98	In c:\windows if profiles are disabled. In c:\windows\profiles if profiles are enabled.
Windows NT	In c:\winnt\profiles
Windows 2000/XP	In Documents and Settings\ <i>username</i>

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.

For more information on Terminal Launcher, see [“Working with Terminal Emulators”](#) in the [Nsure SecureLogin 3.51.2 Administration Guide](#).

Installing Administrative Tools for eDirectory

Administrative tools include the following:

- ◆ ConsoleOne
See [“Installing ConsoleOne”](#) on page 23.
- ◆ The SecureLogin snap-in to ConsoleOne
See [“Installing the SecureLogin Snap-In to ConsoleOne”](#) on page 23.

- ◆ Ndschema.exe

You don't actually install ndschema.exe. You run it to extend the NDS or eDirectory schema and to grant rights. See [“Extending the eDirectory Schema” on page 17](#).

- ◆ Loginwatch.exe

For information on Loginwatch.exe, see [“Using Login Watcher” in the Nsure SecureLogin 3.51.2 Administration Guide](#).

Installing ConsoleOne

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

To install ConsoleOne on the workstation, run c1.exe, available from <http://download.novell.com/filedist/pages/PublicSearch.jsp>.

Installing the SecureLogin Snap-In to ConsoleOne

- 1 Run nslsnapin.exe, found in the \consoleone\snapins directory on the SecureLogin 3.51.2 CD or software image.

- 2 Extract files.

To view or manage SecureLogin in ConsoleOne, you must unzip or extract ConsoleOne and the snap-in to ConsoleOne to the same directory. Typically, files are unzipped to the following directories:

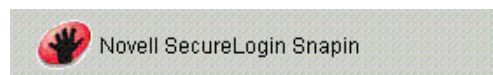
- ◆ c:\novell\consoleone\1.2 on the workstation
- ◆ sys:\public\consoleone\1.2 on the NetWare server

For the snap-in to ConsoleOne to work on a workstation, you must have the following:

- ◆ ConsoleOne running on the workstation
- ◆ SecureLogin running on the workstation
- ◆ eDirectory with the NetWare Core Protocol

You can determine whether the snap-in is installed:

- 1 Bring up ConsoleOne.
- 2 Click Help > About Snapins.
- 3 Look for the SecureLogin Snapin entry.



If it is present, the snap-in is installed.

3

Installing in LDAP Environments

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

SecureLogin LDAP servers do not require the Novell® Client™. However, LDAP does not provide drive mappings or connections to file servers or print servers.

SecureLogin 3.51.2 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:

- ♦ “LDAP with eDirectory” on page 25
- ♦ “LDAP without eDirectory” on page 32
- ♦ “Granting Rights” on page 37
- ♦ “Installing Administrative Tools for LDAP” on page 37

LDAP with eDirectory

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

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 via LDAP must have a simple password assigned to them. Otherwise, the users will be prompted to log in more than once.

Preparing for an LDAP Directory

Extending the eDirectory Schema

If you are installing on workstations that use Novell® eDirectory™, Novell SecretStore®, or Novell Client32™, do the following:

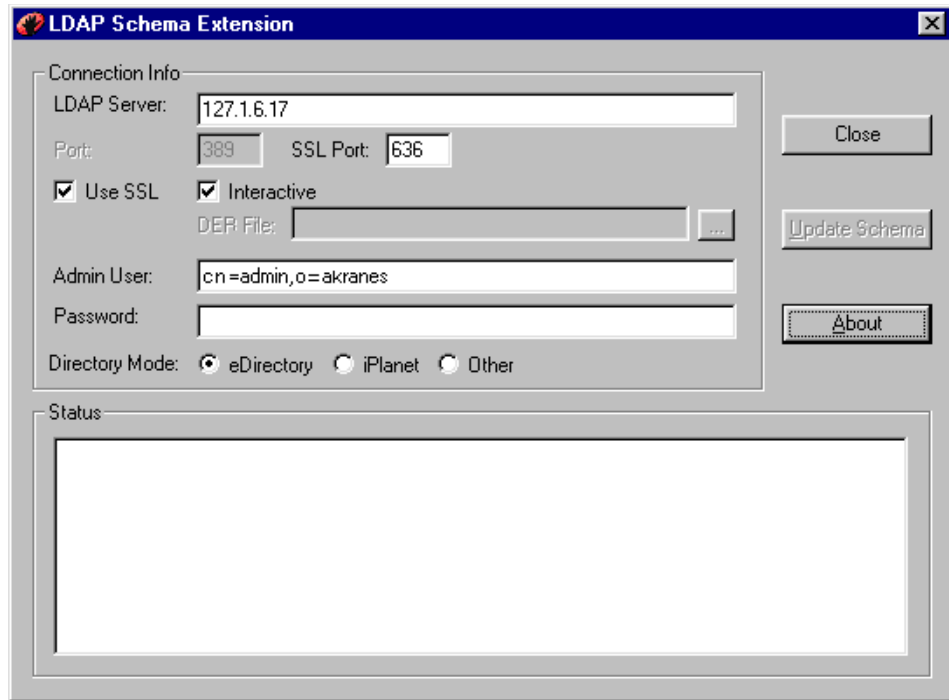
- 1** On an administrative workstation, log in as administrator.
- 2** Extend the eDirectory schema by running `ndsschema.exe`.

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

Typically, `ndsschema.exe` is found in the `c:\securelogin\tools` directory. This directory is available on your workstation after you run `nsl351.exe` from the CD or download. However, if you unzipped 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:

Extending the LDAP Directory Schema

- 1 Run ldapschema, 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 user that you logged 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.

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 IP 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, you or the user can provide this information during installation.

Installing SecureLogin: LDAP with eDirectory

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

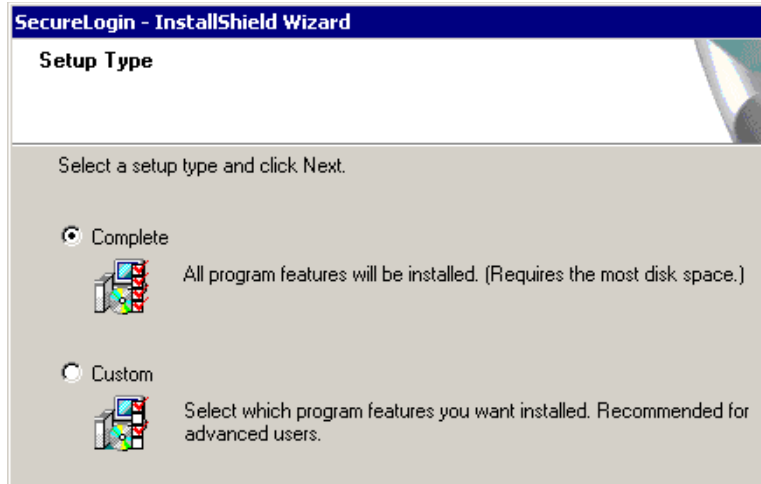
You can install SecureLogin on a Windows NT/2000 server and on workstations. No SecureLogin components are installed on a NetWare[®] server.

You can specify more than one LDAP server for the SecureLogin installation. Although the dialog boxes in the installation program only allow 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.

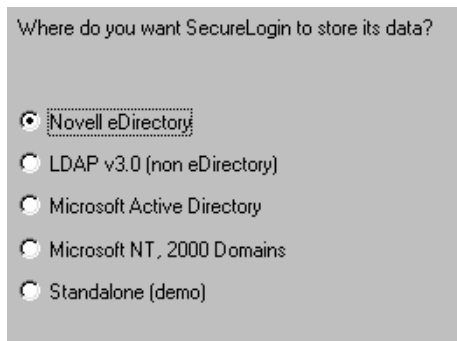
To install the LDAP option:

- 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.

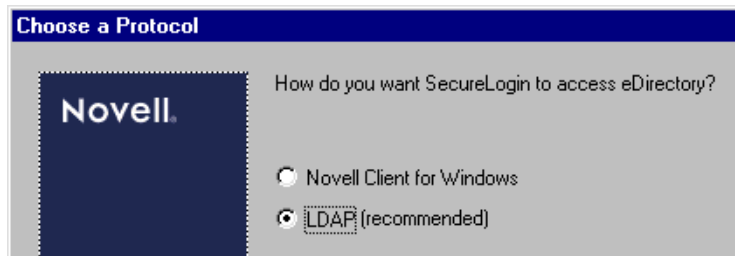


The Complete option uses default values and installs SecureLogin in c:\program files\novell\securelogin. For options available through the Custom option, see [“Using the Custom Option for LDAP on eDirectory” on page 30.](#)

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



- 5 Click the LDAP option.



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).

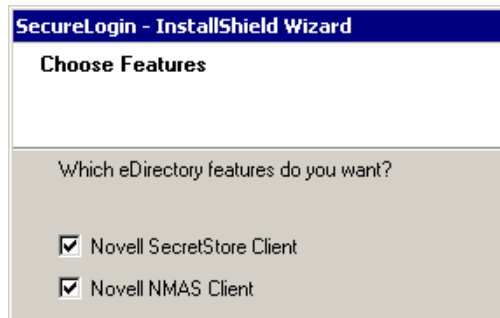
NOTE: The above screen is displayed only if you have Novell Client for Windows installed on your machine. Otherwise, LDAP is auto-selected as the protocol.

- 6 (Conditional) For Windows NT, 2000, XP, or 2003 servers and workstations, select when to log in to LDAP, then click Next.



If the workstation is not running Novell Client software, the When Logging In to Windows option is also provided. This option enables you to log in when GINA starts.

- 7 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 \(http://www.novell.com/documentation/secretstore33/index.html\)](http://www.novell.com/documentation/secretstore33/index.html).

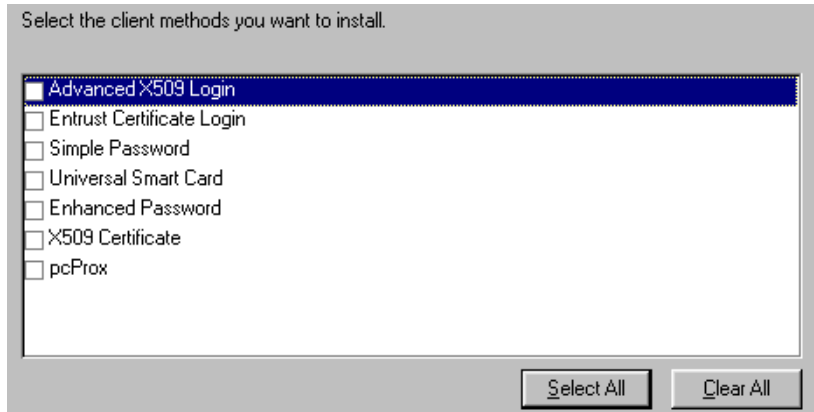
The Novell SecretStore option installs the SecretStore client, which provides additional security. If you deselect this option and want to install it later, you must uninstall SecureLogin, then run the SecureLogin installation again.

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 or configuration data.

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.

- 8 Click Install.
- 9 (Conditional) If you selected the NMAS client, select one or more NMAS login methods, then click Next.



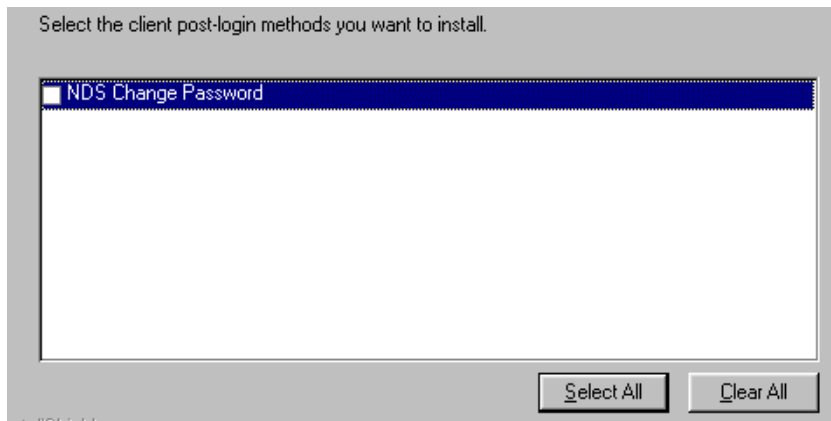
When you use LDAP on eDirectory, the LDAP password can come from one of two places:

- ◆ The eDirectory password
- ◆ The NMAS simple password

The eDirectory password 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. If you do not want a user to have a simple password, use ConsoleOne to remove it from the NMAS options.

- 10** (Conditional) If you selected the NMAS client, select post-login methods, then click Next.

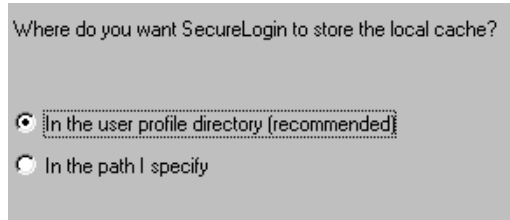


- 11** Click Finish, click Yes, then click OK to restart the computer.

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.

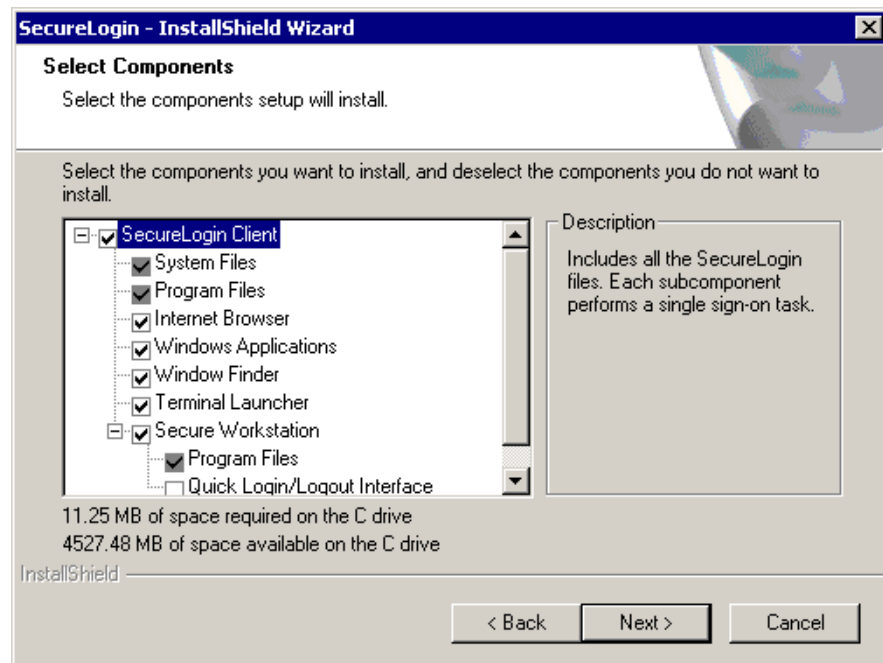


The user profile directory is the default path.

User profiles are in the following locations:

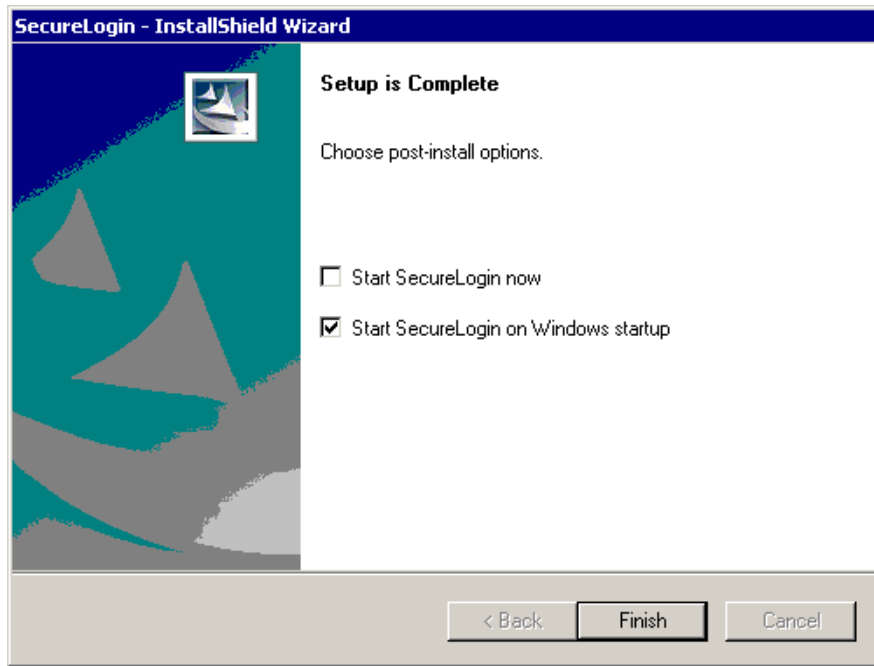
Platform	The User Profile Directory
Windows 98	In c:\windows if profiles are disabled. In c:\windows\profiles if profiles are enabled.
Windows NT	In c:\winnt\profiles
Windows 2000/XP	In Documents and Settings\ <i>username</i>

- ◆ Select SecureLogin components.



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

- ◆ Select options as to when SecureLogin will start.



If the Start SecureLogin Now check box is checked, SecureLogin will be started after the installation, unless you are prompted to restart your workstation.

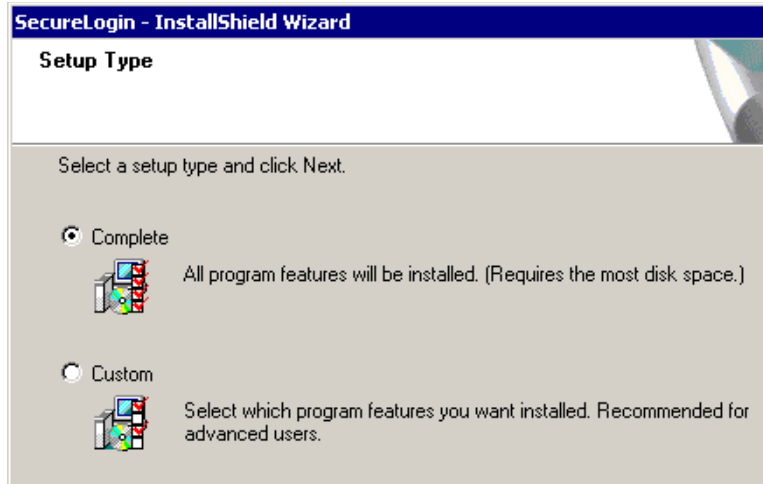
If you check the Start SecureLogin On Windows Startup check box, Windows places the SecureLogin icon on the system tray. You can then access SecureLogin from the system tray or from Start > Programs > Novell SecureLogin > Novell SecureLogin.

LDAP without eDirectory

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

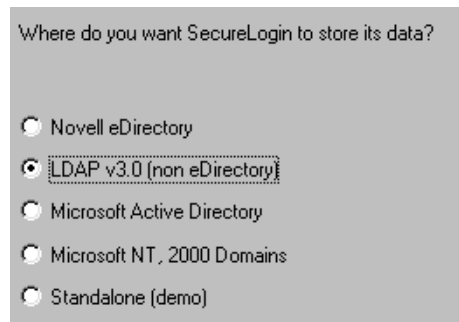
You can specify more than one LDAP server for the SecureLogin installation. Although the dialog boxes in the installation program only allow you to specify one LDAP server, you can specify additional servers by modifying the automate.ini file.

- 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 [“Using the Custom Option for LDAP on eDirectory” on page 30.](#)

- 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 Application mode.

IMPORTANT: LDAP in Application mode is not intended for workstations with multiple people using the same local Windows account (for example, in kiosks). Doing this can cause users to log in as the previous user when SecureLogin is terminated incorrectly.

If the workstation is running Novell Client software, the Application mode option is not available. This option enables you to log in when GINA starts.

- 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.

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:

- ◆ Specify a folder where SecureLogin will be installed.
The default is c:\Program Files\novell\securelogin.
- ◆ Specify whether to associate your Windows username with your LDAP distinguished name.



- ◆ Specify an LDAP server address and port.



The name (ldapauthserver) that appears in the Address text box is a placeholder name. Type a server name or IP address. If you type a name that cannot be found (for example, the name does not exist or the server is unavailable), the login will slow down significantly.

IMPORTANT: If you type a name that cannot be found (for example, the named server does not exist or is unavailable), the login will slow down significantly as LDAP tries to locate the named server. If the server name is in the DNS, LDAP quickly locates the server.

- ◆ Specify a path for SecureLogin’s local cache.

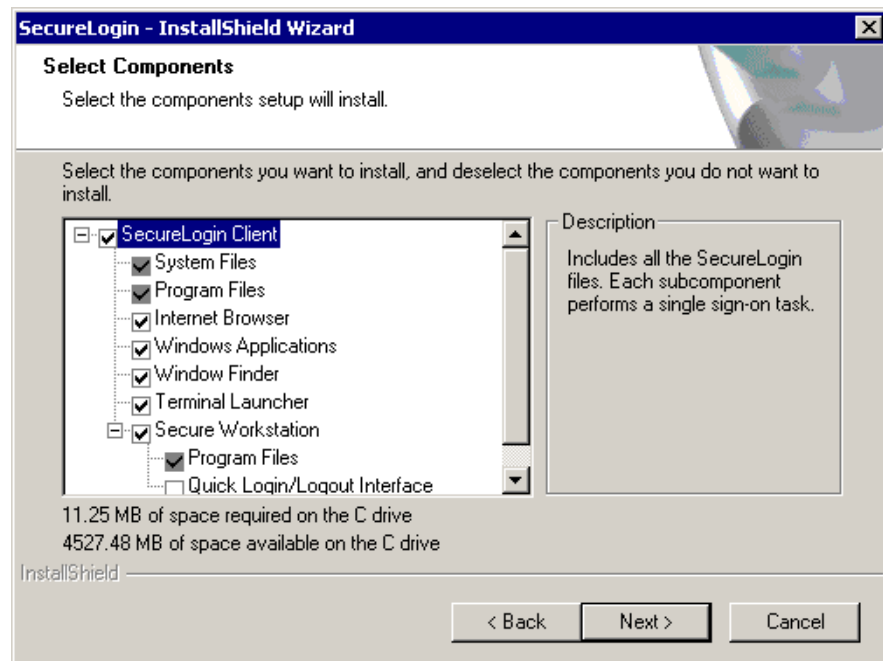


The user profile directory is the default path.

User profiles are in the following locations:

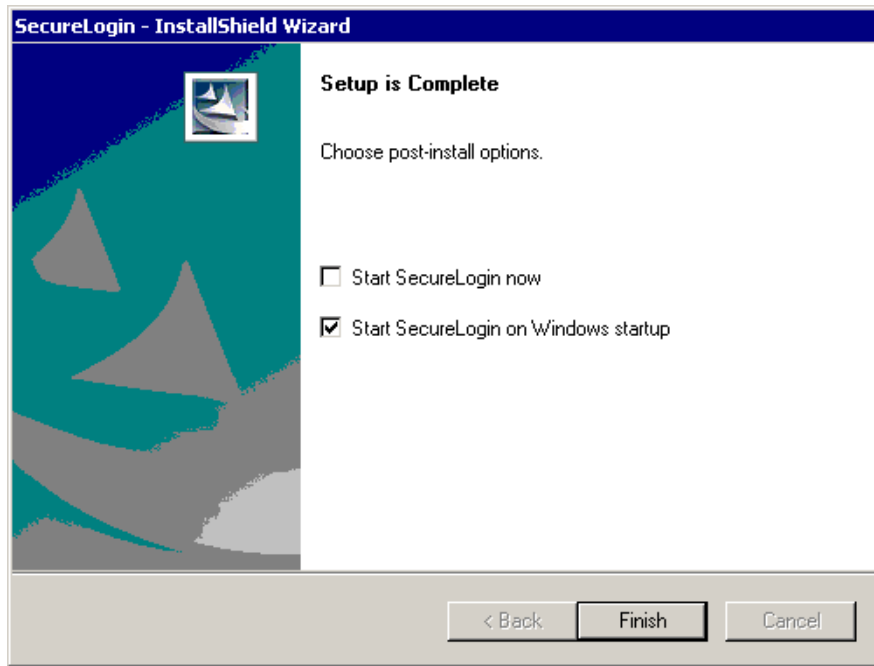
Platform	The User Profile Directory
Windows 98	In c:\windows directory if profiles are disabled. In c:\windows\profiles if profiles are enabled.
Windows NT	In c:\winnt\profiles
Windows 2000/XP	In Documents and Settings\ <i>username</i>

- ◆ Select SecureLogin components.



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

- ◆ Select options for starting SecureLogin.



If the Start SecureLogin Now check box is checked, you do not need to restart your workstation. If the box is not checked, you need to reboot.

If the Start SecureLogin Now check box is not checked but you check it, you will be prompted to restart your workstation, even if you do not want to.

If you check the Start SecureLogin On Windows Startup check box, SecureLogin starts immediately after you log in to Windows.

Granting Rights

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

Users on Windows NT, 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\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.

- ◆ 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).

Installing Administrative Tools for LDAP

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

IMPORTANT: If you administer SecureLogin from a SecureLogin client workstation that has SecureLogin installed in LDAP mode, changes made in ConsoleOne will not be saved.

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

To use ConsoleOne[®] and the SecureLogin snap-in to manage LDAP, see “[Installing the SecureLogin Snap-In to ConsoleOne](#)” on page 23.

The snap-in to ConsoleOne enables you to define an LDAP password policy. However, the snap-in doesn't enforce that policy unless the LDAP schema has been extended.

If the SecretStore client is installed on your workstation, install and use the SecretStore snap-in (`sssnapin.exe`) to ConsoleOne. This file is found in the `\securelogin\consoleone\snapins` directory.

Configuration Issues

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. If you do not want a user to have a simple password, use ConsoleOne to remove the simple password.

Using LDAP on Non-eDirectory Environments

Configuring the Server

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).

For more details, refer to the respective section of the documentation for the directory servers you use.

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.

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

Table 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 26](#).

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 [“Extending the Active Directory Management Schema” on page 42](#).

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.b64
CerttFilePath	REG_SZ	C:\ad_cert.b64

For server certificate file details, refer to [“Retrieving the Certificate” on page 38](#).

Using Contextless Login

If you configure a workstation to use the LDAP GINA as the primary authentication, the LDAP GINA launches a login dialog box, which requires a user DN and password. The LDAP Authentication client provides a contextless login. This feature enables you to type part of your DN.

For example, Henri Dubois' DN is `cn=hdubois,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 inserts Henri's entire DN into the dialog box.

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.

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

- 1** (Conditional) If the Novell Client is installed on the workstation, remove it.
- 2** During the SecureLogin installation, select the LDAP option and the When Logging In to Windows option.

4

Installing in Active Directory Environments

This section contains information on the following:

- ◆ “Preparing Active Directory” on page 41
- ◆ “Installing SecureLogin: Active Directory” on page 48
- ◆ “Setting the Default Domain Policy” on page 51
- ◆ “Installing Management Tools for Active Directory” on page 52

Preparing Active Directory

Prerequisites

- The Microsoft Windows 2000 or 2003 Server family operating system (including Active Directory) is installed on at least one domain controller in your network.
- The latest service pack is installed.
Service packs are required so that you can install the Adminpak for the Windows 2000 or Window 2003 server.
- The Adminpak for the Windows 2000 or Window 2003 server is installed.
If the Adminpak isn't installed, you can't extend the Active Directory schema.

Preparing to Extend the Active Directory Schema

If this is the first installation of SecureLogin on your server, you must extend the Microsoft Active Directory Schema before installing SecureLogin.

Management of the schema is restricted to a group of administrators called schema administrators. The Active Directory Schema snap-in allows schema administrators to manage the Active Directory schema by doing the following:

- ◆ Creating and modifying classes and attributes.
- ◆ Specifying which attributes are indexed and which attributes are to be catalogued in the global catalog.

WARNING: Extending the schema is a highly sensitive operation, with implications potentially throughout your network. Improper schema modifications can impair or disable Windows 2000 Server and possibly your entire network. Please seek the advice of a qualified systems administrator if you are uncertain about schema extension.

As a schema administrator, you won't perform schema management tasks frequently. Observe three safety precautions that control and limit schema modification:

- ◆ By default, all domain controllers permit Read access to the schema. A registry entry must be set on a domain controller to permit Write access to the schema on that domain controller.
- ◆ The schema object is protected by the Windows 2000 Security model. Therefore, administrators must be given explicit permissions or be members of the Schema Administrators group to make changes to the schema.
- ◆ Although Active Directory is based on a multi-master administration model, some operations support only a single master. One of these operations is schema management. Only one domain controller can write to the schema at any given time. This role is known as Schema Floating Single Master Operations (FSMO).

To manage the schema, you must be connected to the schema FSMO. By default, the schema snap-in is targeted to the schema FSMO role.

Extending the Active Directory Management Schema

You can transfer the schema FSMO from one server to another. However, if you have installed a single Windows 2000 domain controller in your network, this procedure is unnecessary. By default, that single domain controller handles the schema FSMO role.

Transferring the Schema FSMO

- 1** From the left pane of the Microsoft Management Console (MMC), right-click Active Directory Schema.
- 2** Click Change Domain Controller.
- 3** (Conditional) If the name in the Current DC field is not the target server, click Specify Name, type the name of the target domain controller, then click OK.

The following figure illustrates the Current DC field:

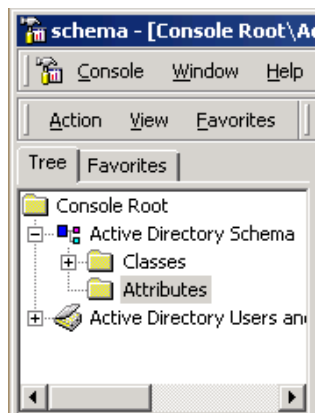


- 4** From the left pane, right-click Active Directory Schema, then click Operations Master > Change.
- 5** Click OK to confirm that you want to change the Operations Master.
- 6** When you receive the message that the Operations Master was successfully transferred, click OK.

Verifying the Domain Controller

- 1 From the left pane of the MMC console, right-click Active Directory Schema, then click Change Domain Controller.

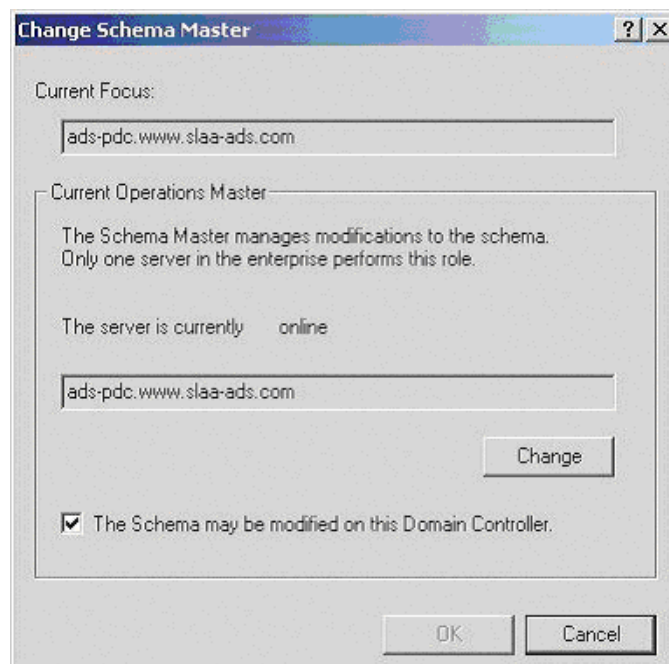
The following figure illustrates Active Directory Schema in the directory structure:



- 2 Verify that the Current DC field lists the domain controller that you are currently working on, then click OK.
- 3 From the left panel, right-click Active Directory Schema, then select Operations Master.
- 4 Check The Schema May Be Modified on This Domain Controller check box, then click OK.

This check box sets a registry entry that permits schema updates. The server automatically detects the change to this registry. You don't have to restart the server to permit the schema to be updated.

The following figure illustrates this check box:



Extending the Active Directory Schema

To store information such as a user's credentials, application scripts, preferences and corporate configuration, you must extend the Active Directory schema to accommodate six object attributes.

1 Run adsschema.exe.

This file is available on your workstation after you run nsl351.exe from the CD or download image. Typically, this file is in the c:\securelogin\tools directory. However, if you unzipped 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
```

When you run adsschema.exe on the server that is the FSMO master, adsschema.exe adds six attributes to the schema:

protocom-SSO-Auth-Data. This attribute is only for a User object. It is an octet-string type. It contains all user-specific authentication data, such as the passphrase.

protocom-SSO-Entries. This attribute is for User, Container, and Organizational Unit objects. It is an octet-string type. This attribute contains the following:

- ◆ All the user's login user IDs and passwords
- ◆ Specific preferences and application definitions at the User object
- ◆ Corporate application definitions and preferences at the Container and Organizational Unit objects

protocom-SSO-Entries-Checksum. This attribute optimizes the loading of data from Active Directory. Whenever data changes in the protocom-SSO-Entries attributes, the Checksum attribute is updated. When SecureLogin loads, it reads the checksum and compares it to the checksum in memory. If the checksums are different, SecureLogin reloads the Entries attribute from the directory.

protocom-SSO-Profile. This attribute contains the user's distinguished name.

protocom-SSO-Security-Prefs. This attribute stores data required for the Advanced Passphrase policies. This data includes Administrator-set Passphrase questions, Passphrase help information, and settings.

protocom-SSO-Security-Prefs-Checksum. This attribute functions with the protocom-SSO-Security-Prefs attribute much like the protocom-SSO-Entries-Checksum functions with the protocom-SSO-Entries attribute.

2 Reboot the computer.

If you need to verify that the schema has been extended, see [“Verifying the Active Directory Schema” on page 87](#).

Assigning User Rights

You can assign SecureLogin schema attribute rights to user objects, containers, and organizational units. Assigning rights to containers and organizational units filters down to all associated user objects. Therefore, unless you have a specific requirement to do so, it is unnecessary to assign rights at the individual user object level.

To assign user rights:

- 1 If it is not already running, run adsschema.exe, found in the \securelogin\tools directory.

- 2 Click Assign User Rights, then click OK.

The Assign Rights to This Object dialog box appears.



In the above figure, rights are assigned to the User container.

The User container definition is:

cn=users, dc=www, dc=training2, 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 Click OK.

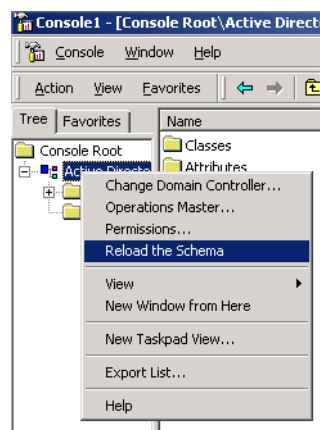
The Active Directory Schema dialog box reappears. Click OK to enter another context, or click Cancel.

If an error appears during an attempted login immediately after the install of SecureLogin on the Active Directory server, OK the message and wait for a few minutes before trying again. The reason for this error is because Active Directory takes time to synchronize. If the error continues, you might need to reboot the server.

Refreshing the Directory Schema

To do this,

- 1 From the left pane of the Microsoft Management Console (MMC), right-click Active Directory Schema.
- 2 Select the Reload the Schema option from the menu.



- 3 Select Exit from the Console menu to close the MMC.

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

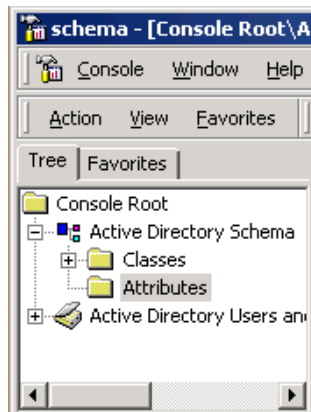
NOTE: Rights to objects can be assigned at any time after extending the schema. If you add organizational units, you need to rerun the adschema.exe tool and assign rights to the new OU to enable SecureLogin functionality.

Replicating Six Attributes

To enable other servers to have the protocom-SSO-Auth-Data, protocom-SSO-Entries, protocom-SSO-Entries-Checksum, protocom-SSO-Profile, protocom-SSO-Security-Prefs, and protocom-SSO-Security-Prefs-Checksum attributes, you must replicate the attributes.

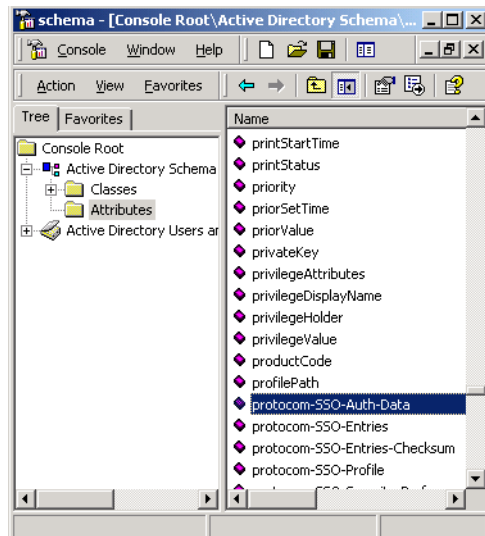
- 1 In the MMC tool, navigate to the Attributes folder.

The following figure illustrates the Attributes folder:



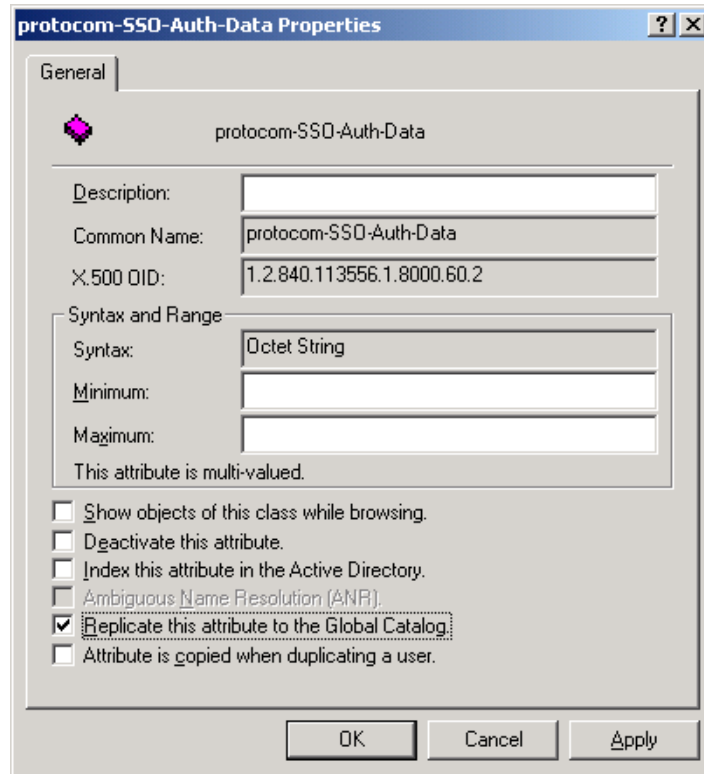
- 2 Right-click the protocom-SSO-Auth-Data attribute, then click Properties.

The following figure illustrates the protocom-SSO-Auth-Data attribute:



- 3 Check the Replicate This Attribute to the Global Catalog check box, then click OK.

The following figure illustrates this check box:



- 4** Repeat this process for protocom-SSO-Entries, protocom-SSO-Entries-Checksum, protocom-SSO-Profiles, protocom-SSO-Security-Prefs, and protocom-SSO-Security-Prefs-Checksum attributes.
- 5** Shut down and restart the management console.

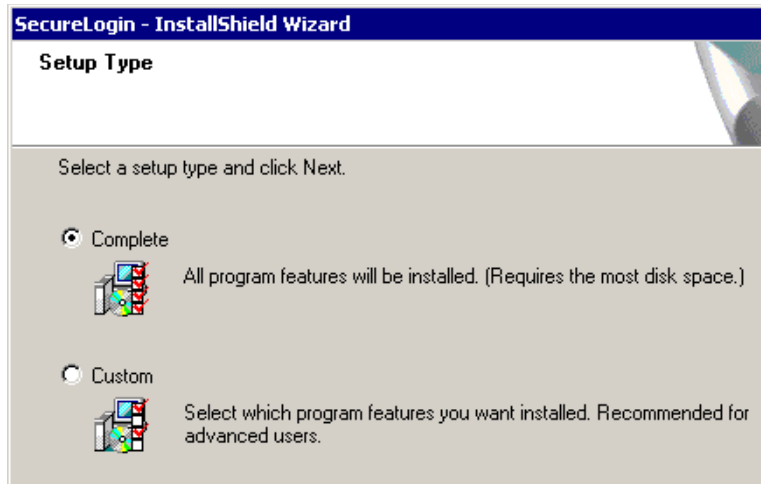
Active Directory doesn't incorporate the new attributes until the management console is restarted.

Installing SecureLogin: Active Directory

For Windows 2000 and Windows XP Pro workstations, install SP6A for NT4.

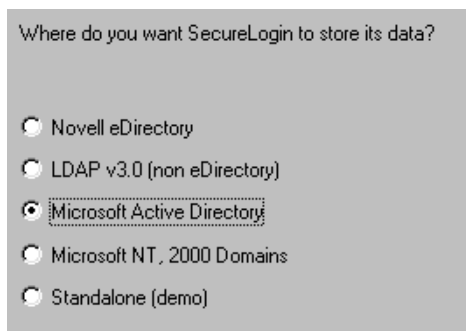
The following information assumes that you have installed the Microsoft Windows 2000 or 2003 Server family operating systems (including Active Directory) on at least one domain controller in your network.

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

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

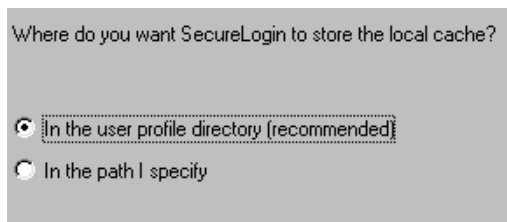


- 5 Click Finish, click Yes, then restart your workstation by clicking OK.
- 6 After the workstation restarts, provide a passphrase question and passphrase answer, then click OK.

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:

- ◆ Specify a path for SecureLogin's local cache.

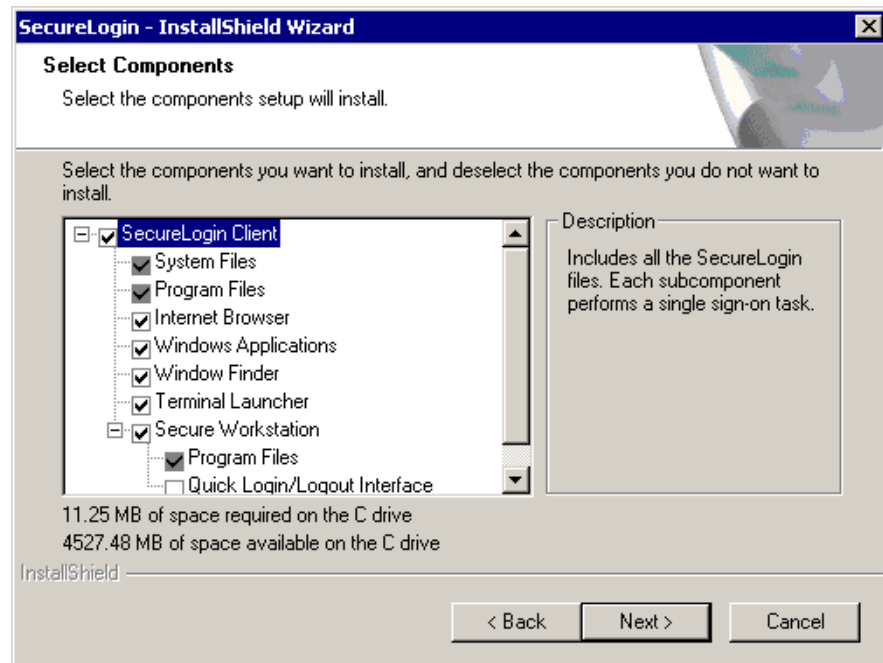


The user profile directory is the default path.

User profiles are in the following locations:

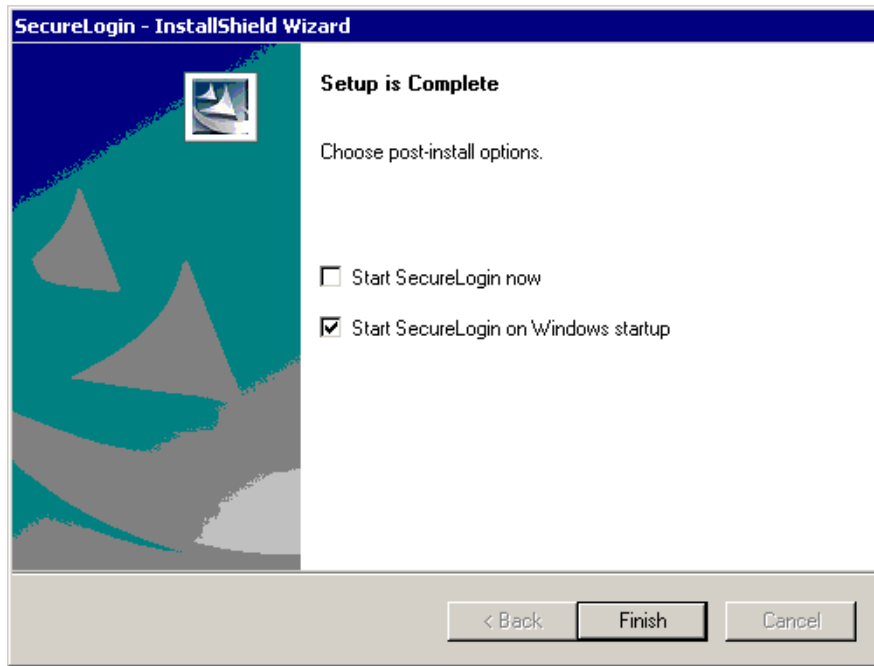
Platform	The User Profile Directory
Windows 98/NT	In c:\windows directory if profiles are disabled. In c:\windows\profiles if profiles are enabled.
Windows 2000/XP	In Documents and Settings\ <i>username</i>

- ◆ Select SecureLogin components.



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

- ◆ Select options for starting SecureLogin.



If the Start SecureLogin Now check box is checked, SecureLogin will be started after the installation, unless you are prompted to restart your workstation.

When the Start SecureLogin On Windows Startup check box is checked, SecureLogin starts immediately after you log in to Windows.

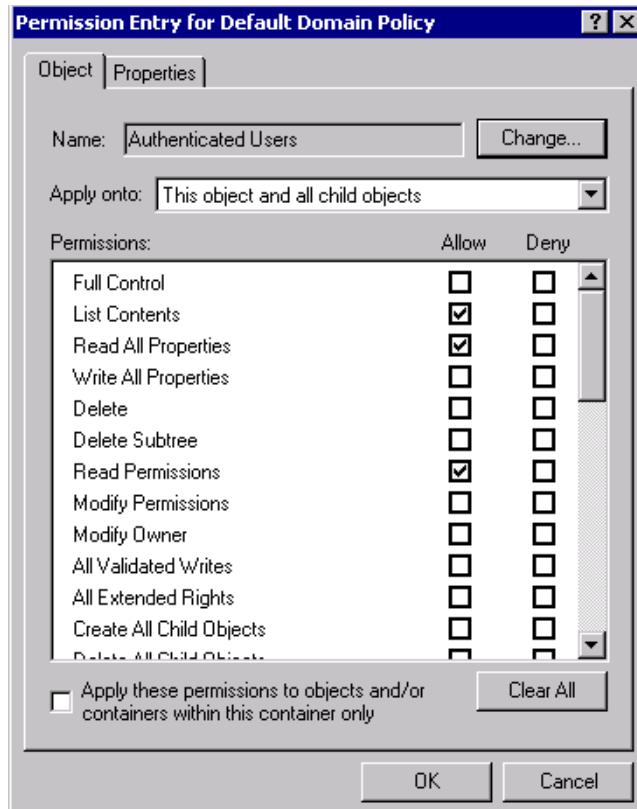
- ◆ Select when to restart the computer.

Setting the Default Domain Policy

At the domain level, make sure that the Default Domain policy allows all authenticated users to have Read rights to All Properties.

- 1** Expand Active Directory Users and Computers, right-click the domain name, then select Properties.
- 2** Select the Group Policy tab, click Properties, then select the Security tab.
- 3** Click Advanced.
- 4** Select Authenticated Users Special, then click View/Edit.
- 5** Under the Allow column, verify that the Read All Properties check box is checked.

The following figure illustrates this check box:



6 Click OK.

Installing Management Tools for Active Directory

When you run setup.exe on a server, the installation program does the following:

- ◆ Detects that the computer is a server and that Active Directory is installed.
- ◆ Installs ssommc.dll, which is the SecureLogin snap-in to MMC.
- ◆ Registers ssommc.dll.

Setup.exe is in the \securelogin\client directory.

In addition to using MMC, you can use slmanager.exe to administer SecureLogin for Active Directory. This utility is found in the \securelogin\tools directory.

5

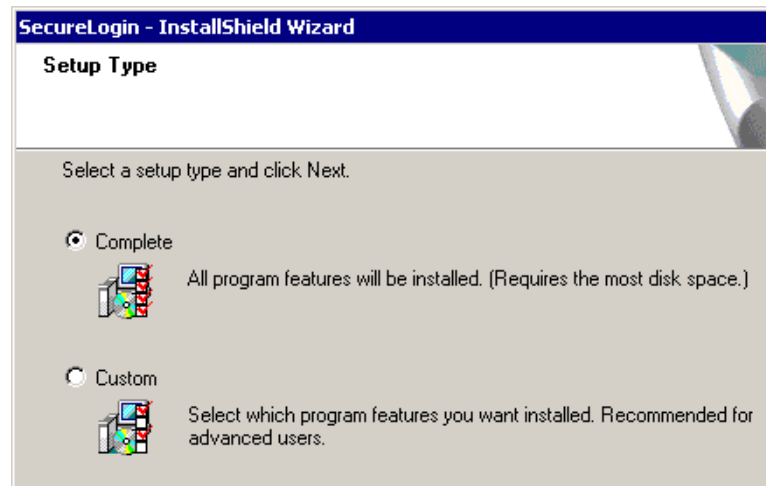
Installing in Windows NT/2000 Domains

This section contains information on the following:

- ♦ [“Installing SecureLogin: Microsoft NT/2000 Domains”](#) on page 53
- ♦ [“Using Administrative Tools”](#) on page 55

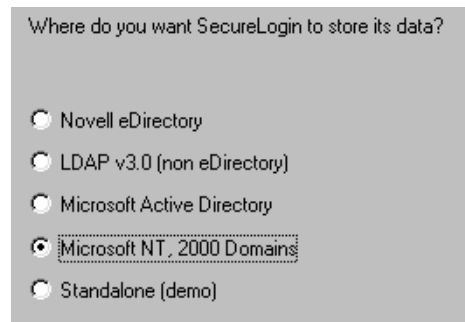
Installing SecureLogin: Microsoft NT/2000 Domains

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



The Complete option uses default values. For options available through the Custom installation, see [“Using the Custom Option: SecureLogin in NT/2000 Domains”](#) on page 54.

- 4 Click Microsoft NT/2000 Domains > Next.



5 At the Ready to Install SecureLogin dialog box, click Install.

6 Click Finish.

7 Click when to restart the computer, then click OK.

7a (Optional) Start SecureLogin now.

If the Start SecureLogin Now check box is checked, SecureLogin will be started after the installation, unless you are prompted to restart your workstation.

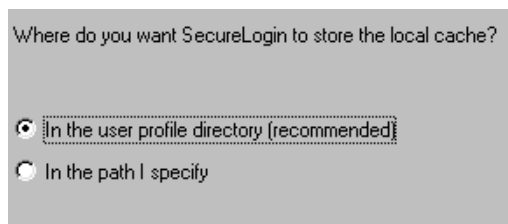
If you check the Start SecureLogin On Windows Startup check box, Windows places the SecureLogin icon on the system tray. You can then access SecureLogin from the system tray or from Start > Programs > Novell SecureLogin > Novell SecureLogin.

7b (Optional) Start SecureLogin whenever Windows starts up.

Using the Custom Option: SecureLogin in NT/2000 Domains

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

- ◆ Specify the folder 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.



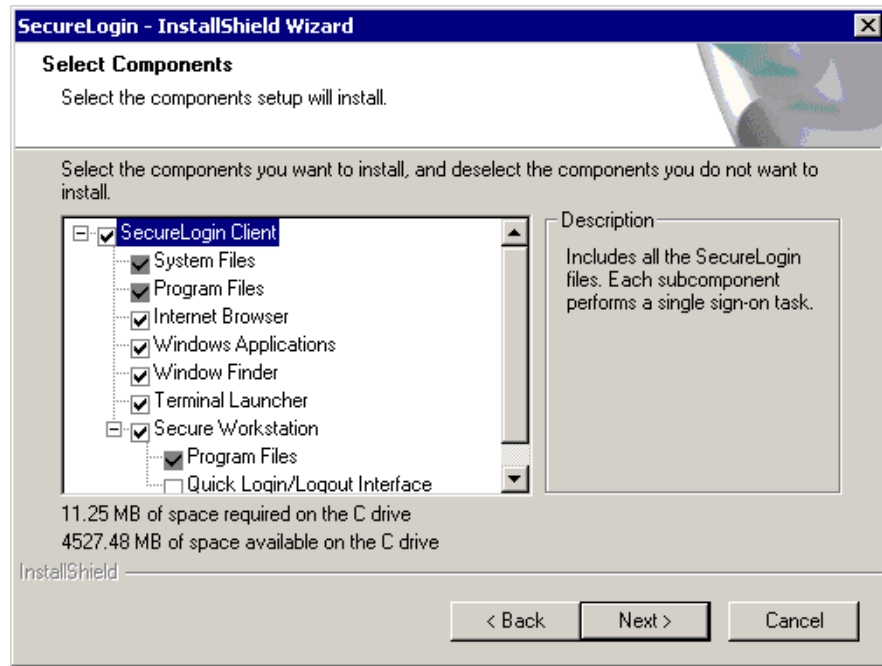
The user profile directory is the default path.

User profiles are in the following locations:

Platform	The User Profile Directory
Windows 9x	In c:\windows directory if profiles are disabled. In c:\windows\profiles if profiles are enabled.
Windows NT/2000	In Document and Settings\ <i>username</i>

- ◆ Select SecureLogin components.

You must install the SecureLogin client component. As the following dialog box illustrates, this option is selected by default.



Using Administrative Tools

You can use `slmanager.exe` to administer SecureLogin for NT 4 Domains. This utility is found in the `\securelogin\tools` directory.

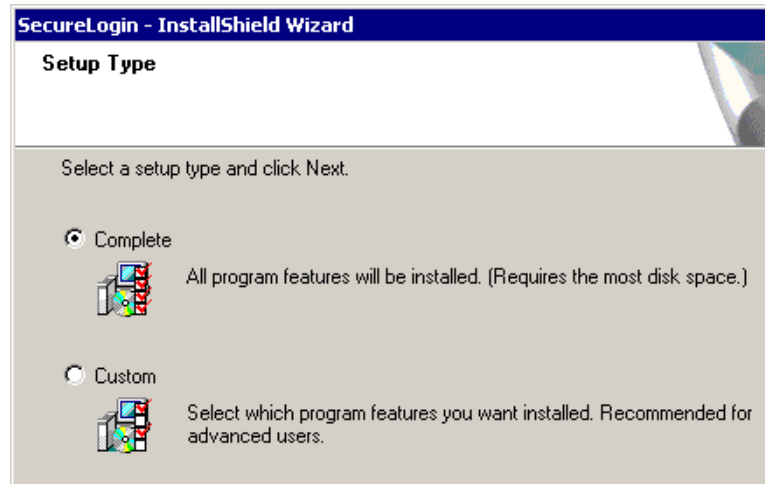
6

SecureLogin on a Standalone Workstation

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

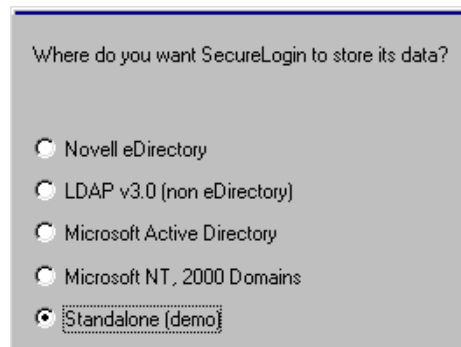
Installing SecureLogin: Standalone Workstations

- 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.



- 5** Click Next > Install.
- 6** Click when to restart the computer, then click OK.
- 6a** (Optional) Start SecureLogin now.

If the Start SecureLogin Now check box is checked, SecureLogin will be started after the installation, unless you are prompted to restart your workstation.

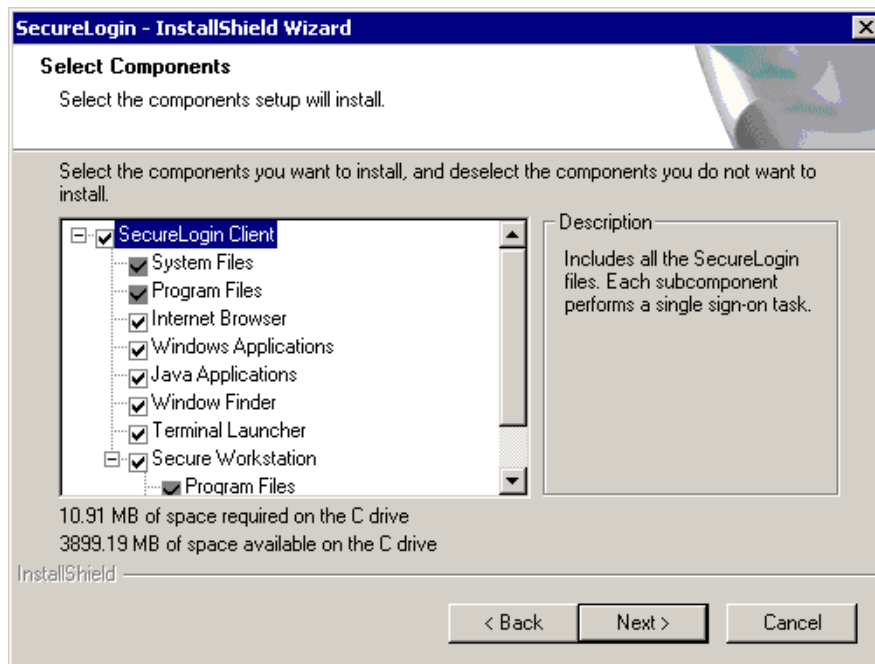
- 6b** (Optional) Start SecureLogin whenever Windows starts up.

If the Start SecureLogin On Windows Startup check box is checked, SecureLogin starts immediately after you log in to Windows.

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 SecureLogin's local cache.
- ◆ Select SecureLogin components.



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

If the Java Runtime Environment (JRE) isn't 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.

Also, Secure Workstation isn't available for Windows 98 or NT workstations. Otherwise, it is selected and installed by default.

7

Upgrading from Earlier Versions

This section provides information on the following:

- ♦ “Upgrading from Novell SecureLogin 2.5” on page 59
- ♦ “Upgrading from Novell SecureLogin 3.0.x” on page 59

Upgrading Entirely to SecureLogin 3.51.2

If you plan to upgrade all previous versions to SecureLogin 3.51.2, use information in this section. If you plan to have a mixed environment, where some workstation are running SecureLogin 3.51.2 but other workstations are running earlier versions, see Running SecureLogin 3.51.2 in Mixed Environments.

Before upgrading from SecureLogin 3.0.x to SecureLogin 3.51.2, close SecureLogin. The installation program can normally handle locked files. However, some problems can occur on Windows 9x computers due to the short-name limitation of 8.3 filenames.

Upgrading from Novell SecureLogin 2.5

SecureLogin 2.5 could be deployed to run in standalone mode or with eDirectory™. Even if SecureLogin 2.5 was deployed to work with eDirectory, 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 2.5 and automatically works with it.

If all SecureLogin 2.5 data was stored in eDirectory, and if SecureLogin 3.51.2 is installed to work with Novell SecretStore®, SecureLogin 3.51.2 is able to use the data from SecureLogin 2.5. This usage occurs because SecureLogin 3.51.2 still uses the Prot:* attributes in the directory, even if it is deployed to use SecretStore.

To upgrade from SecureLogin 2.5:

- 1** Uninstall SecureLogin 2.5.
- 2** Install SecureLogin 3.0.6.
- 3** Uninstall SecureLogin 3.0.6.
- 4** Install SecureLogin 3.51.2 by running setup.exe, found in the \securelogin\client directory on the Novell SecureLogin 3.51.2 software image or CD.

Upgrading from Novell SecureLogin 3.0.x

To upgrade from SecureLogin 3.0.x versions:

- 1** Make sure that SecureLogin isn't running on your workstation.

The installation program can normally handle locked files. However, some problems can occur on Windows 9x computers due to the short-name limitation of 8.3 filenames.

2 Run setup.exe.

SecureLogin 3.51.2 overwrites earlier files but preserves data in the cache. The installation program detects the previous installation settings and uses them as the default.

For example, the cache option defaults to the profile directory, unless the previous installation placed the cache elsewhere.

Setup.exe is in the \securelogin\client directory on the Novell SecureLogin 3.51.2 image or CD.

Running SecureLogin 3.51.2 in Mixed Environments

You can run SecureLogin 3.51.2 and SecureLogin 3.0.x in the same environment.

However, you can't run SecureLogin 2.5 and SecureLogin 3.51.2 in the same environment. You must upgrade SecureLogin 2.5 to SecureLogin 3.0.6 and then (optionally) to SecureLogin 3.51.2.

When SecureLogin 3.51.2 runs in the same environment as SecureLogin 3.0.x, SecureLogin 3.51.2 does the following:

- ◆ Versions the SecureLogin data store.
- ◆ Saves SecureLogin 3.51.2 single sign-on data in the SecureLogin 3.0 data format.

This mixed mode enables you to gradually deploy SecureLogin 3.51.2 in a SecureLogin 3.0 environment while still allowing you to perform most administration tasks during the transition.

Deploying SecureLogin 3.51.2 in a mixed environment has the following limitations:

- ◆ Limited administrative functionality

When you run SecureLogin 3.51.2 in mixed mode, new features such as shadow variables will not work. Also, some SecureLogin 3.51.2 settings and changing script descriptions aren't supported in mixed mode.

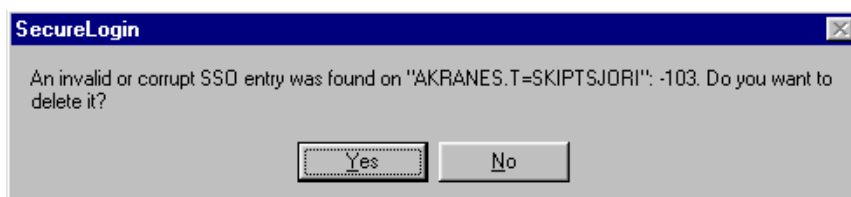
- ◆ Warning messages

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.

Upgrading to SecureLogin 3.51.2

SecureLogin's single sign-on functionality 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 3.51.2 schema tool, SecureLogin uses the new data format.

If you install SecureLogin 3.51.2 into a tree that is using SecureLogin 3.0 data formats, a warning message appears when you run the schema extension tool:



If you select No, SecureLogin runs in mixed mode. In this mode, SecureLogin 3.0 and SecureLogin 3.51.2 clients are both able to run, but SecureLogin 3.51.2 clients lose some functionality.

In mixed environments, SecureLogin 3.51.2 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 3.51.2, 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 3.51.2 workstations.

After all users in the tree have been upgraded to SecureLogin 3.51.2, you can run the schema extension tool and upgrade the directory schema. All SecureLogin clients will then upgrade their data stores to the SecureLogin 3.51.2 format.

If any SecureLogin clients remain in the tree after the schema has been updated to include the SecureLogin3.51.2 attributes, the SecureLogin 3.0 clients will receive the "corrupt data" error message.

After the directory schema has been extend for SecureLogin 3.51.2, it isn't possible to revert to the SecureLogin 3.0 data format.

Managing Mixed Environments

While SecureLogin is running in mixed mode, you will be able to modify most 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 3.51.2 but was not present in SecureLogin 3.0. Incompatible data could come from the following:

- ◆ Dialog position information
- ◆ New settings
- ◆ Shadow variables

8

Installing and Configuring Secure Workstation

This section provides information on the following:

- ◆ “Overview” on page 63
- ◆ “Setting Up Secure Workstation” on page 64
- ◆ “Understanding Secure Workstation Policies” on page 65
- ◆ “The Local Policy Editor” on page 66
- ◆ “Configuring Secure Workstation Events” on page 69
- ◆ “Advanced Settings” on page 73
- ◆ “The Secure Workstation Post-Login Method for NMAS” on page 76
- ◆ “Quick Login/Logout” on page 78
- ◆ “Details about Policy Enforcement” on page 81

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. For other Windows platforms, use Workstation Access.

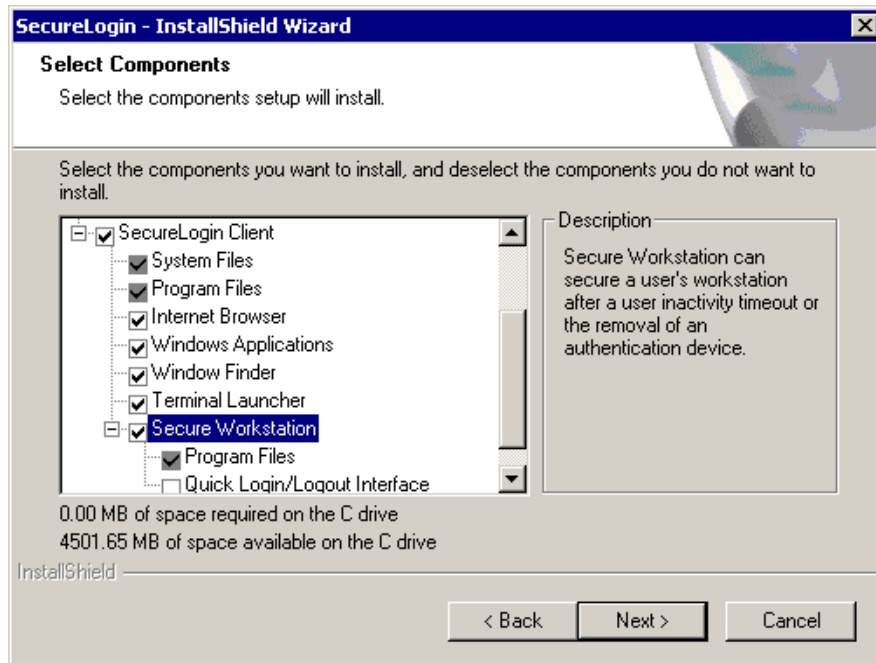
Setting Up Secure Workstation

This section provides information on the following:

- ◆ “Installing Secure Workstation” on page 64
- ◆ “Installing the ConsoleOne Snap-In to Secure Workstation” on page 65

Installing Secure Workstation

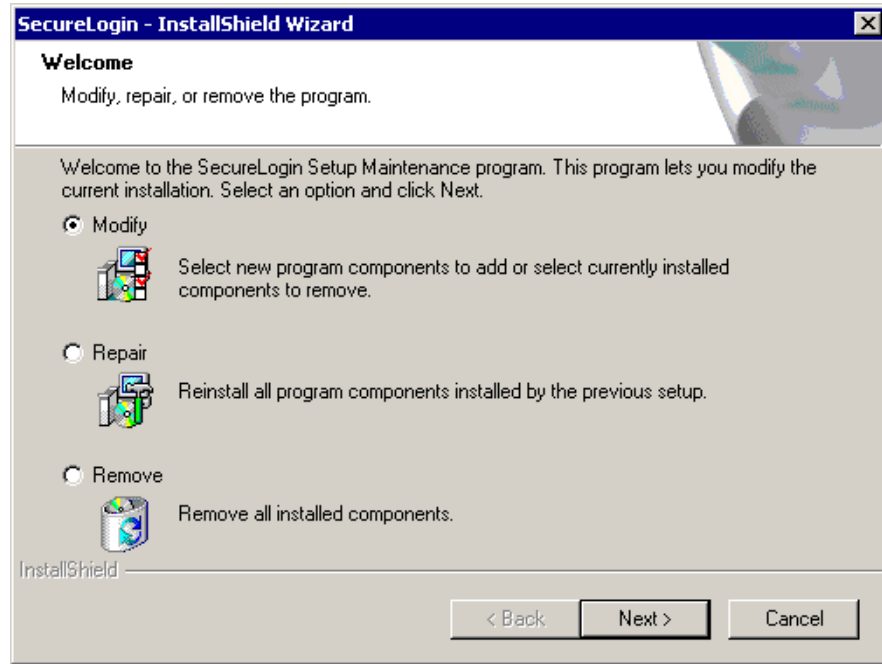
By default, Secure Workstation program files are installed with the Complete option during a SecureLogin 3.51.2 client installation. As the following figure illustrates, however, the Quick Login/Logout Interface isn't installed by default.



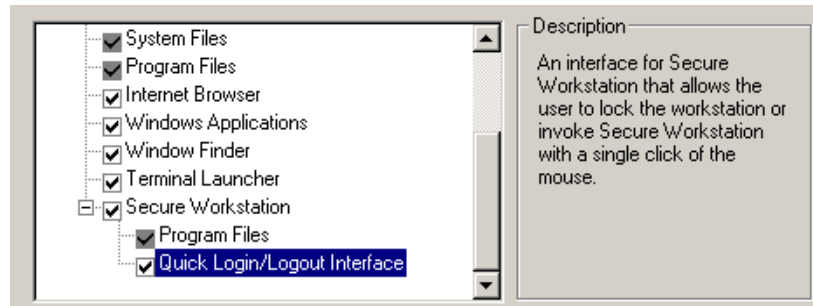
If you selected the Custom option and deselected the Secure Workstation component, you can quickly add it.

- 1 Run setup.exe, found in the \client directory on the SecureLogin 3.51.2 image.

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



- 2** Select Modify, then click Next.
- 3** Check the SecureLogin check box and the desired subcomponents.



- 4** Click Next, then click Finish.

Installing the ConsoleOne Snap-In to Secure Workstation

You administer Secure Workstation by using ConsoleOne™ and by configuring Secure Workstation settings on the workstation.

The Secure Workstation snap-in to ConsoleOne is installed when you install the post-login method. You can also run `nwsnapin.exe`, found in the `\consoleone\snapins` directory on the SecureLogin 3.51.2 image.

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 “[The Secure Workstation Post-Login Method for NMAS](#)” on [page 76](#)). 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.

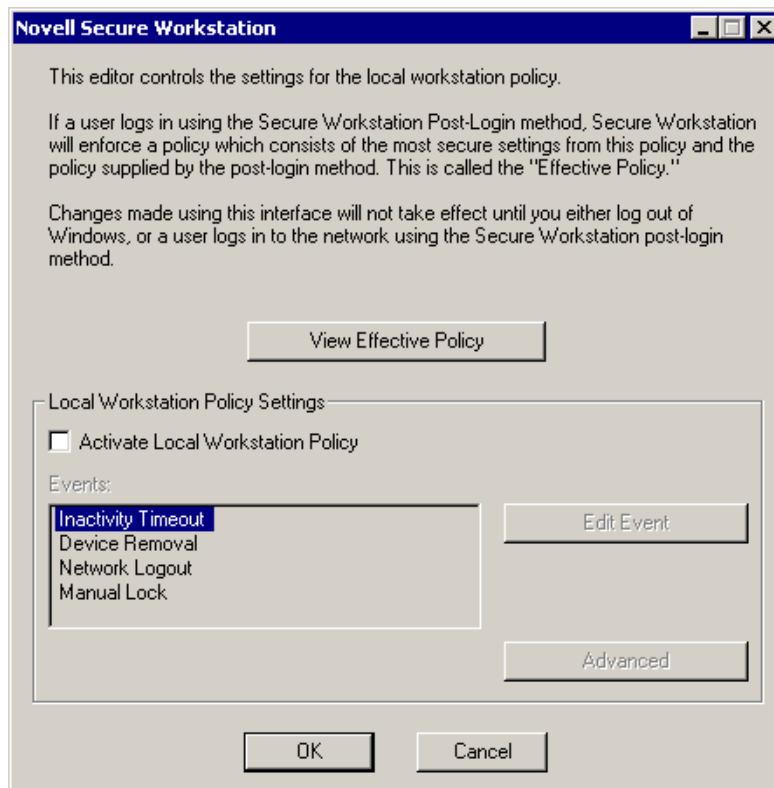
When a user logs in to the network using the Secure Workstation Post-Login Method for NMAS, the post-login method sends the Network policy to the Novell Secure Workstation Service. The service reads the Local policy and combines it with the Network policy to create the Effective policy. The Effective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

The 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.

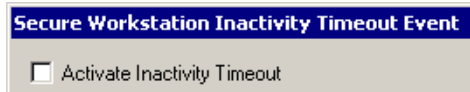
The following figure illustrates the Local Policy Editor's main dialog box:



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.

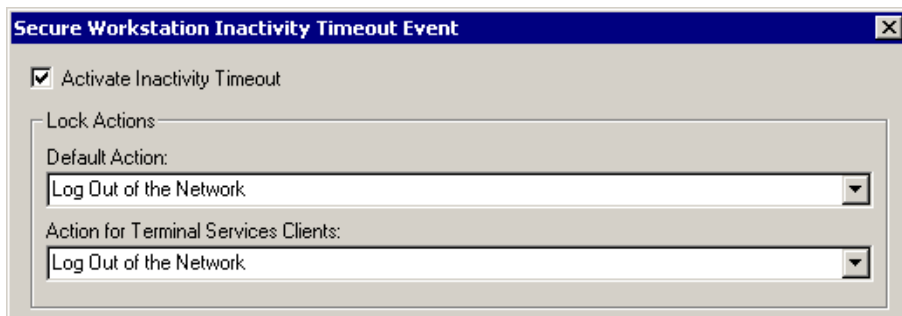
You can edit settings for a specific event by selecting the event in the list box and clicking Edit Event. A dialog box is displayed with settings for the event you select. As the following figure illustrates for the Inactivity Timeout event, the dialog box for each event contains an Activate check box.



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 3.51.2, 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 clients.

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 [“Understanding Secure Workstation Policies” on page 65](#).

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.

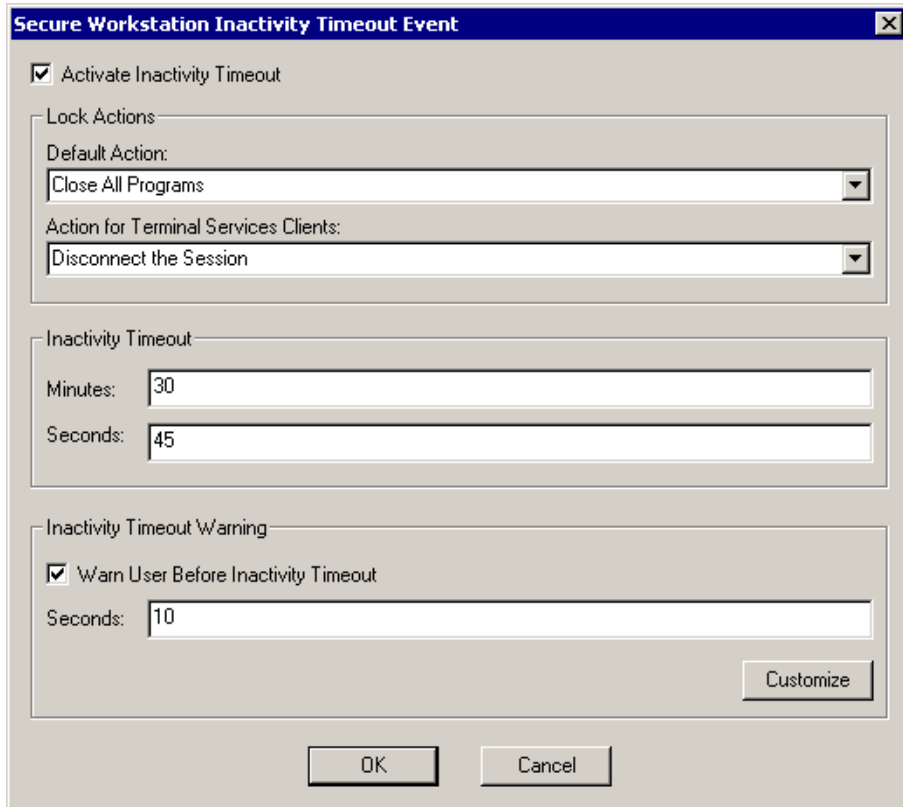
Configuring Secure Workstation Events

This section provides information on the following:

- ◆ [“Configuring an Inactivity Timeout Event” on page 69](#).
- ◆ [“Configuring a Device Removal Event” on page 70](#).
- ◆ [“Configuring a Network Logout Event” on page 71](#).
- ◆ [“Configuring the Manual Lock Event” on page 73](#).

Configuring an Inactivity Timeout Event

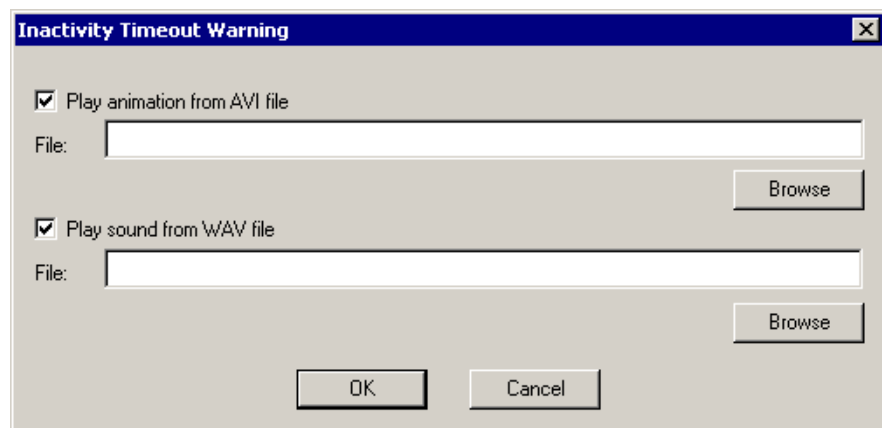
The following figure illustrates the dialog box for configuring Inactivity Timeout events.



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.



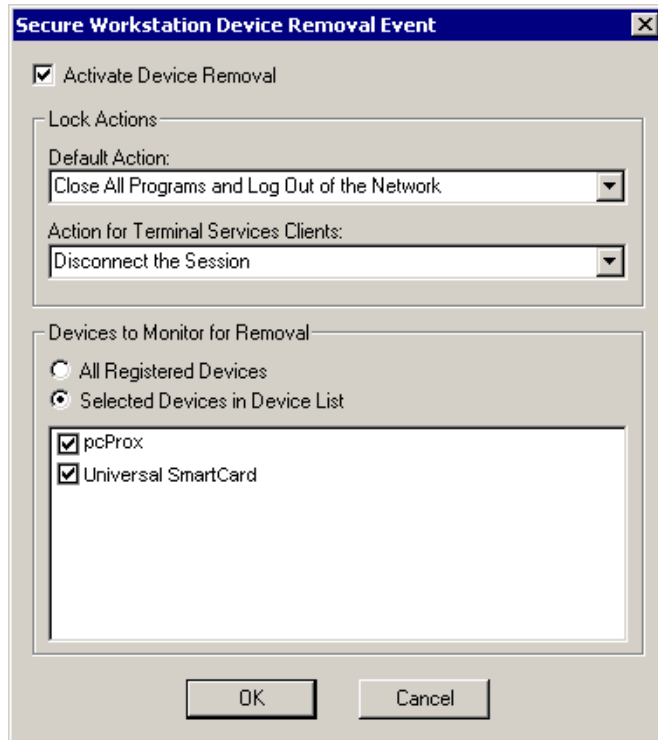
- 3 Browse to and select .avi or .wav files.
- 4 Click OK.

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.

Configuring a Device Removal Event

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



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

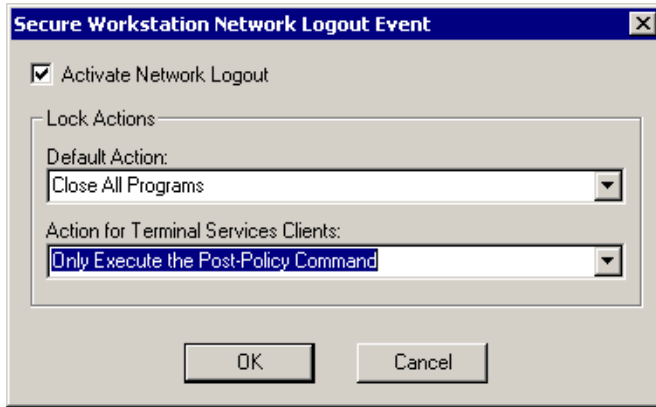
This dialog box enables you to specify which devices are included in the policy. If a device is included in the policy, it must be present during the user's session. If a device in the list is not present, Secure Workstation executes the lock action.

For SecureLogin 3.51.2, 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.

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 [“The Post-Policy Command” on page 76](#).

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.

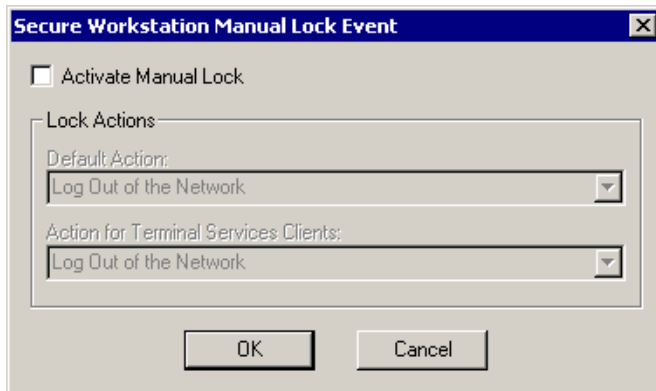
The Network Logout event is the only event that includes the Only Execute the Post-Policy Command action. This action is actually a substitute for the Log Out of the Network action that is available with other events. If you want to execute a Post-Policy Command on network logout, but not do anything 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 [“The Post-Policy Command” on page 76](#).

Configuring the Manual Lock Event

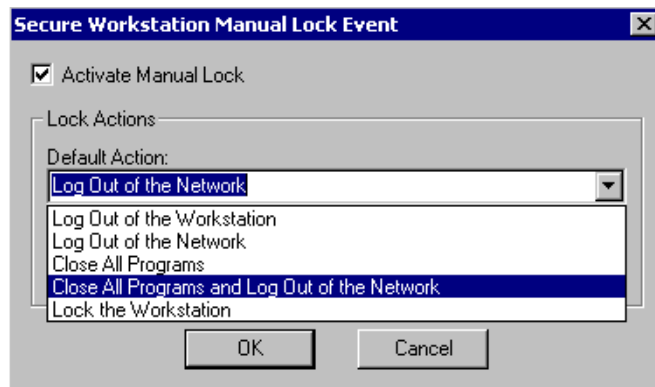
The Manual Lock event gives users the ability to manually trigger Secure Workstation. A user can manually trigger Secure Workstation either by clicking the Logoff button on the Quick Logon/Logoff Interface or by executing SWLock.exe in the System32 directory.

The following figure illustrates the Manual Lock dialog box.



To configure Manual Lock:

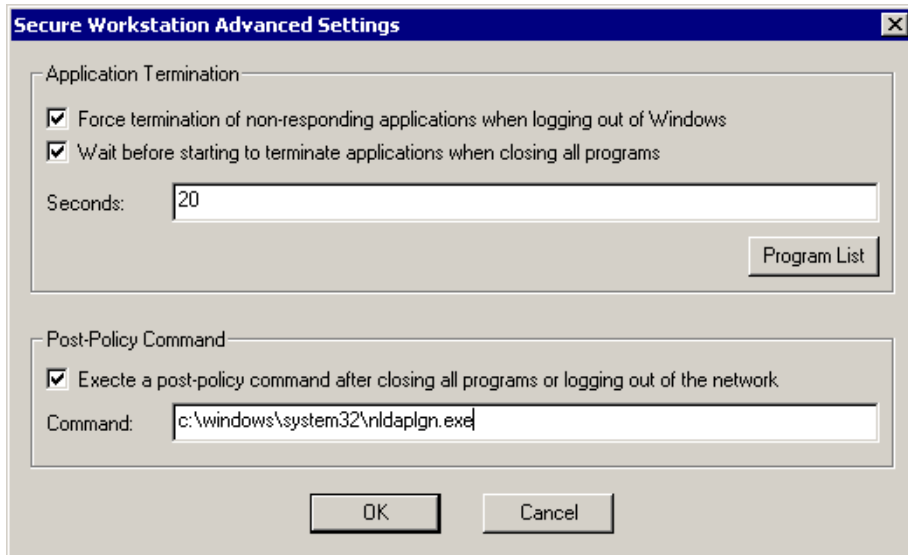
- 1 Select Manual Lock from the main page, then click Edit Event.
- 2 Check the Activate Manual Lock check box.
- 3 (Optional) Select an option from the Default Action drop-down list.



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

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

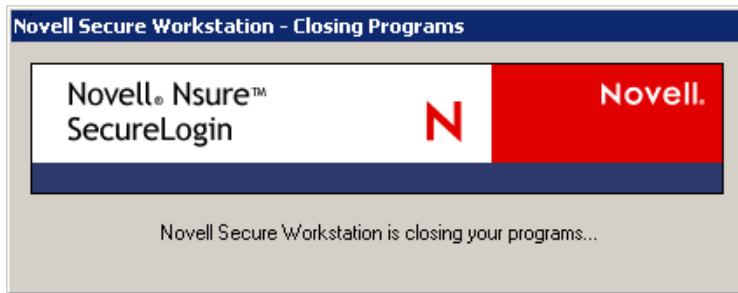
The Force Termination of Non-Responding Applications When Logging Out of Windows check box affects the way that programs will be shut down when Secure Workstation logs a user out of Windows. If this box is checked, Windows terminates programs that don't respond to a "close" message in a timely manner. 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.

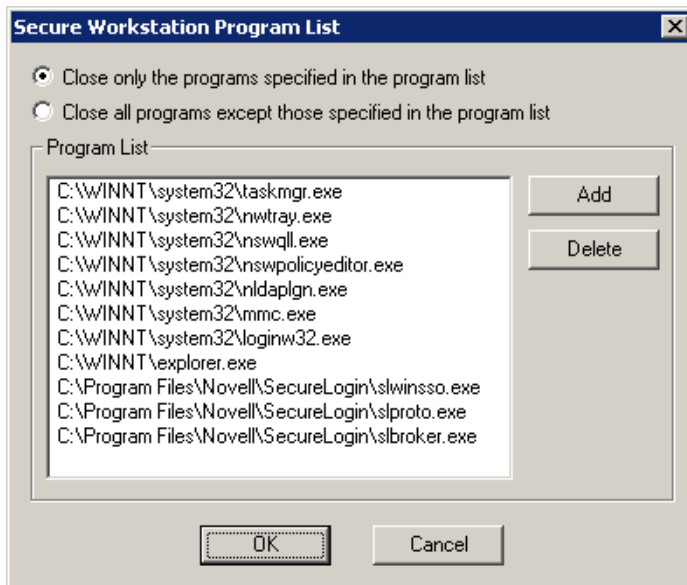
On the other hand, if the Wait Before Starting to Terminate Applications When Closing All Programs check box is checked, Secure Workstation checks to see if the programs are still running after the specified timeout. Any programs that are still running at this point are terminated and might not have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

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



So that you can use Novell SecureLogin scripts to close applications, the dialog box shown in the Novell Secure Workstation Closing Programs figure is displayed while Secure Workstation is executing the Close All Programs action. This feature allows you to set a global variable in your script. The script can use the global variable to distinguish between Secure Workstation closing an application and the user closing an application.

The following figure illustrates a program list:



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 the 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.

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.

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 ConsoleOne to configure the policy. The Network policy contains the same items as the Local policy.

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

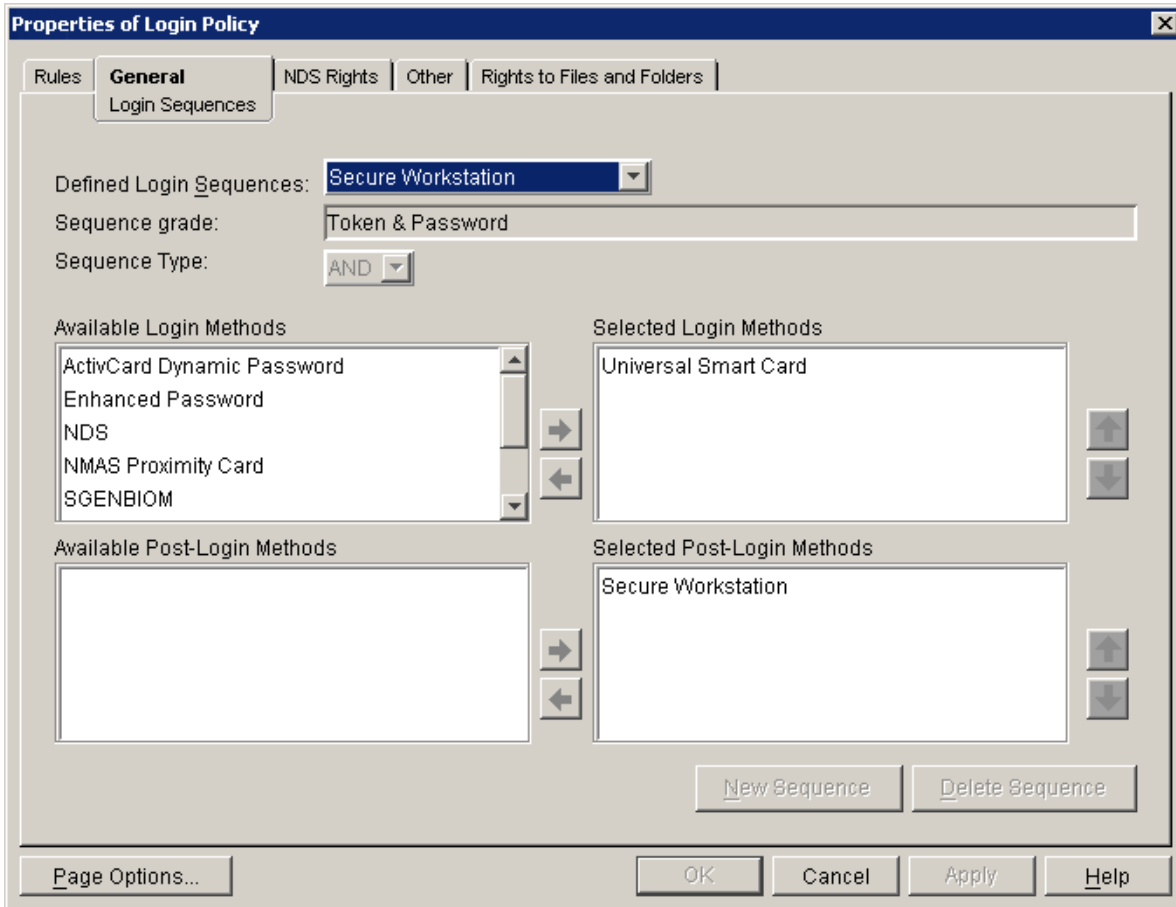
To use the NMAS Method Installer, run methodinstaller.exe, found in the nmas\nmasmethods directory on the Novell SecureLogin 3.51.2 software image or CD.

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 3.51.2 image or CD in the nmas\nmasmethods\novell\secureworkstation 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 ConsoleOne, right-click the Login Policy Object in the Security container and select Properties. You will see the following dialog box:



- 3** Click New Sequence, then select a name for the login sequence.

For example, select Secure Workstation. You can use any name.

- 4** Add methods to your login sequence.

When NMAS executes your login sequence, NMAS executes the methods in the Selected Login Methods list box and then executes the methods in the Selected Post-Login Methods list box. The figure above contains a sequence that executes the Universal Smart Card method and then executes the Secure Workstation method.

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

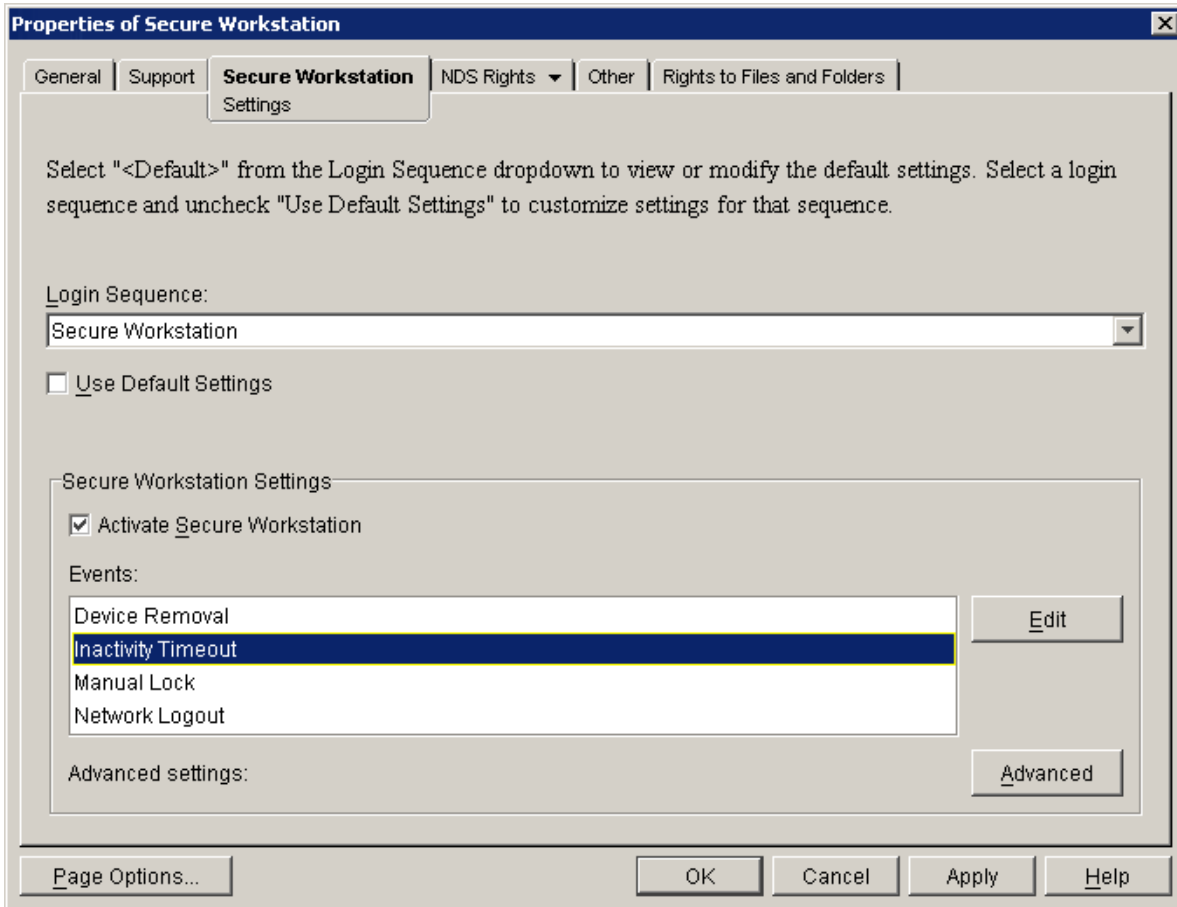
- 5** Configure a policy for the login sequence.

5a Open the Authorized Post-Login Methods located in the Security container.

5b Right-click the Secure Workstation container, then select Properties

5c Select Secure Workstation in the subsequent dialog box.

The following dialog box is displayed:



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.

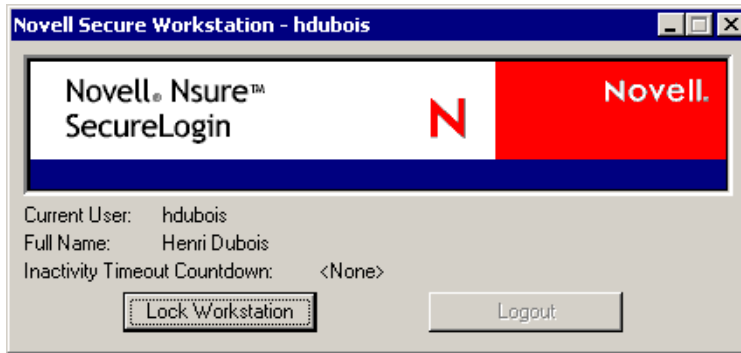
NOTE: You can create as many login sequences that contain the Secure Workstation method as you need. Also, you can associate a different policy with each sequence and then associate each sequence with a different set of users. For information on configuring login sequence restrictions and configuring a user's default login sequence, see the [NMA Administration Guide \(http://www.novell.com/documentation/lg/nmas22/index.html\)](http://www.novell.com/documentation/lg/nmas22/index.html).

The ConsoleOne 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 [“The Local Policy Editor” on page 66](#).

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

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.

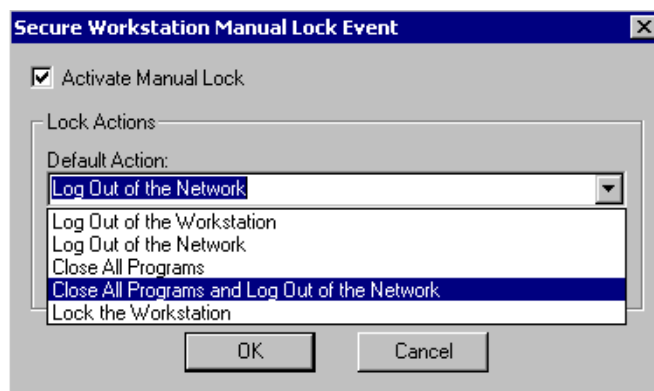
Scenario: Unlocking a Locked Workstation. So that a workstation in the General Services section doesn't remain locked for long periods of time, Sandy changes a registry setting in the LDAP Authentication Client. The setting enables other users to use the locked workstation. Sandy also selects the Network 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.

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 74](#).

Scenario: Sharing a Workstation. Nurses at VMPClinic 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.

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.

9

Troubleshooting

- ♦ [“Can’t Find a Server” on page 81](#)
- ♦ [“If ?sysuser\(system\) and ?syspassword\(system\) Are Unavailable” on page 90](#)
- ♦ [“Useful TIDs” on page 90](#)

For information on error codes, see [“Error Codes”](#) in the [Nsure SecureLogin 3.51.2 Administration Guide](#).

Can’t Find a Server

After you install SecureLogin, use this section if you get an error stating that a directory can’t be found.

- 1** Verify that the DNS name or IP address of your server is correct.
- 2** Verify that the server is up and running.
- 3** Verify that the schema has been extended on that server.

For Novell® eDirectory™, see [“Verifying the eDirectory Schema” on page 81](#)

For LDAP, see [“Verifying the LDAP Directory Schema” on page 84](#).

For Active Directory, see [“Verifying the Active Directory Schema” on page 88](#).

- 4** Verify that rights have been granted.

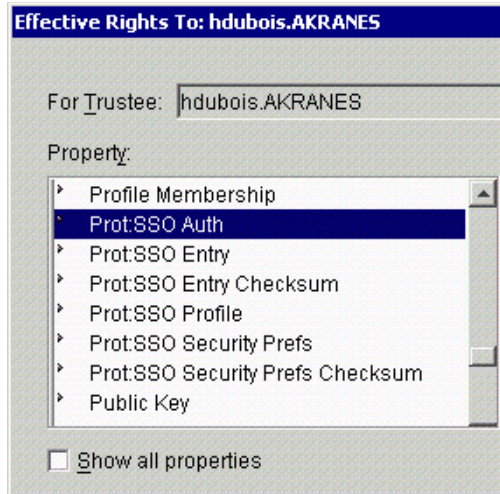
Verifying the eDirectory Schema

For eDirectory, verify that the SecureLogin attributes exist in the extended schema and that rights have been granted. If necessary, add rights.

Verifying SecureLogin Attributes and Rights

When ndsschema.exe extends the NDS® or eDirectory schema, six SecureLogin attributes are added to the directory. You can verify that the attributes exist and that rights have been assigned.

- 1** In ConsoleOne®, right-click an object (for example, Admin).
- 2** Click Rights to Other Objects, then click OK.
- 3** Click Effective Rights.
- 4** In the Property pane, scroll to Prot:SSO Auth, Prot:SSO Entry, Prot:SSO Entry Checksum, Prot:SSO Profile, Prot:SSO Security Prefs, and Prot:SSO Security Prefs Checksum.

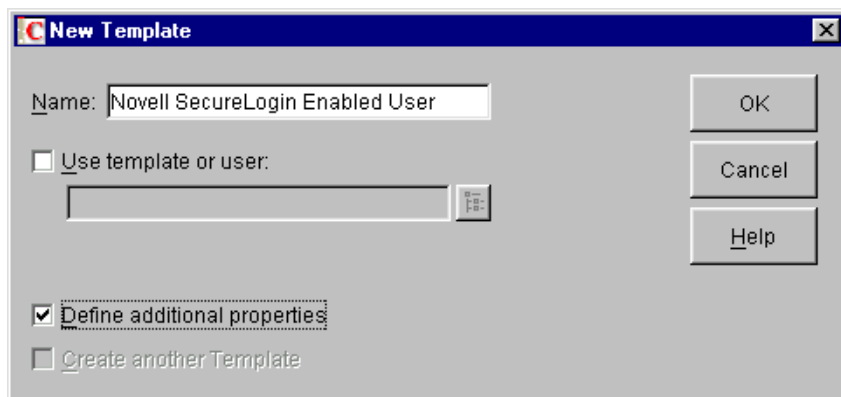


If the attributes don't appear, rerun ndsschema.exe.

Manually Adding Rights

Ndsschema.exe assigns rights to objects in the container that you specify. If you don't specify a container, rights are assigned at the root. If for some reason the rights don't exist, you can manually add them.

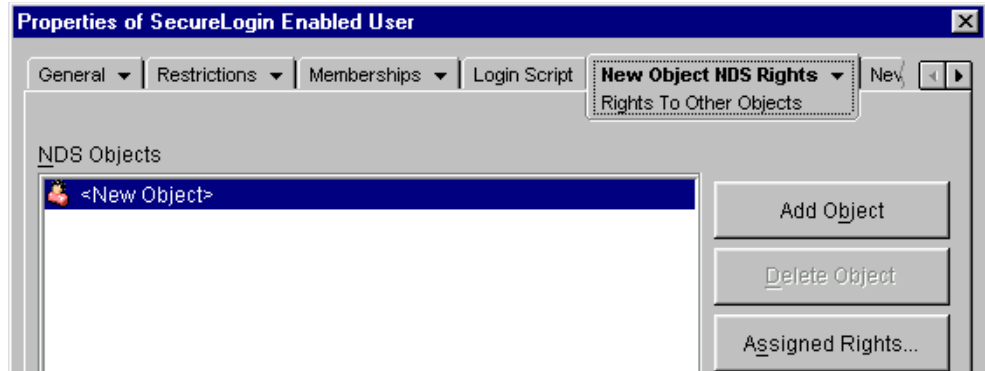
- 1** In ConsoleOne, select an O or OU Container object that will contain the Template object.
- 2** Create a new object of the class Template.
- 3** At the New Template dialog box, name the template, check the Define Additional Properties check box, then click OK.



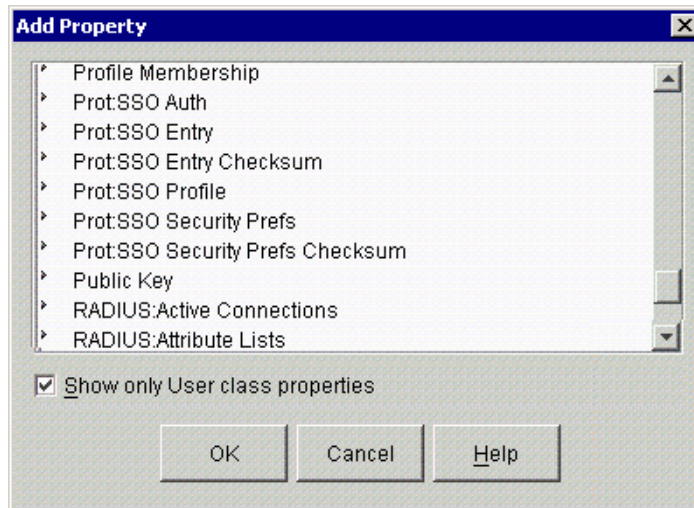
- 4** At the properties page for the new Template object, navigate to and select New Object NDS Rights, then select Rights To Other Objects from the drop-down list.



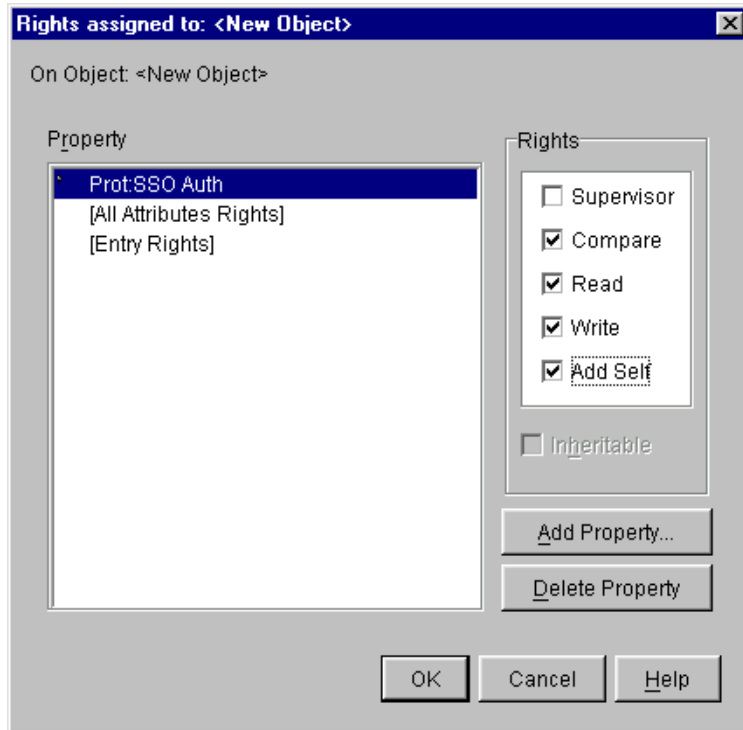
- 5** Click New Object > Assigned Rights.



- 6 Click Add Property, select the Prot:SSO Auth attribute, then click OK.



- 7 At the Rights Assigned To dialog box, check the Compare, Read, Write, and Add Self check boxes, then click OK.



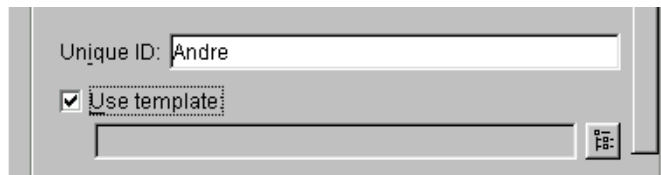
- 8 Configure the Prot:SSO Entry, Prot:SSO Entry Checksum, Prot:SSO Security Prefs, and Prot:SSO Security Prefs Checksum attributes by repeating Steps 5, 6 and 7 for the Prot:SSO Entry attribute.

NOTE: Do not add the Prot:SSO Profile attribute.

- 9 Exit by clicking OK.

To use the new template:

- 1 Create a new User object.
- 2 At the New User property page, enter a name, enter a surname, check the Use Template check box, then click the Browse button.



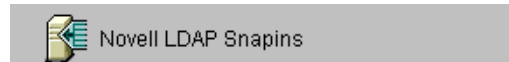
- 3 Navigate to and select the Template object that you created, then click OK twice.
- 4 Type and confirm a password for the new user, then click Set Password.

Verifying the LDAP Directory Schema

To determine whether the LDAP snap-in to ConsoleOne is installed:

- 1 Bring up ConsoleOne.
- 2 Click Help > About Snapins.

- 3 Locate the Novell LDAP Snapins entry.



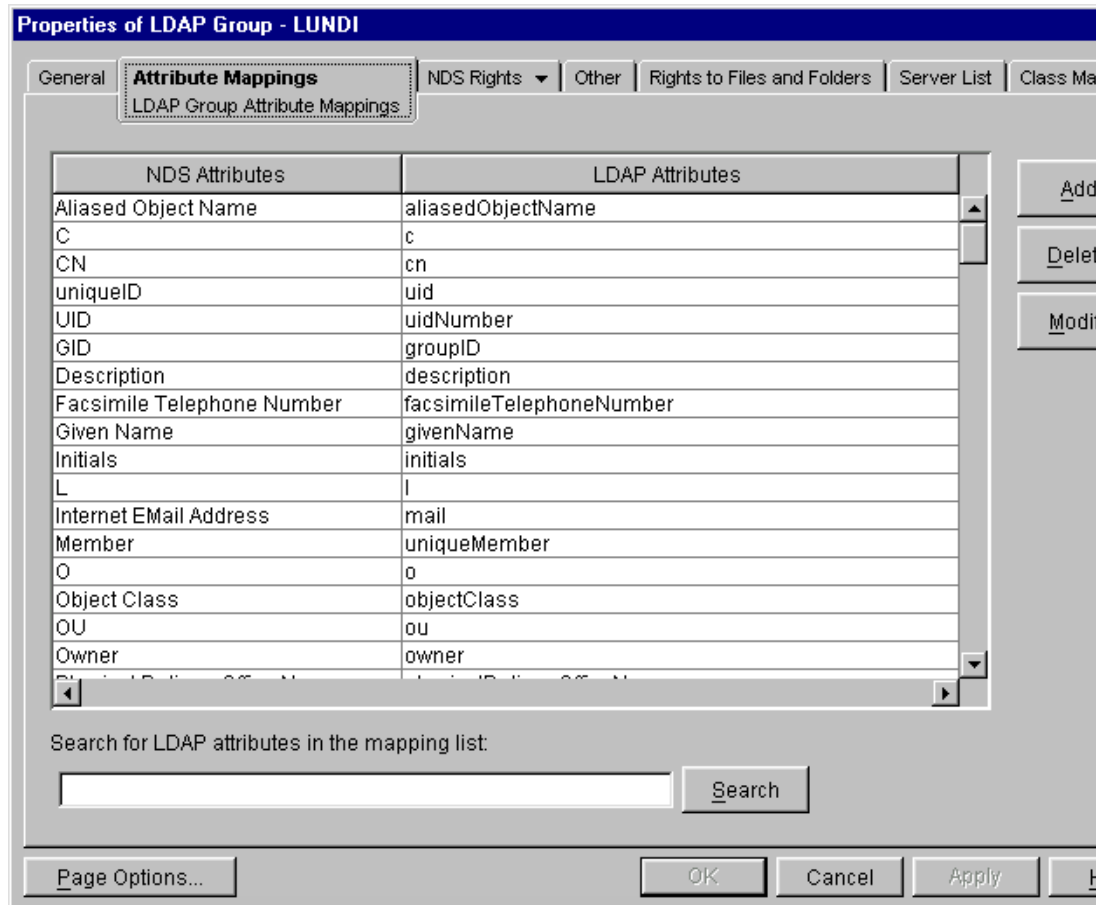
Before LDAP client support can be used, eDirectory attribute names must be mapped to LDAP names.

The LDAP v3.0 client option supports servers that have the following:

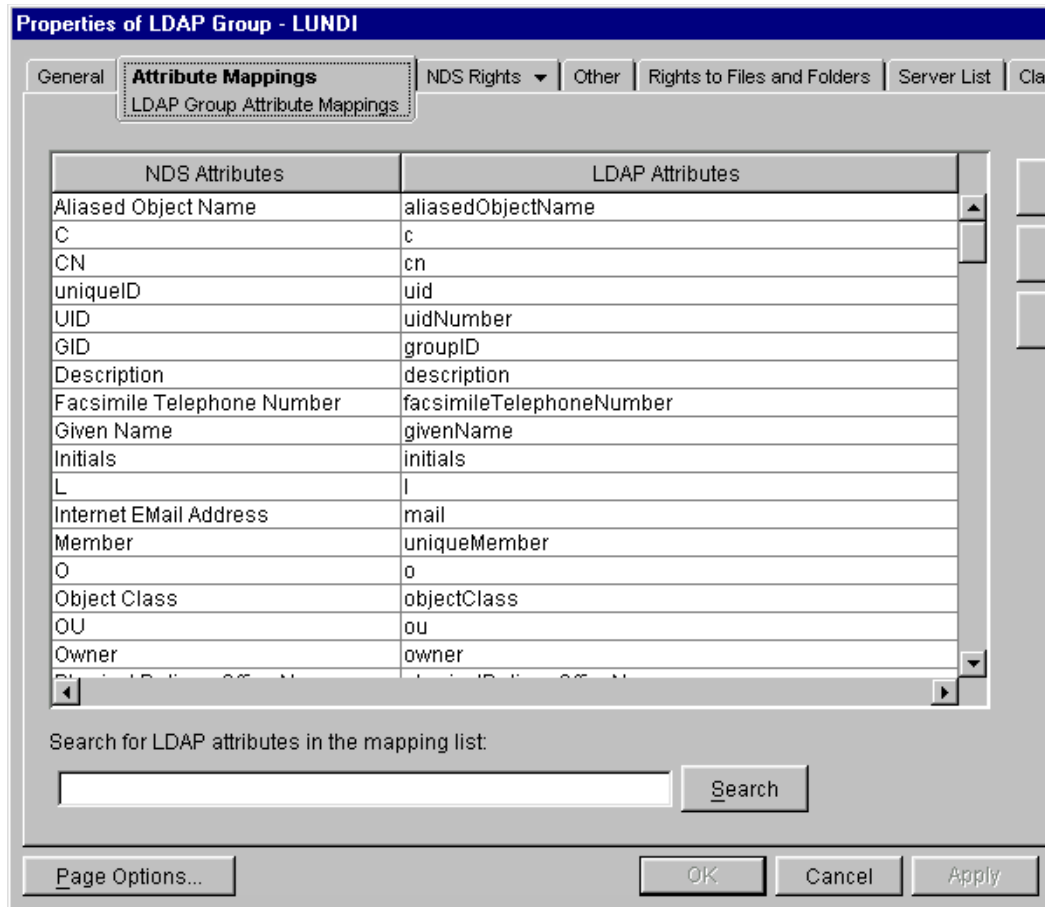
- ♦ Novell eDirectory 8.6.2 or later.
- ♦ LDAP support installed and running.

To verify LDAP mappings:

- 1 Establish a Novell Client connection to the NDS or eDirectory server where you want to run LDAP compatibility mode.
- 2 From that client connection, launch ConsoleOne.
- 3 Select the LDAP Group object for your server.

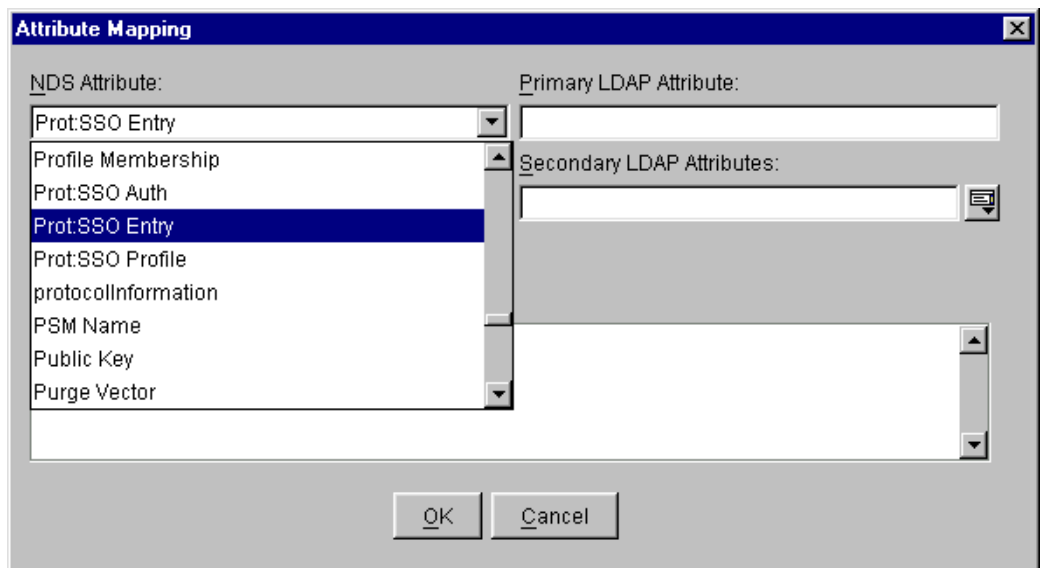


- 4 Display the Attribute Mappings tab by clicking Properties > Attribute Mappings.



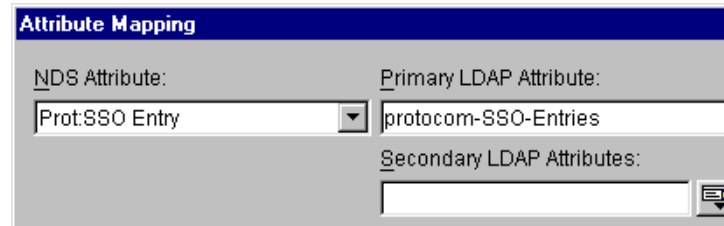
If you can't locate this tab, you must install the LDAP snap-in to ConsoleOne. Download the snap-in from <http://download.novell.com>. Select ConsoleOne Snap-ins > On NetWare > NDS eDirectory 8.6.2 Snap-in.

- 5 Click Add.
- 6 From the NDS Attribute drop-down list, select the Prot:SSO Entry attribute.



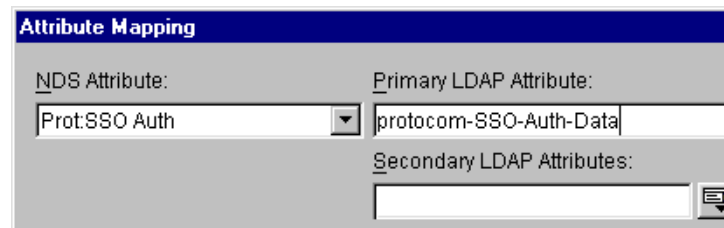
If the Prot:SSO Entry attribute is unavailable, run NDSSchema.exe or LDAPSchema.exe. These files are in the securelogin\tools directory.

- 7 Map the Prot:SSO Entry attribute to protocom-SSO-Entries, as indicated in the following figure.



The screenshot shows the 'Attribute Mapping' dialog box. It has a title bar 'Attribute Mapping' in a blue header. Below the header, there are three fields: 'NDS Attribute:' with a dropdown menu showing 'Prot:SSO Entry', 'Primary LDAP Attribute:' with a text box containing 'protocom-SSO-Entries', and 'Secondary LDAP Attributes:' with an empty text box and a small icon to its right.

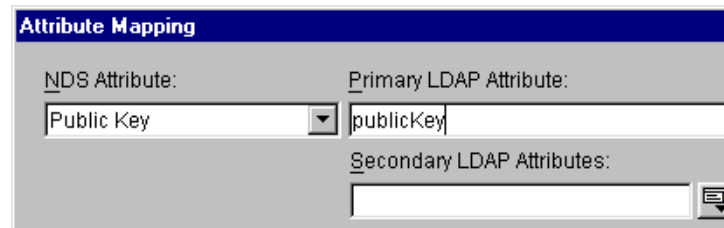
- 8 Similarly, map the other Prot:SSO attributes to corresponding protocom-SSO attributes.



The screenshot shows the 'Attribute Mapping' dialog box. It has a title bar 'Attribute Mapping' in a blue header. Below the header, there are three fields: 'NDS Attribute:' with a dropdown menu showing 'Prot:SSO Auth', 'Primary LDAP Attribute:' with a text box containing 'protocom-SSO-Auth-Data', and 'Secondary LDAP Attributes:' with an empty text box and a small icon to its right.

For a list of attributes and corresponding mappings, see [“Extending the LDAP Directory Schema” on page 26](#).

- 9 Similarly, map the Public Key attribute to publicKey.



The screenshot shows the 'Attribute Mapping' dialog box. It has a title bar 'Attribute Mapping' in a blue header. Below the header, there are three fields: 'NDS Attribute:' with a dropdown menu showing 'Public Key', 'Primary LDAP Attribute:' with a text box containing 'publicKey', and 'Secondary LDAP Attributes:' with an empty text box and a small icon to its right.

- 10 Click Apply, then click Close.

- 11 Refresh the LDAP server.

If you are using ConsoleOne, right-click the LDAP Server object, click Properties, then click Refresh NLDAP Server Now.

If you are using Novell iManager, click LDAP Management, click LDAP Overview, click View LDAP Servers, select the LDAP server, then click Refresh.

Verifying the Active Directory Schema

You might need to verify that the Active Directory schema has been extended.

Adding Administrative Tools for Active Directory

The following procedures assume that you are logged in as an administrator with the required permissions to manage the schema.

- 1** Click Start > Settings > Control Panel > Add/Remove Programs.
- 2** Click Windows 2000 Administration Tools > Change > Next.
- 3** Click Install All Administrative Tools > Next.
- 4** After components and files are installed, click Finish > Close.

Starting the Active Directory Schema Plug-In

You manage Active Directory from a Windows NT or Windows 2000 server. Therefore, you must install SecureLogin on a server.

The Active Directory Schema plug-in is a Microsoft Management Console (MMC) tool. Because schema management is not frequently performed, there is no saved Schema console or Administrative Tool on the Administrative Tools menu. You must manually load the Schema Manager into MMC.

Run the following procedure on the domain controller that contains the schema:

- 1** Click Start > Run.
- 2** In the Open box, type **MMC . EXE**, then click OK.
- 3** From the Console drop-down list, click Add/Remove Snap-In, then click Add.
- 4** Click Active Directory Schema, then click Add.
- 5** Click Active Directory Users and Computers, then click Add.
- 6** Click Close, then click OK.
- 7** Save the MMC containing the schema snap-in.
 - 7a** From the Console drop-down list, click Save As.
 - 7b** Type a name for the saved console (for example, schema.msc).
 - 7c** Click Save.

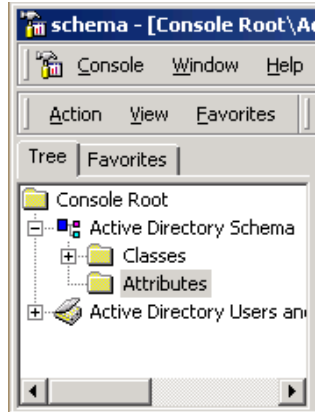
Verifying Attributes in the Active Directory Schema

- 1** Close and restart MMC.

After extending the schema, you must close and restart MMC before you can verify that the schema has been extended

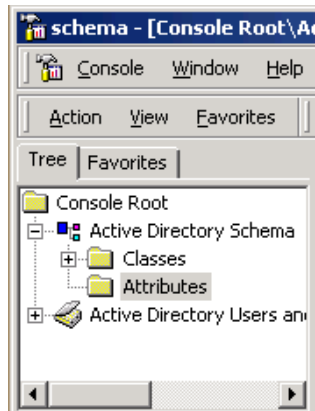
- 2** In the MMC tool, navigate to the Attributes folder.

The following figure illustrates the Attributes folder:

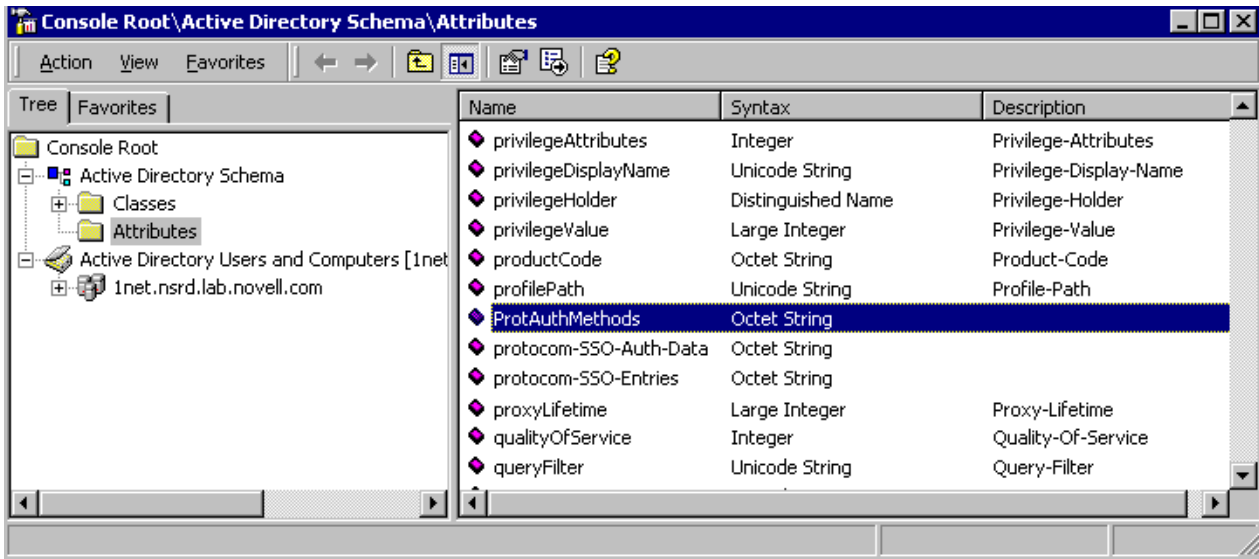


- 3** In the Console1 window, click Console > Add/Remove Snapin (Ctrl+M).
- 4** Click Add, select Schema Management, click Add, then click OK.
- 5** At the root of the directory, browse to the attributes and verify that all six Protocom attributes are in the directory.

The following figure illustrates the Attributes folder:



- 6** Identify the six attributes.
 Ensure that protocom-SSO-Auth-Data, protocom-SSO-Entries, protocom-SSO Entries-Checksum, protocom-SSO-Profiles, protocom-SSO-SecurityPrefs, and protocom-SSO-Security-Prefs-Checksum appear in the ADS list of attributes. The following figure illustrates these attributes in the extended schema:



If the attributes don't appear, rerun adsschema.exe.

If ?sysuser(system) and ?syspassword(system) Are Unavailable

If you use the Novell Client but turn off NMAS after installing SecureLogin 3.51.2, and then update your password, ?sysuser(system) and ?syspassword(system) variables aren't available.

To resolve this issue, get a TID from Novell Technical Support. This TID does the following:

- ◆ Installs slinac.dll on your client workstation
- ◆ Adds a registry setting, so that the workstation can register slinac.dll as a login extension to the Novell client.

The TID provides you with username and password variables for use with internal scripts and the passthrough to Citrix.

Useful TIDs

Issue	TID
Registry keys and values used by Secure Workstation	10087272 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10087272.htm)
Registry settings for the Quick Login/Logout Interface	10087273 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10087273.htm)
Configuring SecureLogin for 16-bit Windows applications	10082829 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10082829.htm)
Upgrading from vGO NSSO	2966500 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966500.htm)
Setting up and configuring an advanced generic emulator	10086962 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10086962.htm)

Issue	TID
Script to configure SecureLogin for Citrix	10089667 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10089667.htm)

A Lotus Notes

This section provides information on migrating Lotus* Notes* from Novell® SecureLogin 3.0.4 or later to SecureLogin 3.51.2.

Migrating Lotus Notes

- 1** Run the Novell SecureLogin 3.51.2 installation.

If Lotus Notes is installed on the workstation, the installation program detects that it is installed.

- 2** Select the Lotus Notes option.

The installation program does the following:

- ◆ Copies nslasst.dll to the path where Lotus Notes has been installed, usually .../Lotus/Notes.
- ◆ Updates the notes.ini file.
- ◆ Deletes the existing pronotes.dll file.

- 3** From Add Applications in SecureLogin, select the Lotus Notes script from the list of prebuilt scripts.

This prebuilt script automatically generates the nlnotes.exe application entry. When you run SecureLogin 3.51.2, a flag is set once migration has completed. The flag is a Complete value, which is set in a Migration key in the newly created User ID for each Lotus Notes user.

You can view this flag in Manage Logins from the SecureLogin icon on the system tray.

The nslasst.dll file provides SecureLogin with user data from Lotus Notes. The nslasst.dll is only for migration. After migration has taken place, nslasst.dll is not needed for SecureLogin to provide single sign-on to Lotus Notes. If you want to, you can delete nslasst.dll after migration. Single sign-on is provided via the prebuilt script.

