AUTHORIZED DOCUMENTATION

Installation Guide

Novell® SecureLogin

6.1 SP1

June, 2009

www.novell.com

Legal Notices

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

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

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

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

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

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This document provides the following information:

Audience

This guide is intended for:

- Network Administrators
- Systems Administrators
- IT Support Staff

Feedback

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

Documentation Updates

For the most recent version of the *Novell SecureLogin Installation Guide*, visit the Novell Documentation Web site. (http://www.novell.com/documentation/securelogin61/index.html)

Additional Documentation

The *Installation Guide* is part of documentation set for Novell SecureLogin 6.1 SP1.

Other documents part of this release are:

- *Novell SecureLogin 6.1 SP1 Administration Guide*

- *Novell SecureLogin 6.1 SP1 Application Definition Guide*
- *Novell SecureLogin 6.1 SP1 Citrix and Terminal Services Guide*
- *Novell SecureLogin 6.1 SP1 User Guide*
- Quick Start: "NMAS Login Method and Login ID Snap-In for pcProx"
- Readme. Available online at the Novell Documentation Web site. (http://www.novell.com/documentation/securelogin61/index.html)

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.

Overview

1

Novell® SecureLogin is an enterprise Single Sign-on (eSSO) product. It eliminates the necessity for users to remember multiple usernames and passwords. It stores usernames and passwords and automatically retrieves them for users when required.

Novell SecureLogin consists of multiple, integrated security systems that provide authentication and single sign-on to networks and applications.

This release of Novell SecureLogin runs on Microsoft* Vista* 32-bit as well as Windows 2000 and XP so, migrating to Vista is transparent to users and the deployment is easy for administrators.

Preparing to Install Novell SecureLogin

2

This section consists information on the following:

2.1 Support for Non-English Languages

In this version, the approach for language support is different from the previous versions of Novell SecureLogin. In the earlier versions, the user was prompted to choose a language for the setup during the installation.

In this version of Novell SecureLogin, this option is not offered, and the installation uses English throughout.

However, you can use a command line option to install in non-English languages.

1 At the command line, specify the following command:

```
msiexec.exe /i "Novell SecureLogin.msi" TRANSFORMS=<lang-code>.mst
```

<lang-code> denotes a specific language.

- 1041 represents the Japanese language
- 1036 represents the French language
- 1046 represents the Brazilian language
- 1031 represents the German language
- 1034 represents the Spanish language

2.2 Support on Microsoft Windows Vista

Novell recognizes Microsoft Windows Vista as a Citrix or Terminal Services client.

Citrix and Terminal Services support is always installed when Novell SecureLogin is deployed to a Vista client or workstation and the *Install Citrix and terminal services support* option is not displayed.

Microsoft Windows Vista is not supported as a Citrix or Terminal Services server.

2.3 Requirements for Microsoft Windows 2003 Server

The following information applies to the configuration of a server in a Microsoft Windows Server* 2003 operating system environment.

2.3.1 Internet Explorer Enhanced Security

By default, Microsoft Windows 2003 server installs the Internet Explorer Enhanced Security Configuration, which is designed to decrease the exposure of enterprise servers to potential attacks that might occur through the Web content and application scripts.

When you use Internet Explorer, this means that some Web sites might not display or perform as expected when Novell SecureLogin is installed.

For more information on enhanced security, see the Microsoft Support Web site. (http://support.microsoft.com/kb/815141)

Disable the Microsoft's Internet Explorer Enhanced Security Configuration before deploying Novell SecureLogin.

You can remove the Internet Explorer Enhanced Security Configuration through *Start > Control Panel > Add/Remove Windows Component*.

2.4 Required Rights for Installing Novell SecureLogin

The `Novell SecureLogin.msi` is a per-machine installer package. A per-machine installation can be done only by a privileged user or an administrator.

A privileged user is a regular user who has belongs to the administrator group or, a user who has administrator privileges.

NOTE: In a Microsoft Windows XP environment, only an administrator can install Novell SecureLogin.

2.5 Supported Platforms

Novell SecureLogin supports the following platforms:

- Section 2.5.1, "Servers," on page 14
- Section 2.5.2, "Client," on page 15
- Section 2.5.3, "Browsers," on page 15

2.5.1 Servers

- eDirectory™ 8.8.5, 8.8.4, and 8.8.3

  Without SecretStore, Novell SecureLogin runs against eDirectory on any platform.
- Microsoft* Windows 2000 Server, Terminal Server, or Advanced Server with Active

Directory*.

- Microsoft Windows 2003 Server or Terminal Server with Active Directory.
- Any server running LDAP-compliant directories.

2.5.2 Client

- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows 2000

2.5.3 Browsers

- Internet Explorer 7.0 and 8.0
- Mozilla* Firefox* 2.0 and 3.0

Novell SecureLogin and Mozilla Firefox

If a user wishes to continue using Mozilla Firefox 1.0.*x* or earlier, then the `SLoMoz.xpi` extension that is installed with Novell SecureLogin must be uninstalled and the `SLoMoz` extension available with the Novell SecureLogin product installer must be reinstalled.

Installing in Novell eDirectory Environments

3

This section provides information on the following:

WARNING: If you are upgrading and are already using SecretStore, upgrade SecretStore on your server to version 3.3.5 before installing SecureLogin 6.1 Otherwise, secrets might be lost.

3.1 Prerequisites

3.1.1 NICI

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

- eDirectory LDAP protocol
- The SecretStore client feature
- The NMAS™ client feature

If you are using NMAS, install NICI manually before installing NMAS Client.

3.1.2 NMAS

Novell SecureLogin requires NMAS Client 3.4.

- When installing Novell SecureLogin in eDirectory mode, install `NMASClient` manually before installing Novell SecureLogin.

- For installing on Vista, NMAS is available in `\Nmas\NmasClient\Vista-x86\nmasclient_setup_v32.exe` that is found as part of your Novell SecureLogin installer package.
- For installing on Windows XP, 2000, and 2003, NMAS is available in `\Nmas\NmasClient\win32\nmasclient_setup.exe` that is found as part of your Novell SecureLogin installer package.

NMAS is not uninstalled when you uninstall Novell SecureLogin.

3.1.3 Novell SecureLogin and SecretStore

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

3.1.4 Using the SecretStore Client

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

To determine whether SecretStore is installed on a NetWare server:

1. At the server console, type `nwconfig`, then press Enter.
2. Select *Product Options* > *View/Configure/Remove Installed Products*, then press Enter.
3. Scroll to find the SecretStore product (for example, SS 3.3.5 Novell SecretStore).

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

If SecretStore is not installed, see “Installing SecretStore” in the SecretStore 3.4 Administration Guide. (http://www.novell.com/documentation/secretstore34/index.html)

To install the SecretStore client:

1. Upgrade SecretStore on the server.

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

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

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

3.1.5 Extending the eDirectory Schema

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

To extend the schema of a given tree, you must have sufficient rights over the [root] of the tree. In addition, make sure that you have Novell Client 4.91 or later installed on your machine.

1. Run `ndsschema.exe`.

   Typically, this file is in the `securelogin\tools` directory. However, if you unzipped it to the `Temp` directory on a Windows 2000 workstation, you might need to display 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

   If you use iManager to administer Novell SecureLogin, you must also extend the LDAP Schema. For information on extending the LDAP schema, see Section 4.2.2, “Extending The LDAP Directory Schema,” on page 35.

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

3. At the prompt, define a context where you want the User objects' rights to be updated, allowing users access to their own single sign-on credentials.

   If you do not specify a context, rights begin at the root of the eDirectory tree.

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

4. (Conditional) Grant rights to local cache directories.

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

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

     or,

     (`c:\users\<usersv2slc>\applicationdata` on a Windows Vista machine.

The default location is the user's profile directory or the user's application 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.

If user selects the non-default directory to store the cache, the `SecureLogin\cache` is appended to the specified path.

- During the installation, specify a path to a location that the user has rights to (for example, the user's documents folder).

3.2 Installing in an eDirectory Environment

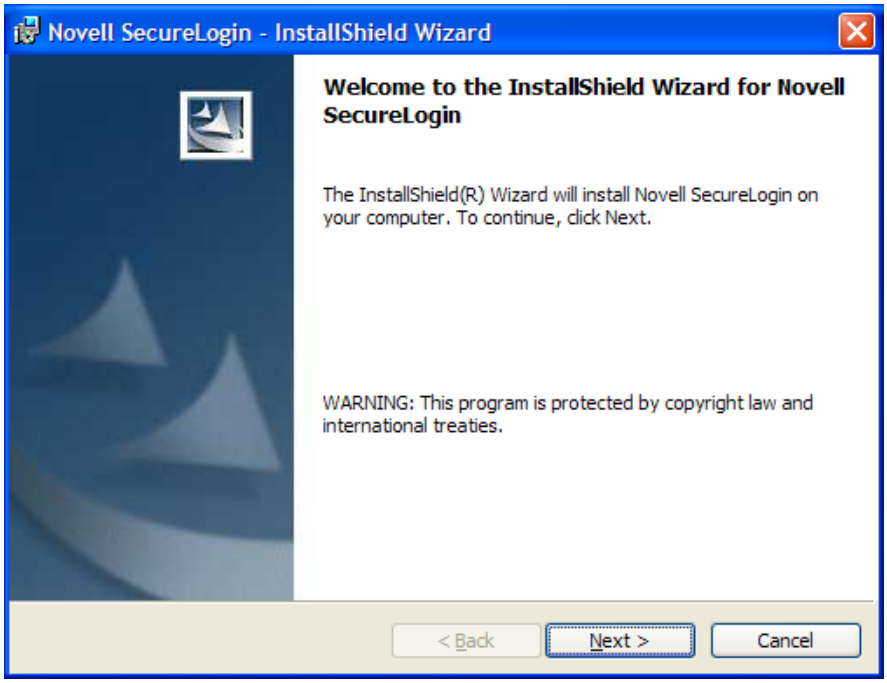
The Novell eDirectory option installs Novell SecureLogin onto networks that are running eDirectory. This option provides secure, centralized storage of user login data by performing encryption once on the workstation before the data is saved to eDirectory.

- Section 3.2.1, "Using the Complete Option to Install," on page 20
- Section 3.2.2, "Using the Custom Option for Novell eDirectory," on page 29

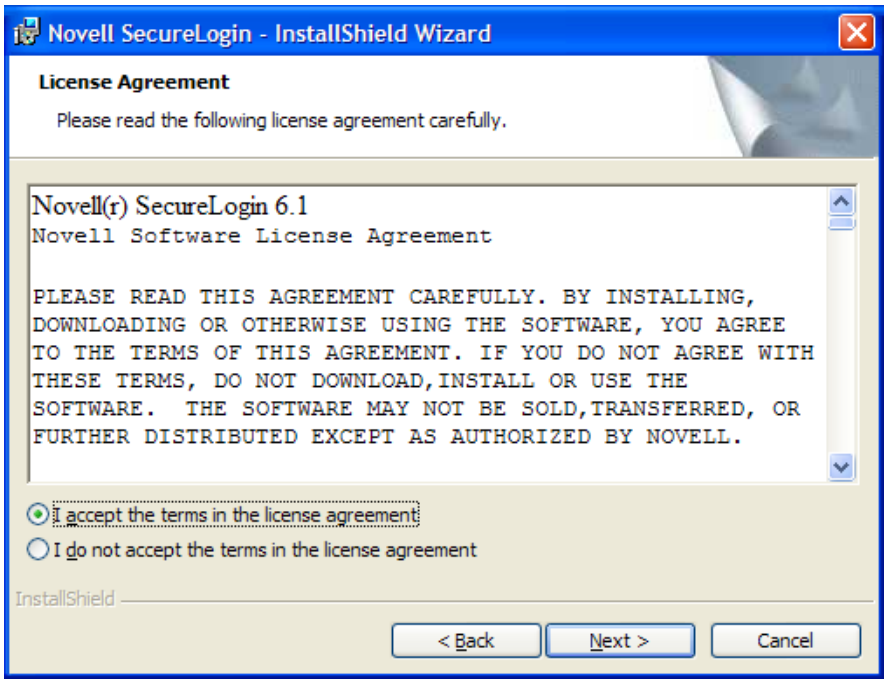
3.2.1 Using the Complete Option to Install

The *Complete* options uses the default values and install Novell SecureLogin in `c:\program files\novell\securelogin`. For options available through the *Custom* option, see Section 3.2.2, "Using the Custom Option for Novell eDirectory," on page 29.

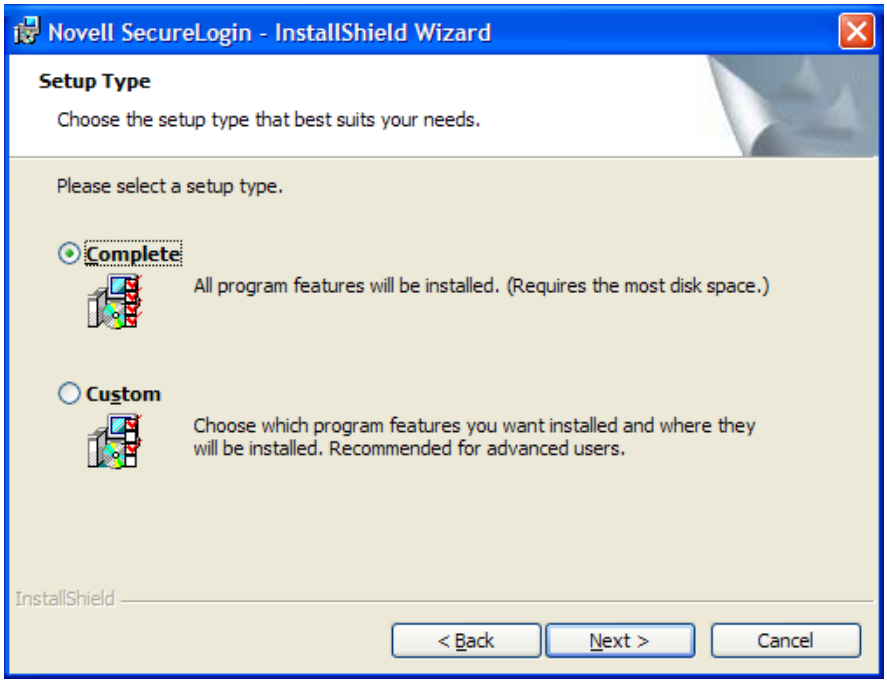
1. Run `Novell SecureLogin.msi`, found in the `Securelogin\Client` directory of the installer package.



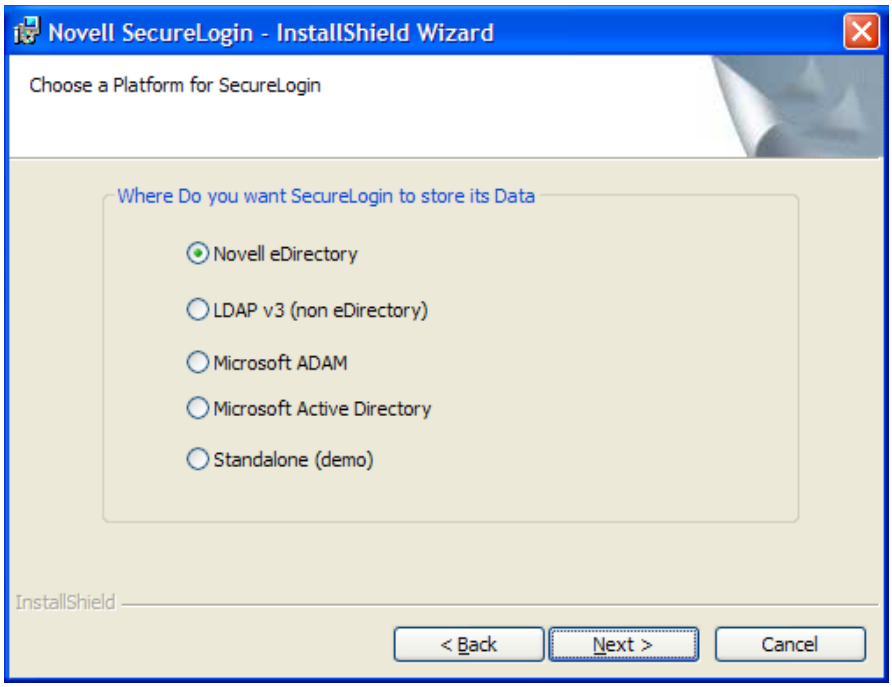
2. Accept the license agreement, then click *Next*.



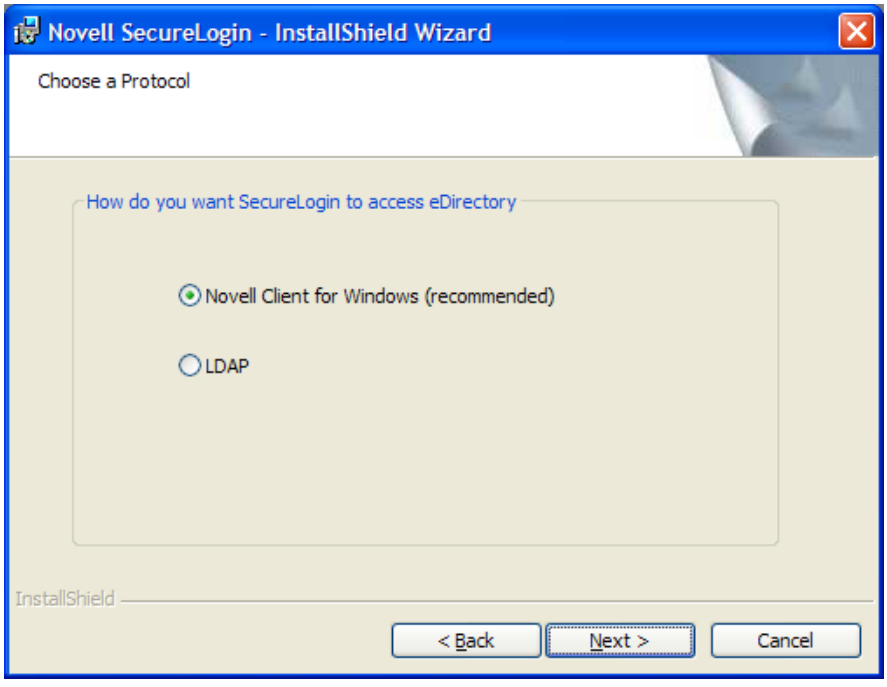
3 Select *Complete*, then click *Next*.



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



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



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

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

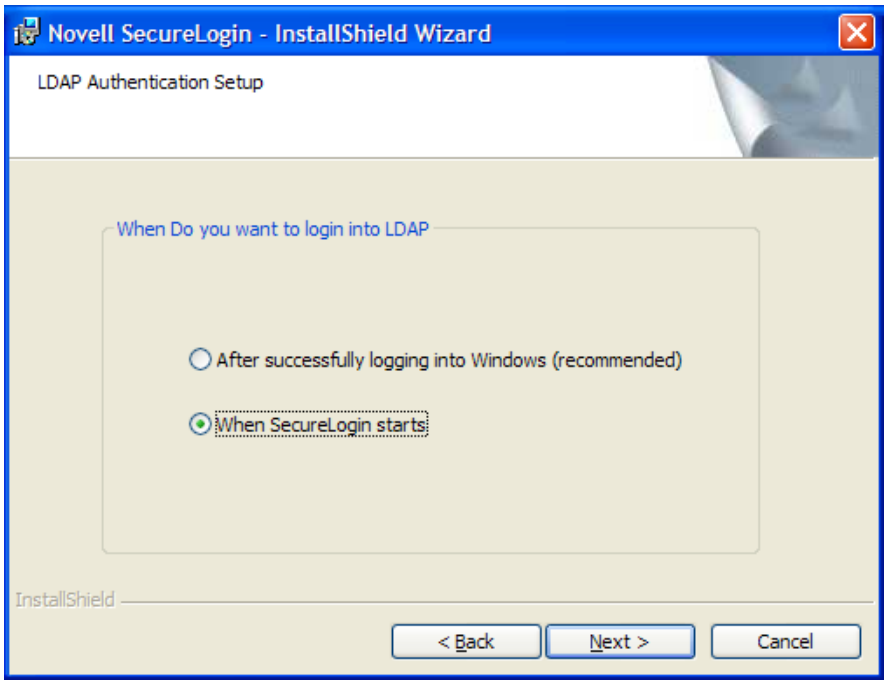
In the complete mode of installation, the install takes the default values and proceeds with the installation. If the Novell Client is installed, the default Account association is Novell Client association. If you do not have not Novell Client installed, the default Account association is Windows association.

However, if you want to associate the account association to Novell Client, change the registry setting in `hklm/software/novell/login/ldap` as follows:

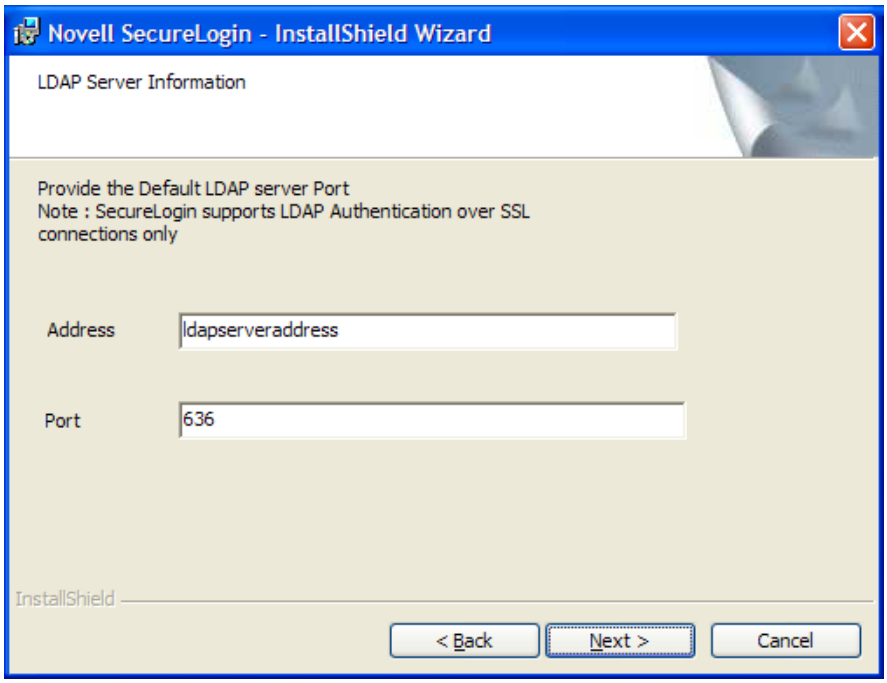
`DoNTAssoc REG_SZ` *1*

`DoClient32Assoc REG_SZ` *0*

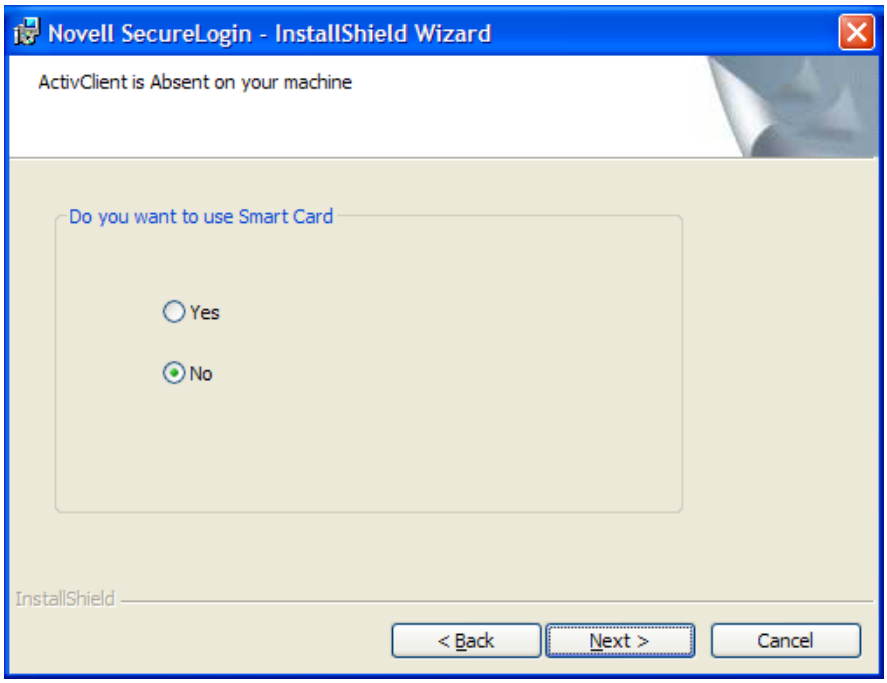
6 If you have selected LDAP, choose when you want to log in to LDAP.



7 Specify the LDAP server information.



8 (Optional) If you do not want to use smart card, select *No,* click *Next,* then continue with Step 10.

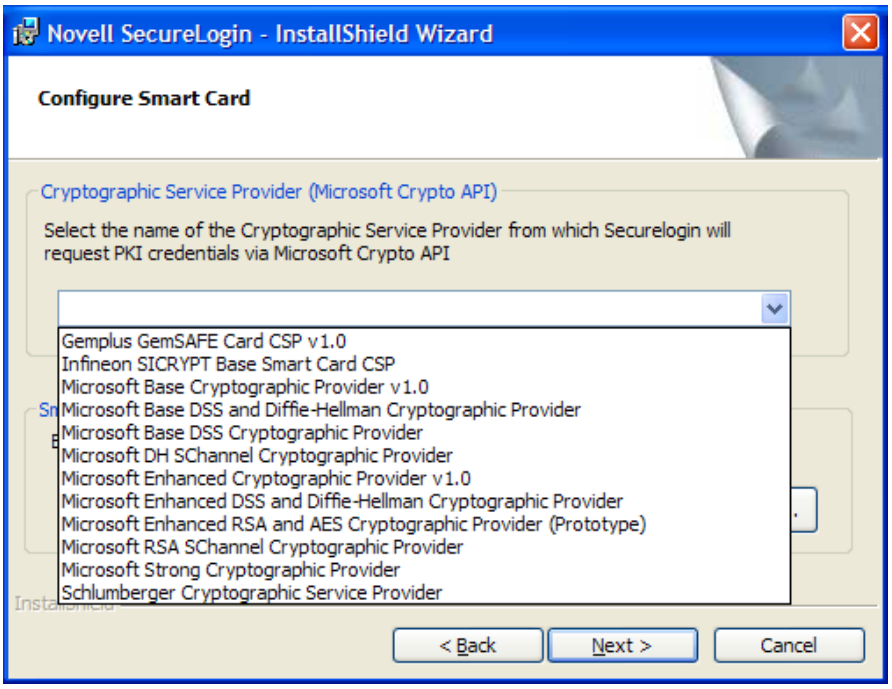


9 (Optional) If you want to use smart card and if ActiveClient is detected in your system, select *Yes* > click *Next,* then continue with Step 10.

10 (Conditional) If you want to use smart card and if ActiveClient is not detected in your system:

10a Select *Yes,* then click *Next.*

10b Select a cryptographic service provider from which Novell SecureLogin requests PKI credentials through a Microsoft Crypto API.



10c Select a PKCS#11 compatible library required for accessing the smart card, then click *Next*.

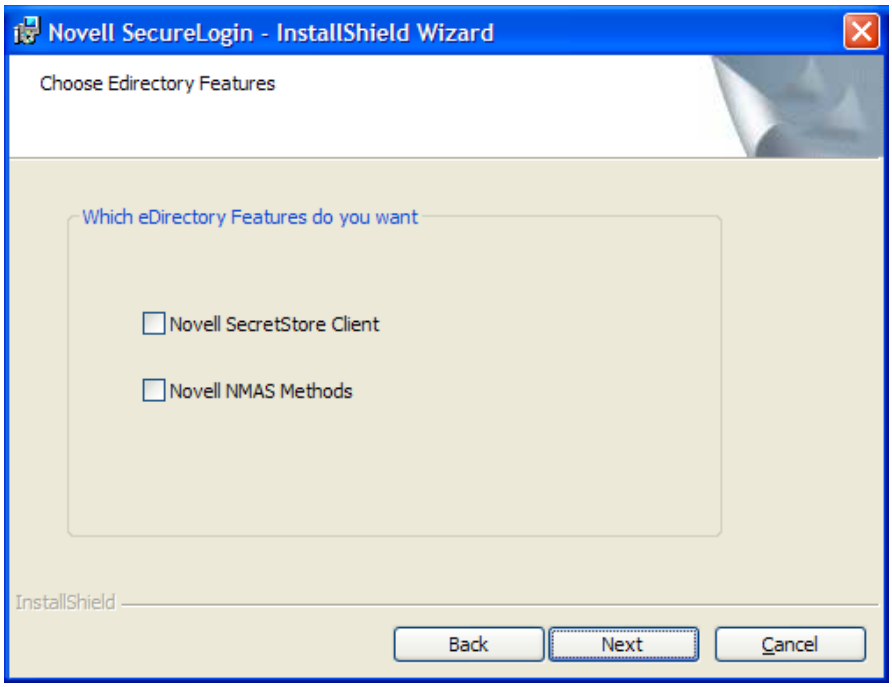
NOTE: This specifies the location of the Cryptographic Token Interface installed as part of the smart card vendor's software. These API files are used by Novell SecureLogin to communicate with the smart card.

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

---

11 Select the eDirectory features that you want to release, then click *Next*.

You can select both the features.



IMPORTANT: Install the `NMASClient` manually.

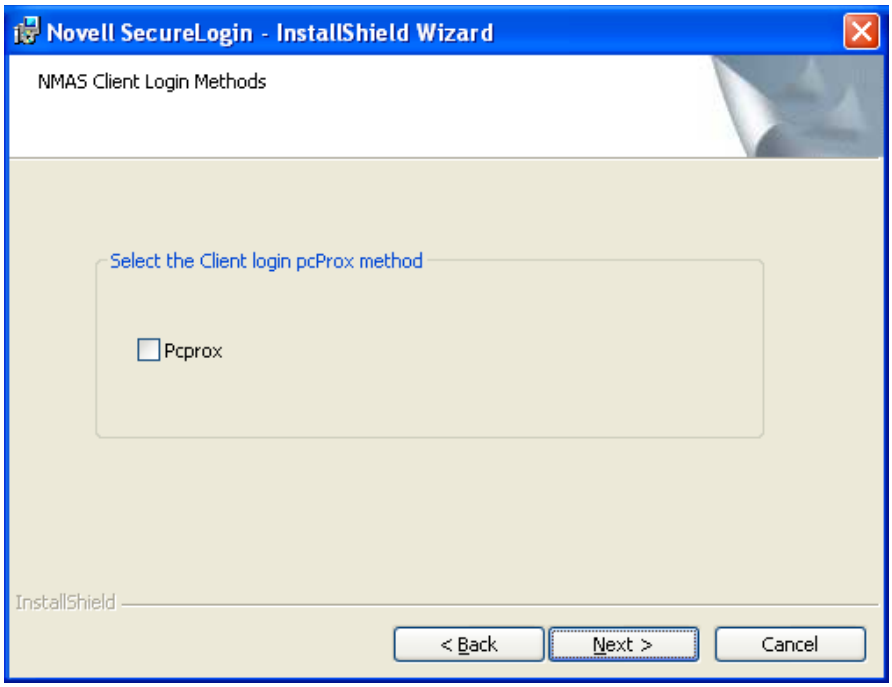
- For installing on Vista, NMAS is available in `\Nmas\NmasClient\Vista-x86\nmasclient_setup_v32` that is available as part of the Novell SecureLogin installer package.
- For installing on Windows XP, 2000, and 2003, NMAS is available in `\Nmas\NmasClient\win32\nmasclient_setup_v32` that is available as part of the Novell SecureLogin installer package.
- Install the Challenge Response before installing Novell SecureLogin. To install Challenge Response, run setup from `\NMAS\NMASMethods\ChallengeResponse` that is available as part of the Novell SecureLogin installer package.

The user still needs to install NMASClient manually, select the NMAS Methods like pcProx, Challenge Response, and Secure Workstation, and proceed with the installation.

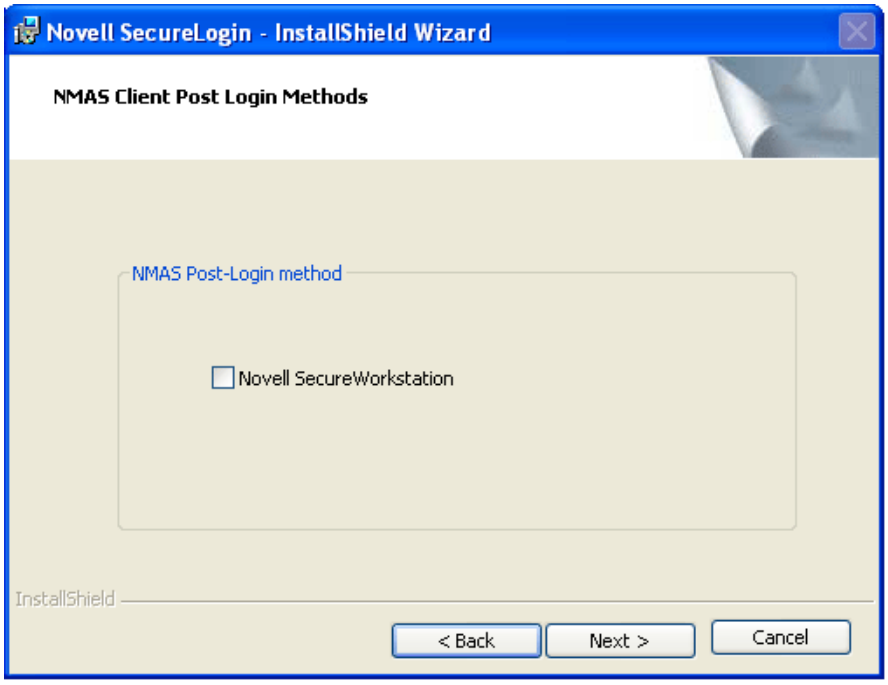
Select Novell SecretStore only if SecretStore is installed on a server. For more information on SecretStore, see "Installing SecretStore" in the *SecretStore 3.4 Administration Guide*. (http://www.novell.com/documentation/secretstore34/index.html)

12 If you select *Novell NMAS Methods* and if NMAS is available, the NMAS Client Login Methods dialog box is displayed.

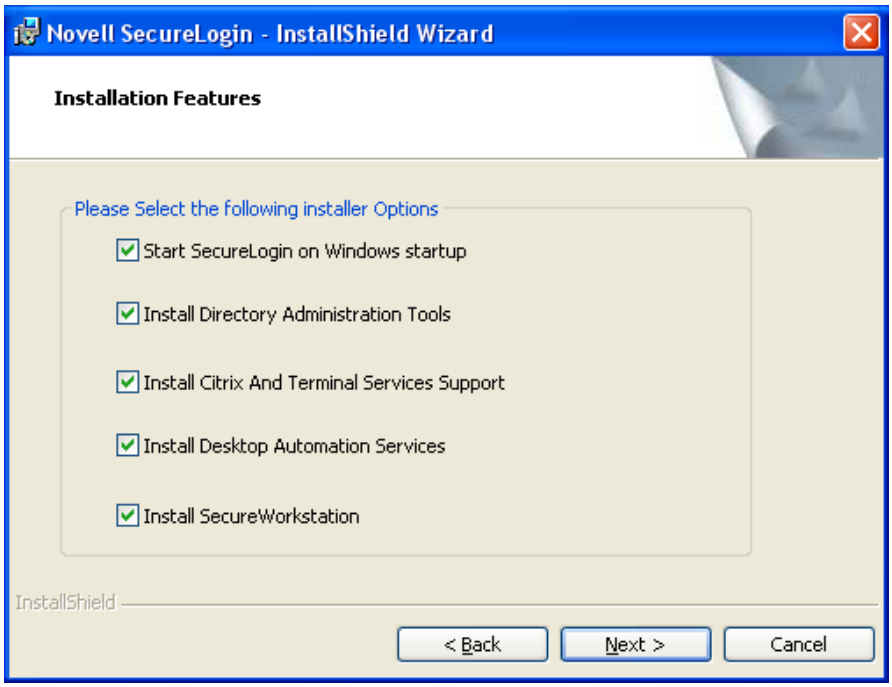
Select *pcProx* , then click *Next*. The NMAS Client Post Login Methods dialog box is displayed.



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



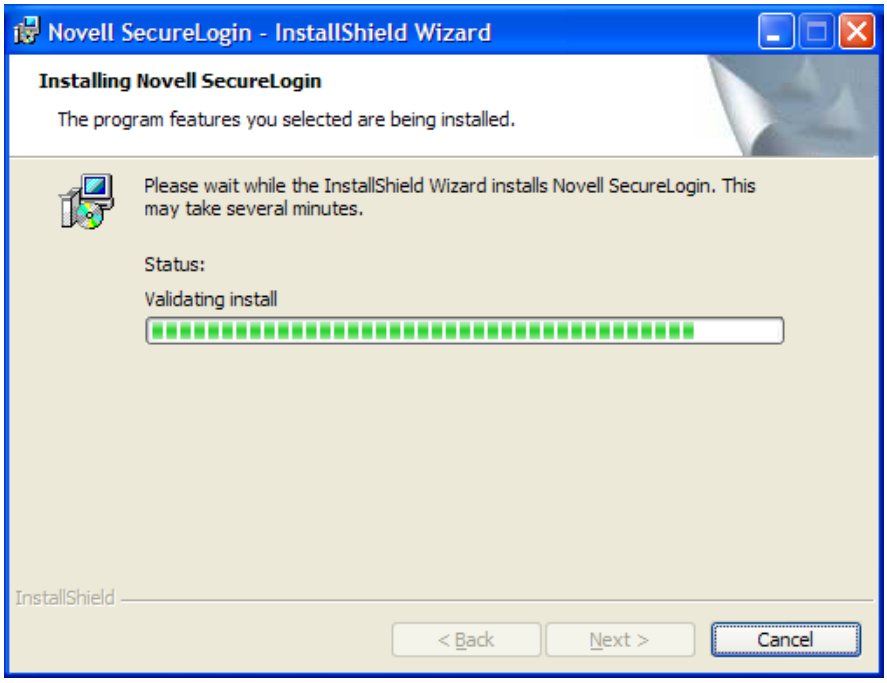
14 Select the installation features. Click *Next*.



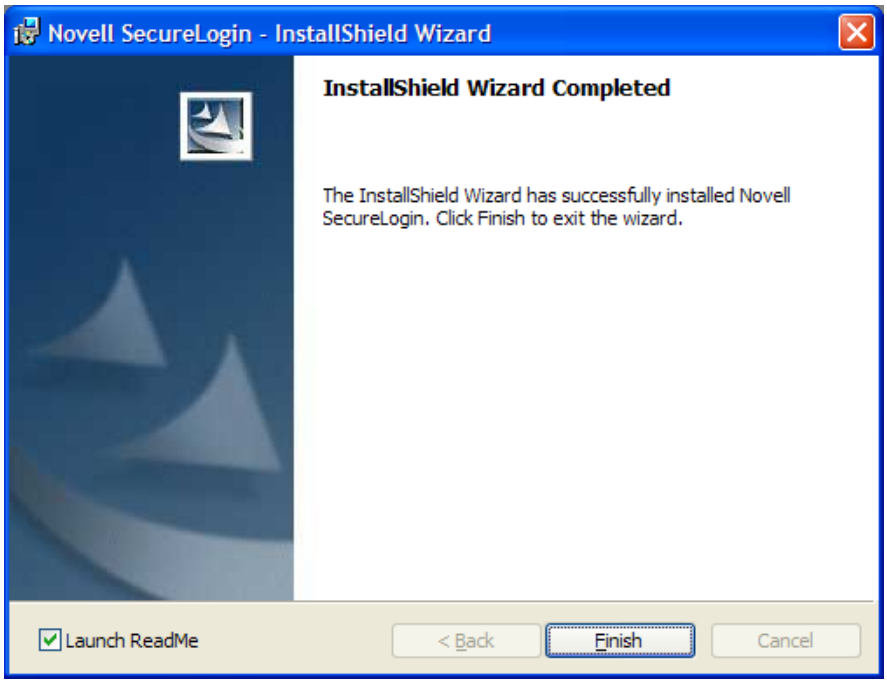
The Install SecureWorkstation option is available on this page if you have selected the option on the previous page.

15 Click *Next*. The Ready to Install the Program dialog box is displayed.

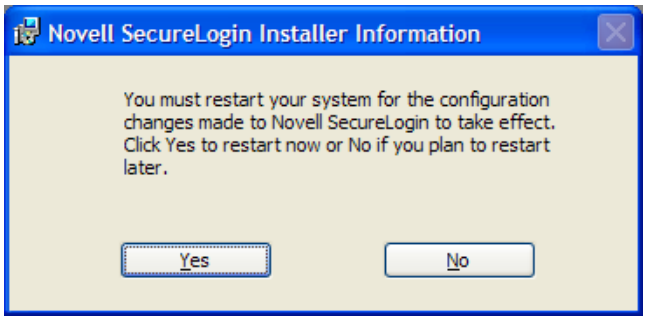
16 Click *Install*.



17 Click *Finish*. By default, the *Launch ReadMe* option is selected.



18 You are prompted to restart your system. Select *Yes* to restart the system so Novell SecureLogin can take effect.



3.2.2 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 Novell SecureLogin files should be stored.

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

- Specify a path for the Novell SecureLogin's local cache.

  The user profile directory is the default path.

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

  User profiles for Windows Vista are in `c:\users` *`username`*.

- Select Novell SecureLogin components (for example, Citrix and Terminal support) and SecretStore client components (for example, SecretStore Status).

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

3.3 Installing Administrative Tools for eDirectory

To administer Novell SecureLogin for eDirectory, use the administrative tool that you typically use to manage the server.

You can use iManager. Refer to Chapter 10, "Accessing iManager and Installing the iManager Plug-In," on page 145.

You can also use `slmanager.exe`. This utility is found in the `\securelogin\tools` directory that is available as part of the Novell SecureLogin installer package.

3.4 Setting Up a Passphrase

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

During installation, the passphrase security is enabled to enforce passphrase setup during the initial login. You can disable the passphrase policy by deselecting *Use Passphrase Policy* option in the *Advanced Settings* pane of the Administrative Management utility.

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

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

WARNING: Remember the passphrase answer. If you forget the answer, it cannot be accessed.

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

After installing Novell SecureLogin successfully, when you attempt to log in to the workstation, you are prompted to set your passphrase question and answer.

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

NOTE: When you upgrade, SecureLogin stores all users data, including the user's passphrase question and response, from the previous version, so you do not need to re-create the passphrase.

You can create passphrase questions for users to select from in a directory environment; however, because you are the first SecureLogin user, you must create your own passphrase question.

3.5 Deploying Novell SecureLogin in Shared Workstations

If Novell SecureLogin in deployed in a shared workstation where more than one users share the local credentials, users must either use Secure Workstation or DAS to close all programs and log out of the network.

The option is mandated because,

- If a user who has logged in to Novell SecureLogin in Novell Client™ mode in Microsoft Windows Vista or Microsoft Windows XP or in LDAP mode (in Microsoft Windows Vista) locks the workstation and later tries to unlock using the workstation credentials, Novell SecureLogin fails to log off the directory user.

  However, the directory user is still logged in and Novell SecureLogin continues to run. Because of this, the user who has logged in using workstation credentials has access to the directory credential store.

  In such a scenario, avoid using the workstation lock. Instead, use secure workstation or DAS to configure the workstation to close all programs and log out of the network on an inactivity timer.

Installing in an LDAP Environment

4

Lightweight Directory Access Protocol (LDAP) is an open-directory structure that provides fast access to the directory.

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

The LDAP Authentication client uses LDAP to connect to a server and securely administer enabled applications.

Novell SecureLogin supports LDAP authentication over SSL connections only.

4.1 Installation Overview

Before proceeding with installing Novell SecureLogin in LDAP mode, make sure that the following prerequisites are in place.

The instructions apply to the standard architecture of the directory managed using an administration workstation.

- Make sure that certificate services are installed and are available on your LDAP server.
- Export a copy of the server certificate server in `.der` format to a temporary location for user deployment. Ensure that the certificate filename extension is `.der`. If not, rename the file.
- Make sure that you have administrator access to the server, directory, and administration workstation.
- Uninstall all versions of Novell SecureLogin prior to version 3.5.*x* and later.
- Back up the existing directory.

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

1. Verify whether you have an exported certificate from the Enterprise Root Certificate Authority (CA) for the LDAP directory to use the Novell SecureLogin data store.

   The certificate must be in the Distinguished Encoding Rules (DER) and use `.der` as the filename extension.
2. Copy the certificate files to workstations.

3. If the application type is single sign-on enabled, install the Citrix and Terminal Services client on a user workstation prior to installing Novell SecureLogin.
4. Uninstall any previous version of Novell SecureLogin, if necessary.
5. Extend the LDAP directory schema on the server.

   For information, see Section 4.2.2, “Extending The LDAP Directory Schema,” on page 35.
6. Install or upgrade the Novell SecureLogin on the administration workstation.
7. Configure a test Novell SecureLogin environment, including enabling single sign-on and the required application, and testing it on test users.
8. Copy the test users’ Novell SecureLogin single sign-on environment for mass deployment.
9. Deploy Novell SecureLogin on users’ workstations.

IMPORTANT: If the LDAP-compliant directory extension is deployed by copying and running the `ldapschema.exe` file from another location rather, you need to copy the entire directory containing the LDAP schema and three Microsoft Foundation Class (MFC) library files to the preferred location. The LDAP schema and the three MFC files must be co-located in the same directory for the LDAP compliant directory extension instance to deploy successfully.

4.2 Installing

Installing or upgrading the Novell SecureLogin in an LDAP directory environment requires you to extend the directory with Novell SecureLogin attributes.

You can access the executable `ldapschema.exe` file that is available in the `Tools` directory of the Novell SecureLogin installer package.

As an administrator, you must manually assign read and write access to the new Novell SecureLogin attributes. Because of a wide variety of LDAP-compliant directories, Novell SecureLogin does not provide a specific tool for assigning permissions to directory attributes.

4.2.1 Extending the eDirectory Schema

If you are installing a workstation that uses Novell eDirectory, do the following:

1. From your workstation, use Novell Client to log in to a tree as a admin from your workstation.
2. Extend the eDirectory schema by running `ndsschema.exe`.

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

   The `ndsschema.exe` file is found in the `\securelogin\tools` directory of your Novell SecureLogin installer package.

4.2.2 Extending The LDAP Directory Schema

Do the following to extend the LDAP directory schemas from the server or the administration workstation.

If you have Novell SecureLogin versions 3.5 installed, you do not need to extend the Directory schemas, because the attributes are the same. However, for any new Directory objects, such as organizational units, you still need to assign rights.

In addition, if you copy the `ldapschema.exe` from the Novell SecureLogin installer package and run it from another location rather than running from the installer package, you need to copy the entire directory containing the LDAP schema files to the new location.

IMPORTANT: If you are using iManager to administer Novell SecureLogin, you must also extend the LDAP schema.

In the following example, the schema is extended on the server.

1. Log in to the server as administrator.
2. Run `ldapschema.exe`, which is found in the `\securelogin\tools` directory of the Novell SecureLogin installer package. The Novell SecureLogin - Active Directory Schema dialog box is displayed.
3. In the *LDAP Server* field, provide the IP address or the name of the LDAP server.
4. In the *Admin User* field, provide the distinguished name (DN) for the server administrator. For example,

   `CN=admin`
5. Provide the password and select the relevant directory mode (in this example, *eDirectory*), then click *Update Schema*.

   The certificate information is displayed.
6. Click *Accept*.
7. When the *Schema Extension* dialog box displayed, click *Close*.

   The schema is now extended and rights are assigned to the server and replicated to all other servers.

Extending the directory schema adds the following six Novell SecureLogin attributes:

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

IMPORTANT: These mappings are case-sensitive. Extend the LDAP schema on all servers if you want them to act as failover servers.

4.2.3 Assigning Rights to Schema Attributes

You must assign permissions to objects in the directory to store data against the new Novell SecureLogin attributes. Assign permissions to all objects that access Novell SecureLogin Assigned User Rights.

The application does not start if you have not set permission to access Novell SecureLogin schema attributes.

NOTE: LDAP implementations are varied. Therefore, Novell SecureLogin does not provide a specific tool for each variation for assigning permissions.

The following permissions are recommended for successful implementation:

- Novell SecureLogin administrators are assigned read and write access to all Novell SecureLogin attributes on all objects.
- Users are assigned read and write access to all Novell SecureLogin attributes on their user objects.
- Users are assigned read access to the Novell SecureLogin attributes on organizational units from which they need to read organizational policies or corporate settings.

4.2.4 Installing Novell SecureLogin in LDAP Mode With eDirectory

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

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

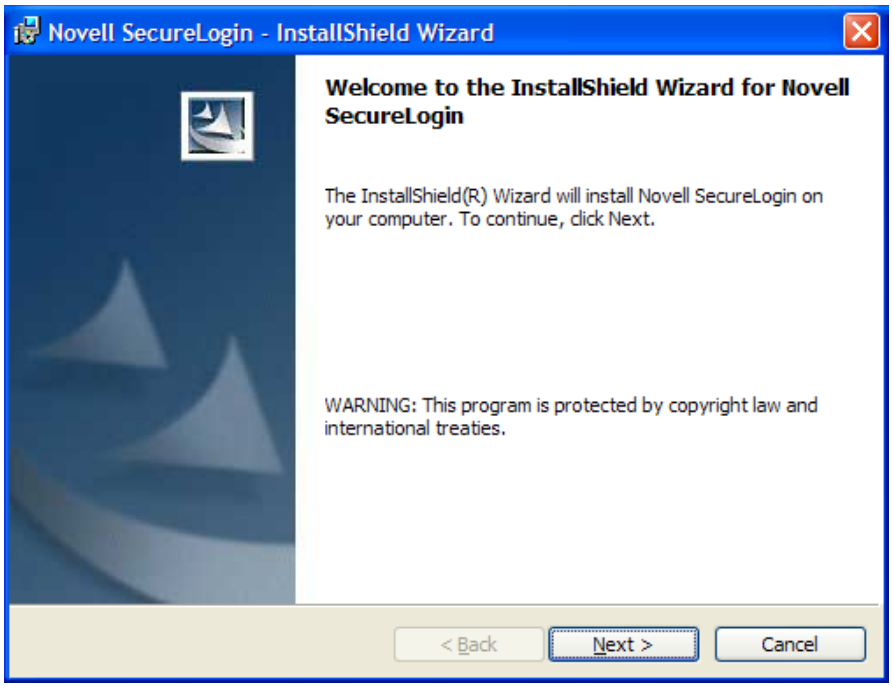
The LDAP option does not require the Novell Client for Windows. However, if Novell Client32™ is installed on the workstation, Client32 is the initial authentication or GINA. If you want LDAP authentication to be the initial authenticator, you must uninstall Novell Client32.

- "Using the Complete Option for LDAP on eDirectory" on page 36
- "Using the Custom Option for LDAP on eDirectory" on page 44

Using the Complete Option for LDAP on eDirectory

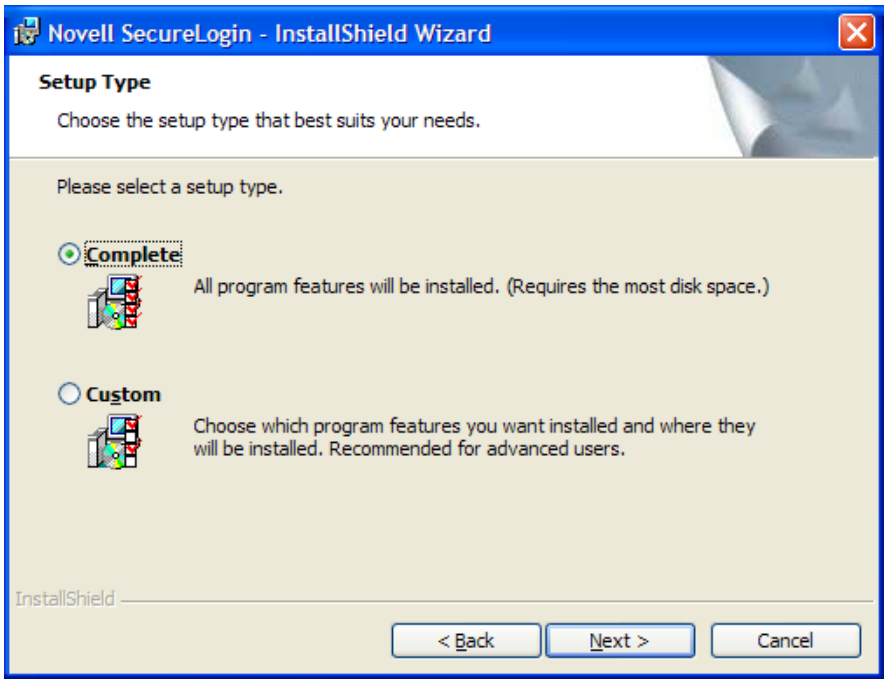
The *Complete* option uses default values and installs Novell SecureLogin in `c:\program files\novell\securelogin`. Refer to "Using the Custom Option for LDAP on eDirectory" on page 44 or options available through the *Custom* option.

1. Run `Novell SecureLogin.msi` found in the `securelogin/client` directory of the installer package.

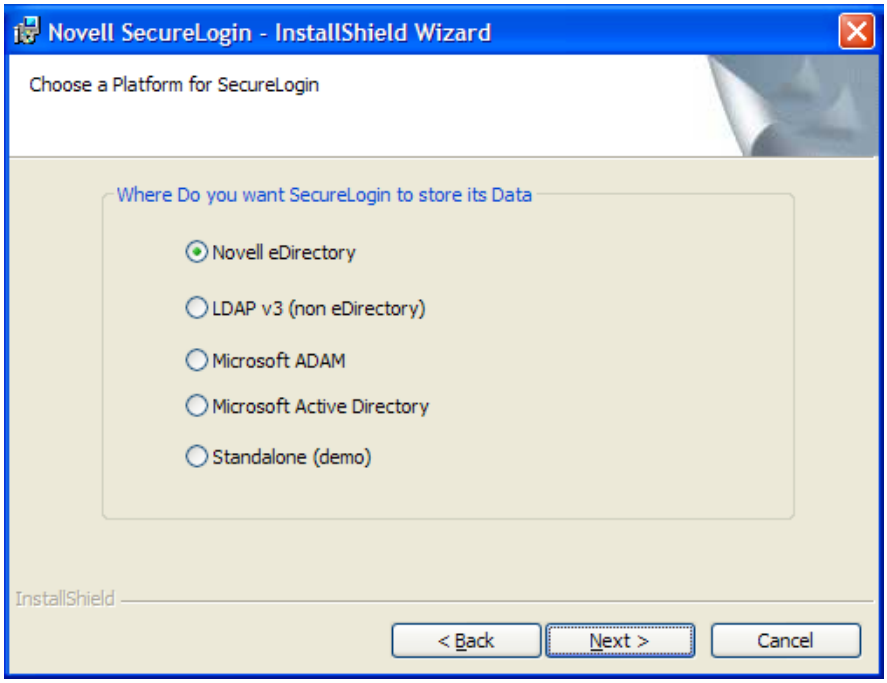


2 Accept the license agreement. Click *Next*.

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



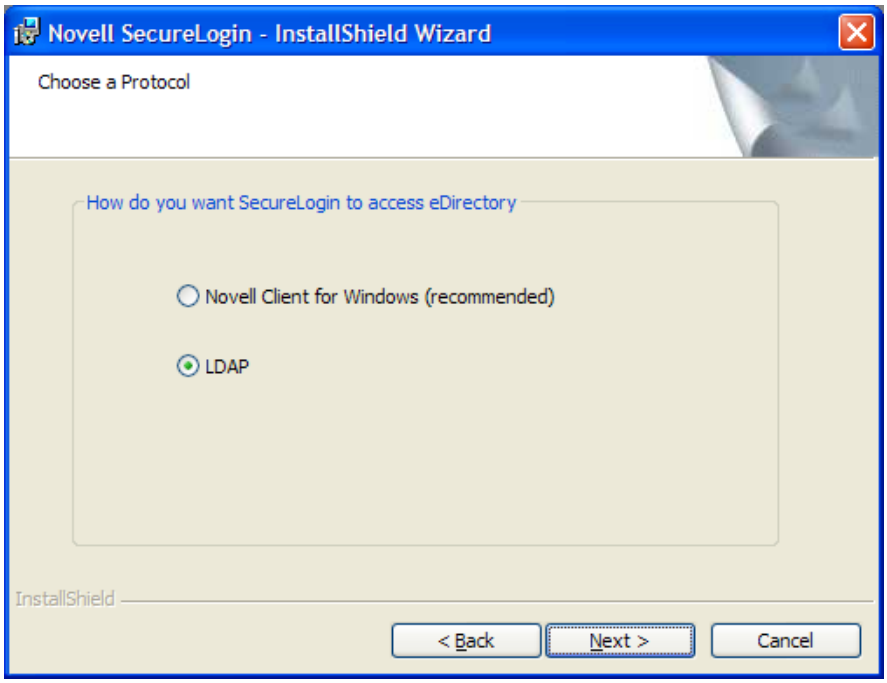
4 Select *eDirectory* as the platform where SecureLogin stores its data, then click *Next*.



5 Select *LDAP* as the protocol.

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

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



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

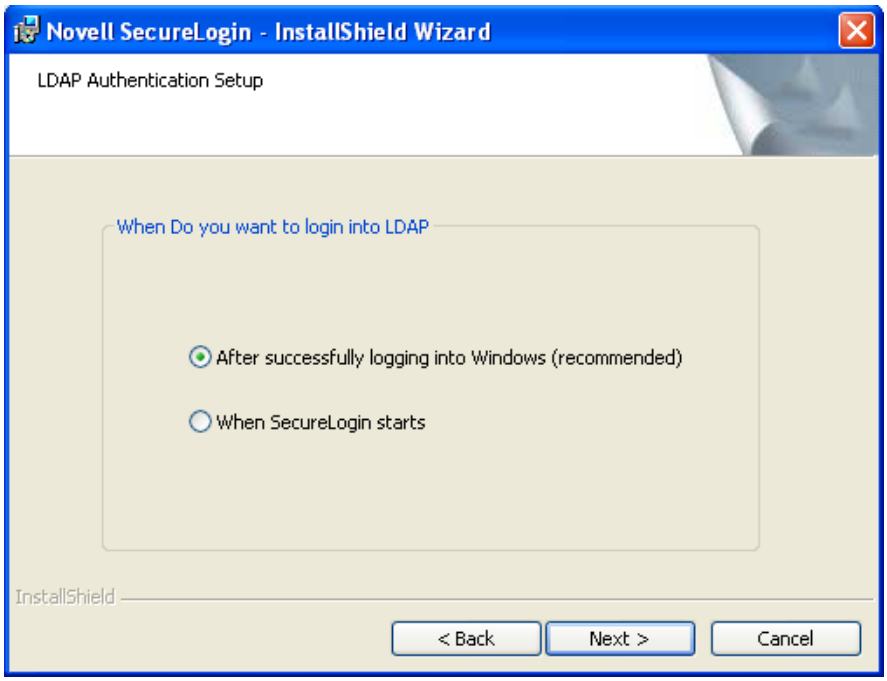
NOTE: If the workstation is running Novell Client software, the *After successfully logging Windows* option is not provided and the primary authentication is always done through the Novell Client.

In the complete mode of installation, the install takes the default values and proceeds with the installation. If the Novell Client is installed, the default Account association is Novell Client association. If you do not have not Novell Client installed, the default Account association is Windows association.

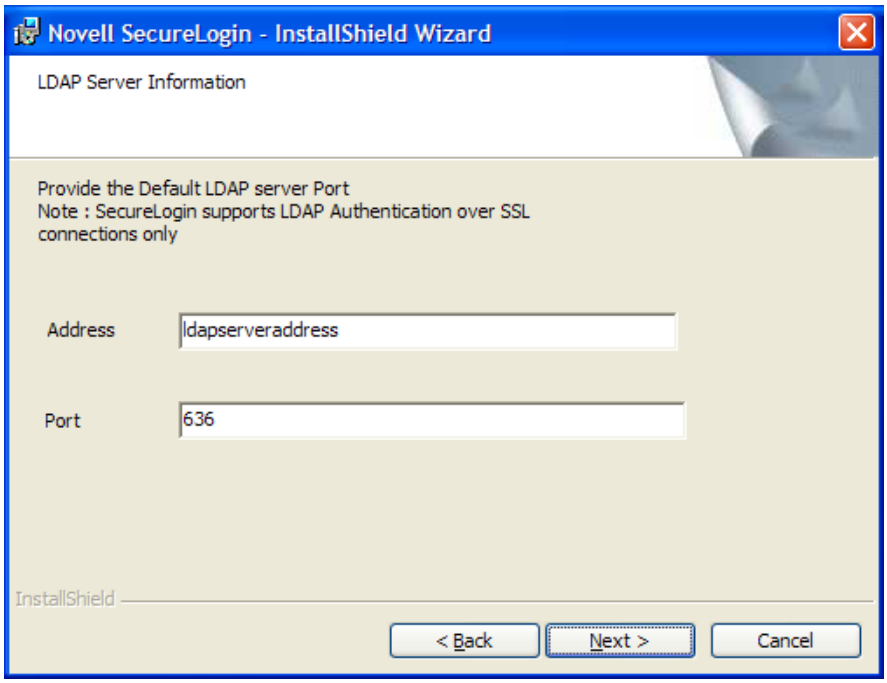
However, if you want to associate the Account association to Novell Client, change the registry setting in `hklm/software/novell/login/ldap` as follows:

`DoNTAssoc REG_SZ` *1*

`DoClient32Assoc REG_SZ` *0*



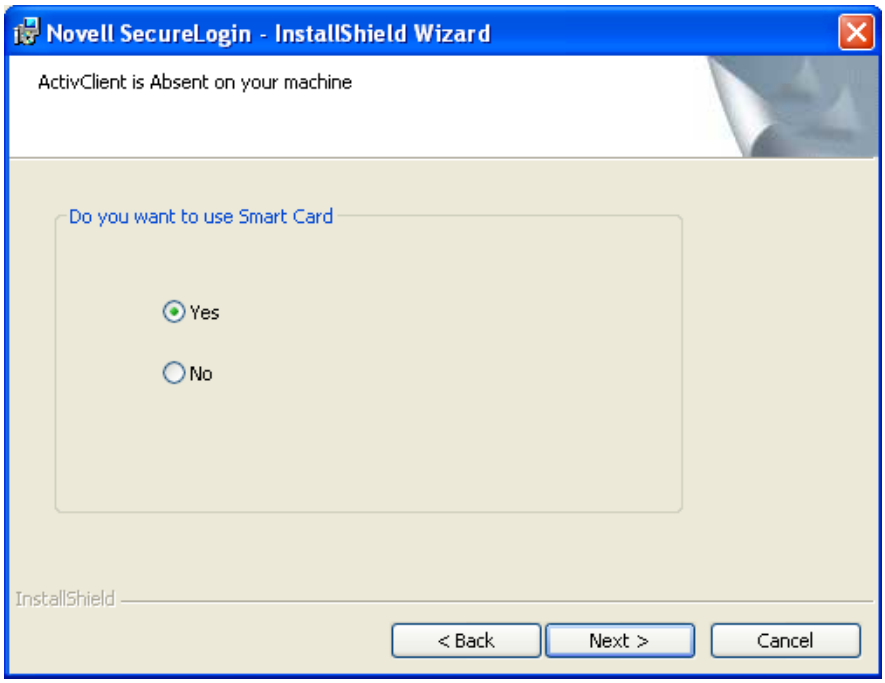
7 Specify the LDAP server address.



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

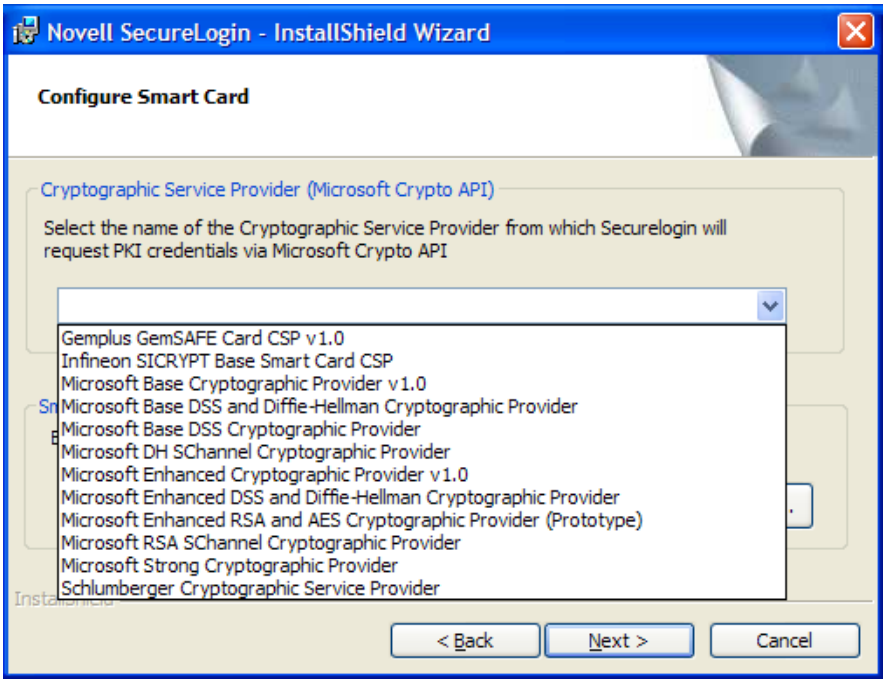
9 (Conditional) If you want to use smart card and if ActiveClient is detected in your system, select Click *Yes,*click *Next,* then continue with Step 10.

10 (Conditional) If you want to use smart card and if ActiveClient is not detected in your system:



10a Select *Yes,* then click *Next.*

10b Select a cryptographic service provider from which SecureLogin will request PKI credentials via the Microsoft Crypto API.



10c Select a PKCS#11 compatible library required for accessing the smart card, then click *Next*.

This specifies the location of the Cryptographic Token Interface installed as part of the smart card vendor's software. These API files are used by SecureLogin to communicate with the smart card.

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

For more information and instructions on smart card settings and cryptographic tokens, see the *Novell SecureLogin 6.1 SP1 Administration Guide*.

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

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

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

However, if you install the SecretStore client and then later run the install program and deselect the SecretStore client, you will cause problems with 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 populates the eDirectory cache.

The uninstall program does not delete user credentials.

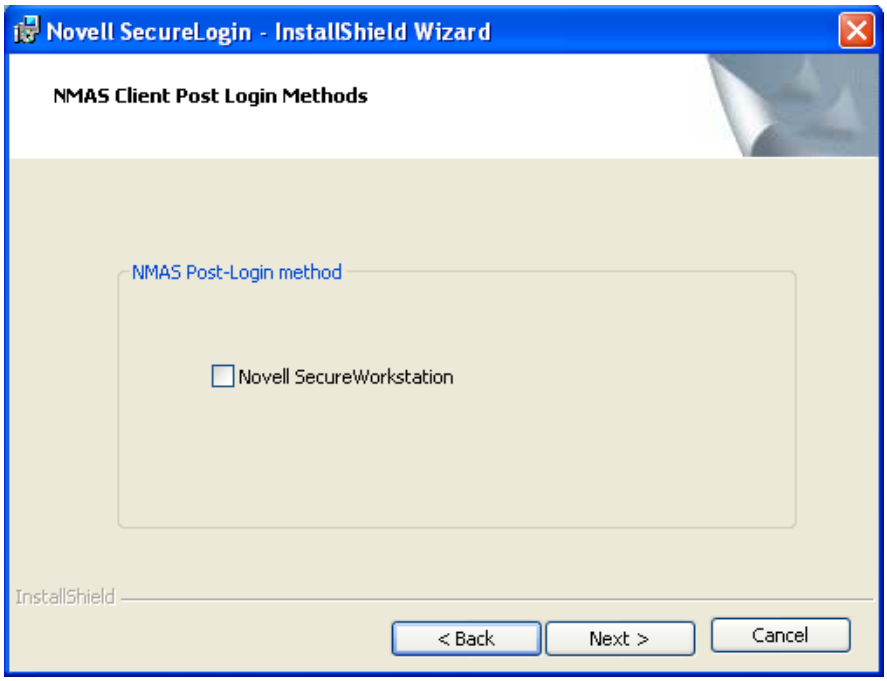
The Novell NMAS Client option installs the NMAS client. SecureLogin uses this option with the `AAVerify` command, to enable advanced authentication access to an application and also for NMAS authentication using LDAP.

---

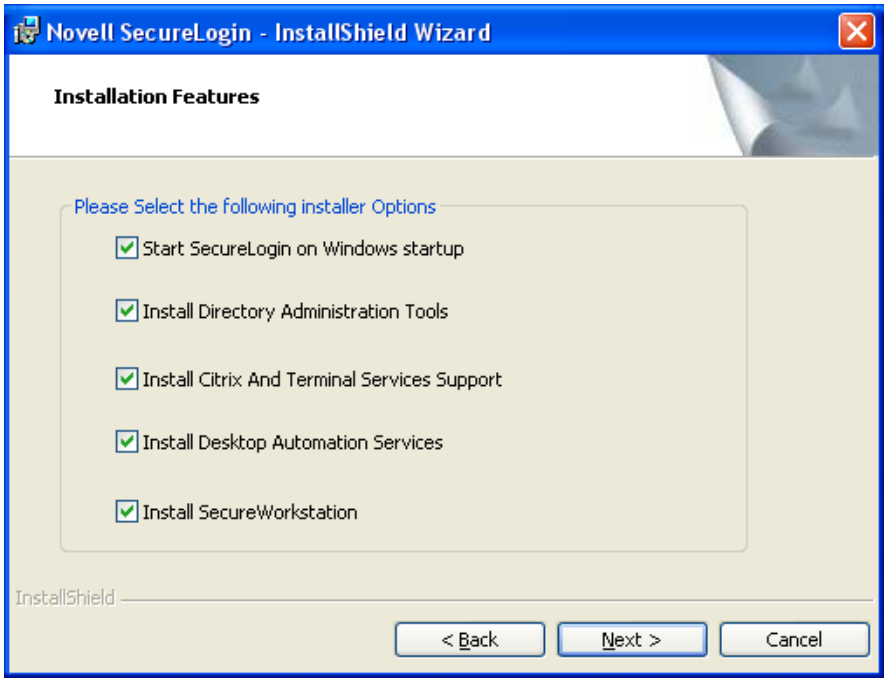
12 (Conditional) If you selected the NMAS client, select one or more NMAS login methods, then click *Next*.

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

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



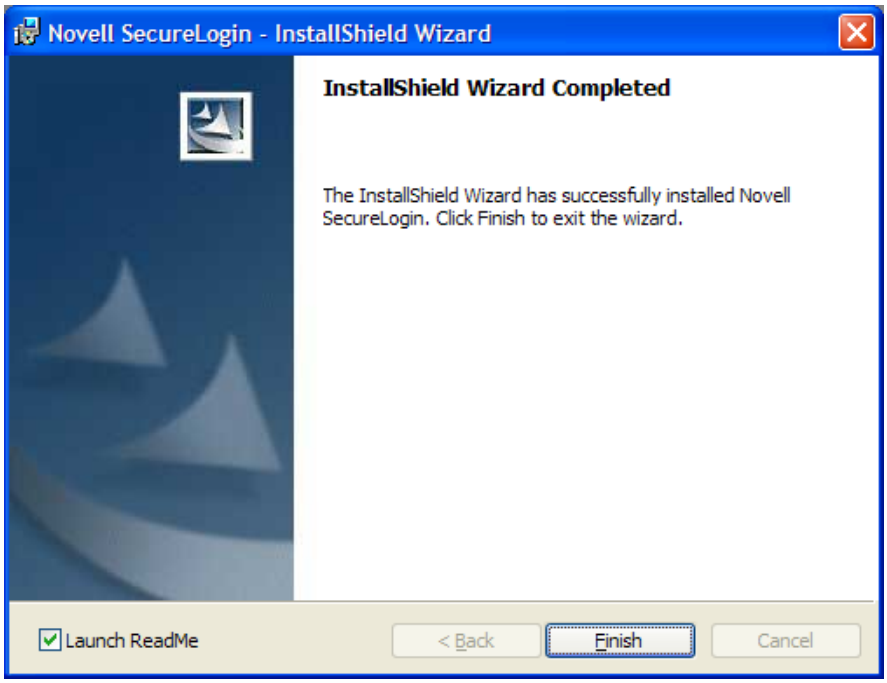
14 Select the installation features. Click *Next*.



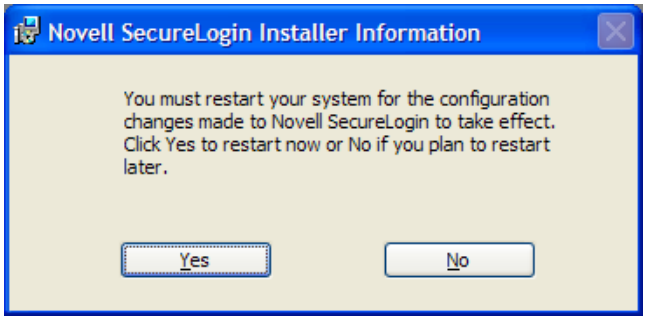
15 Click *Next*. The Ready to Install the Program dialog box is displayed.

16 Click *Install*.

17 Click *Finish*. By default, the *Launch ReadMe* option is selected.



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



Using the Custom Option for LDAP on eDirectory

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

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

  The user profile directory is the default path.

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

  User profiles for Windows Vista are in `c:\users` *`username`*.
- Select the SecureLogin components.

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

4.2.5 Installing Novell SecureLogin in LDAP Mode Without eDirectory

The LDAP option installs SecureLogin into LDAP v3 directory environments.

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

- "Using the Complete Option for LDAP without eDirectory" on page 45
- "Using the Custom Option for LDAP Without eDirectory" on page 45

Using the Complete Option for LDAP without eDirectory

The *Complete* option uses default values and installs Novell SecureLogin in `c:\program files\novell\securelogin`. Refer to "Using the Custom Option for LDAP Without eDirectory" on page 45 for options available through the *Custom* option.

1. Run `Novell SecureLogin.msi`, found in the `Securelogin\Client` directory of the installer package. The Welcome page is displayed.
2. Click *Next*. The license agreement page is displayed.
3. Accept the license agreement, then click *Next*.
4. Select *Complete*, then click *Next*.
5. Select *LDAP v3* as the platform where SecureLogin stores its data, then click *Next*.
6. Select when to log in to LDAP, then click *Next*.

   The *After Successfully Logging in to Windows* option is called the credential manager mode.
7. Configure a workstation to use the LDAP GINA as the primary authentication:

   7a If the Novell Client is installed on the workstation, remove it.

   7b During the SecureLogin installation, select the *LDAP* option and the *When Logging In to Windows* option.
8. In the Ready to Install SecureLogin dialog box, click *Install*.
9. Click *Finish*, click *Yes*, then restart the computer by clicking *OK*.
10. 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:

1. Specify a folder where SecureLogin will be installed.
2. Specify whether to associate your Windows username with your LDAP distinguished name, if LDAP is installed in the Credential Manager mode.
3. Specify an LDAP server address and port.

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

You must provide users with the following:

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

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

NOTE: When you select the *Custom* option, the administrator or the user can provide this information during installation.

---

4. The name (`ldapauthserver`) that appears in the *Address* field is a placeholder name. Specify a server name or IP address.
5. Specify a path for Novell SecureLogin's local cache.
6. The user profile directory is the default path.

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

   User profiles for Windows Vista are in `c:\users` *`username`*.
7. Select Novell SecureLogin components.

   The Description panel provides information about a component that you select.
8. Click *Next*.
9. Select options for starting Novell SecureLogin.

   If you select *No*, make sure to reboot your computer before you start SecureLogin. If you select *Yes*, your computer is automatically restarted.

4.3 Granting Rights

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

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

- Grant rights to the user's cache directory (for example, `c:\program files\novell\securelogin\cache\v3slc`).
- The default location is the user's profile directory. By default, the user already has rights to this directory. However, if the user specified an alternative path during the installation, you might need to grant rights to the cache directory.
- Use the registry setting to relocate the user's cache to a location that the user has rights to (for example, the user's documents folder).

4.4 Installing Administrative Tools for LDAP

In LDAP environments, Novell SecureLogin is managed using the Administrative Management utility. To access the Administrative Management utility, clicking the Windows *Start* > *Programs* > *Administrative Tools*.

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

The single sign-on plug-in to iManager enables you to define an LDAP password policy. However, you must extend the LDAP schema, because the plug-in does not enforce that policy unless the LDAP schema has been extended.

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

NOTE: Novell SecureLogin can be installed, configured, features added, and removed using Microsoft's Windows Installer (`msiexec.exe`) command line options and parameters provided from the command line or supplied through a batch file.

To install Novell SecureLogin on the administration workstation:

1. Log in to the workstation as an administrator.
2. Run the `Novell SecureLogin.msi` available in the `Client` directory of the SecureLogin 6.1 installer package. The Welcome page is displayed.
3. Click *Next*. The License agreement page is displayed.
4. Read the license agreement. Select *I accept the terms in the license agreement* if you want to proceed with the execution of the license agreement. If you do not want to proceed with the execution of the license agreement, click *Cancel* to quit the setup.
5. Click *Next*. The program location folder is displayed. The default location for Novell SecureLogin is, `..\Program Files\SecureLogin\`. If you want to change the location, click *Change* and select an alternative location for Novell SecureLogin on the drive.
6. Click *Next*. The installation environment page is displayed.
7. Select *LDAP directory*.
8. Select *Enable Microsoft Active Directory Group Policies (reboot required)*.

   NOTE: Enabling this is optional in LDAP installation. This group policies option is used only where the LDAP directory is working along side Microsoft Active Directory, or of Microsoft Active Directory is utilized for Novell SecureLogin in LDAP mode.

   ---

9. Click *Next*. The smart card support page is displayed.

   NOTE: The ActivClient card settings are used if detected.

   ---

10. Select *Use smart card or cryptographic token*.

    NOTE: This option is based on the administrator's preference to have Novell SecureLogin users utilize their smart card to store single sign-on data to encrypt the users' directory data using Public Key Infrastructure (PKI) token.

    ---

11 If you are not using *ActivClient smart card* option, or you want to change the smart card or cryptographic token, select *Use ActivClient smart card settings* option.This is the recommended.

12 From the *Cryptographic Service Provider (Microsoft Crypto API)* drop-down list, select the appropriate cryptographic service provider.

13 Browse to locate and select the appropriate *Smart card (PKCS#11) library* link (`.dll`) file.

Configuring manually the third-party smart card PKCS#11 link library assumes a high level of understanding of the cryptographic service provider's product. Hence, we recommend that you use the ActivClient smart card support.

14 Click *Open*.

15 Click *Next*. The installation features page is displayed.

16 We recommend you to select the *Start SecureLogin at Windows startup* option. However, depending on your enterprises's operating environment, you can opt to have Novell SecureLogin start at Windows start up or at user log in.

17 Select *Install Directory administration tools*.

The Directory administration tools are provided for corporate environments to manage users centrally at the directory. In the LDAP mode, Novell SecureLogin installs the Administrative Management utility.

18 If applicable, select *Install Citrix and Terminal Services support*.

19 If applicable, select *Enable aggressive server memory timing management*.

This is highly recommended to enhance the performance of Novell SecureLogin in a citrix environment.

20 Click *Next*. The cache location folder page is displayed.

IMPORTANT: ◆User's application data folder is the Triple DES or optionally AES encrypted repository for all Novell SecureLogin user data, which includes credentials, preferences, password policies, pre-configured applications, and application definitions.

◆By default Novell SecureLogin data is stored in both your organization's corporate directory and in the SecureLogin offline cache on your workstation's hard drive. The data in the directory and the local cache are synchronized to ensure user data is always current.

◆Where the smart card is used to store application credentials, the credentials are stored on the smart card and directory only. The cache and directory contain the application definitions, policies, and settings for single sign-on.

◆If smart cards are not used in the LDAP implementation, you can turn off the cache using an administrative preference so that the users access their single sign-on data from the directory only. This option has an impact on system performance.

---

21 If you want to change the location of the cache folder, select *Custom Location* > *Browse* and locate the an alternative folder.

22 Click *Next*. The Ready to install the program page is displayed.

23 Click *Install*. The installation process takes a few minutes. A confirmation message appears after the installation is complete.

24 Click *OK*.

25 Click *Finish*.

NOTE: If the *Microsoft Active Directory Group Policies* option was selected, a full system reboot is required.

Otherwise, save and close all open data before logging off and logging.

26 If you are prompted for a restart, click Yes. The computer is automatically restarted.

On login or restart, the Novell SecureLogin launches automatically and the Novell SecureLogin icon is displayed in the Windows notification area.

4.5 Deploying

Novell SecureLogin provides centralized management and deployment of user configuration by using the directory structure and administration tools in the same utility

We recommend that you configure Novell SecureLogin on a test user account before deployment.

- Section 4.5.1, "Deployment and Distribution Options," on page 49
- Section 4.5.2, "Installing Novell SecureLogin on a User Workstation," on page 49
- Section 4.5.3, "Setting Up a Passphrase," on page 51
- Section 4.5.4, "Installing for Mobile Users and Laptops," on page 52

4.5.1 Deployment and Distribution Options

Novell SecureLogin provides the following options for deployment and distribution of user configurations:

Table 4-1 *Deployment and Distribution Options*

Option	Description
Copy settings	Copy Novell SecureLogin configuration from one object in a directory to another object in the same directory.
Export and import	Use an XML file to distribute the configuration.
Directory object inheritance	Inherit the configuration from a higher-level directory object, for example, a Group Policy.
Corporate configuration re-direction	Specify the directory object from which the configuration is inherited.

4.5.2 Installing Novell SecureLogin on a User Workstation

We recommend using the industry standard application distribution packages such as Microsoft IntelliMirror*, Systems Management Server, and Novell ZENWorks® to deploy and manage Novell SecureLogin across large enterprises.

Novell SecureLogin can be installed, configured, and features can be added and removed using Microsoft Windows Installer options and parameters from the command line or provided through a batch file.

Prior to installing Novell SecureLogin, ensure the LDAP certificate file is saved in the default certificate location of the LDAP log, for example, `securelogin\rootcert.der`.

The procedure explained here applies to manual installation and is also applicable to installing on a small number of workstations and laptop computers.

1. Log in to the workstation as an administrator.
2. Run the `Novell SecureLogin.msi` from the Novell SecureLogin installer package. The Welcome page is displayed.
3. Click *Next*. The License agreement page is displayed.
4. Read the license agreement. Select *I accept the terms in the license agreement* if you want to proceed with the execution of the license agreement. If you do not want to proceed with the execution of the license agreement, click *Cancel* to quit the setup.
5. Click *Next*. The Program location folder is displayed. The default location for Novell SecureLogin is `..\Program Files\SecureLogin\`. If you want to change the location, click *Change* and select an alternative location for Novell SecureLogin on the drive.
6. Click *Next*. The installation environment page is displayed.
7. Select *LDAP directory*.
8. Select *Enable Microsoft Active Directory Group Policies (reboot required)*.

   Enabling this is optional in LDAP installation. This group policies option is used only where the LDAP directory is working with Microsoft Active Directory, or if Microsoft Active Directory is used for Novell SecureLogin in LDAP mode.
9. Click *Next*. The smart card support page is displayed.

   The ActivClient card settings are used if they are detected.
10. Select *Use smart card or cryptographic token*.

    This option is based on the whether you want to have Novell SecureLogin users use their smart cards to store single sign-on data to encrypt the users' directory data with a Public Key Infrastructure (PKI) token.
11. If you are not using the *ActivClient smart card* option, or if you want to change the smart card or cryptographic token, select *Use ActivClient smart card settings* option. This is the recommended option.
12. From the *Cryptographic Service Provider (Microsoft Crypto API)* drop-down list, select the appropriate cryptographic service provider.
13. Browse to locate and select the appropriate *Smart card (PKCS#11) library* link (`.dll`) file.

    Manually configuring the third-party smart card PKCS#11 link library assumes a high level of understanding of the cryptographic service provider's product, so, we recommend that you use the ActivClient smart card support.
14. Click *Open*.
15. Click *Next*. The Installation features page is displayed.
16. Select the startup options.

    We recommend that you select the *Start SecureLogin at Windows startup* option. However, depending on your enterprises's operating environment, you can opt to have Novell SecureLogin start at Windows startup or at user login.
17. Select *Install Directory administration tools*.

The Directory administration tools are provided for corporate environments to manage users centrally at the directory. In the LDAP mode, Novell SecureLogin installs the Administrative Management utility.

18 If applicable, select *Install Citrix and Terminal Services support*.

Novell recommends that you test all the Citirx environment deployments in a test environment before the actual deployment.

19 Click *Next*. The Cache location folder page is displayed.

IMPORTANT: Consider the following information before changing the cache location:

- The user's application data folder is the Triple DES or optionally AES encrypted repository for all Novell SecureLogin user data, which includes credentials, preferences, password policies, preconfigured applications, and application definitions.
- By default Novell SecureLogin data is stored in both your organization's corporate directory and in the SecureLogin offline cache on your workstation's hard drive. The data in the directory and the local cache are synchronized to ensure user data is always current.
- When the smart card is used to store application credentials, the credentials are stored on the smart card and directory only. The cache and directory contain the application definitions, policies, and settings for single sign-on.
- If smart cards are not used in the LDAP implementation, you can turn off the cache using an administrative preference so that the users access their single sign-on data from the directory only. This option has an impact on system performance.

---

20 If you want to change the location of the cache folder, select *Custom Location* > *Browse* and locate the an alternative folder.

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

22 Click *Install*. The installation process takes a few minutes. A confirmation message appears after the installation is complete.

23 Click *OK*.

24 Click *Finish*.

25 If you are prompted for a restart, click *Yes*. The computer is automatically restarted.

IMPORTANT: Save and close all open data before logging out and logging in by using the Novell SecureLogin.

If you are deploying Novell SecureLogin for the first time and if you have not disabled the passphrase functionality, the next time a user logs in the *Passphrase Setup* dialog box is displayed. For information on setting up a passphrase, see Section 4.5.3, “Setting Up a Passphrase,” on page 51.

4.5.3 Setting Up a Passphrase

A passphrase is a question and answer combination used as an alternative form of identity verification. Passphrase functionality protects SecureLogin credentials from unauthorized access and enables users to access Novell SecureLogin in offline mode. Passphrase verification also prohibits an administrator from accessing a user's single sign-on credentials if they reset the user's

password. Passphrases can also be used as a substitute authentication mode if, for example, a user forgets his or her password. Depending on the preferences, SecureLogin passphrase questions can be generated by the administrator and, or the user.

Administrators can also set up the passphrase questions for the users and enforce strict policies on the passphrase answer. For more information, see the *Novell SecureLogin 6.1 SP1 Administration Guide*.

During installation, the passphrase security is enabled to enforce passphrase setup during the initial login. You can disable the passphrase policy by deselecting *Use Passphrase Policy* option in the *Advanced Settings* pane of the Administrative Management utility.

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

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

WARNING: Remember the passphrase answer. If you forget the answer, it cannot be accessed.

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

After installing Novell SecureLogin successfully, when you attempt to log in to the workstation, you are prompted to set your passphrase question and answer.

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

NOTE: When you upgrade, SecureLogin stores all users data, including the user's passphrase question and response, from the previous version, so you do not need to re-create the passphrase.

You can create passphrase questions for users to select from in a directory environment; however, because you are the first SecureLogin user, you must create your own passphrase question.

4.5.4 Installing for Mobile Users and Laptops

Installing Novell SecureLogin for mobile and remote users is the same as Section 4.5.2, "Installing Novell SecureLogin on a User Workstation," on page 49.

However, it is important for you to ensure that the cache is saved locally, or users will be unable to access applications when they are disconnected from the network.

By default, the *Enable cache file* setting in the *Preferences Properties Table* is set to *Yes*. You can set this at either Organizational Unit level or on a per-user basis.

4.6 Configuration Issues

4.6.1 Contextless Login

If you configure Novell SecureLogin to use LDAP mode, a log page is displayed when Novell SecureLogin is launched.

The login dialog box requires a user distinguished name (DN) and password. The LDAP Authentication client provides a contextless login. This feature allows you to type part of your fully distinguished name (DN) rather than the full string that some users may find confusing.

Table 4-2 *Contextless Login*

If	Then
More than one match is found.	A login dialog box is displayed that allows the user to select the login account.
Multiple IDs exist.	The client lists all user IDs that begin with (for example, Westbye Tim), then selects the Domain Name for his or her user ID and login. You can search using the user’s given name, surname and display name. Surname (sn) and given name (givenname) are the default values.

4.6.2 LDAP Browser

1. Log in to the LDAP browser using your user account or administrator account credentials.
2. Provide your username and password, and click *OK*.

If you cannot view the full LDAP specify information, click *Advanced* to expand the dialog box. If this information is blank, then populate as needed.

- If you are installing Novell SecureLogin for LDAP for the first time, then the *Context* and *Primary host* areas are blank.
- If you are upgrading to Novell SecureLogin for LDAP from a previous version then the users distinguished name (DN) information is normally cached in the system registry.
- As an administrator, you might need to include a system registry update as part of the Novell SecureLogin deployment strategy.

4.6.3 Using LDAP on eDirectory

All the functionality that is available in NMAS is also available in 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 password takes precedence. The Simple Password exists if used in 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.

4.6.4 Using LDAP in Non-eDirectory Environments

This section contains the following information:

- "Configuring the Server" on page 54
- "Configuring the Workstation" on page 55
- "Using Contextless Login" on page 55

Configuring the Server

This section contains the following information:

- "Retrieving the Certificate" on page 54
- "Enabling Anonymous Queries" on page 54
- "Extending the Schema" on page 55

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 section of the documentation for the directory server you use.

Enabling Anonymous Queries

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

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

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

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

Table 4-3 Setting Permissions for Anonymous Login

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 Schema" on page 55.

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

- **Active Directory:** Extend the Active Directory schema.

  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
`CertFilePath`	REG_SZ	C:\ad_cert.der
`CertFilePath`	REG_SZ	C:\ad_cert.b64

Using Contextless Login

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

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

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

Installing in a Microsoft Active Directory Environment

5

This section provides information on the following:

5.1 Installation Overview

- Have administrator-level access to the server and the administration workstations.
- Back up the existing directory.
- For multiple-directory environments:
  - Identify the domain controller to determine the directory where you will install Novell SecureLogin and the order of replication.
  - Have access to the domain controller.

The procedures explained in the following sections apply to the standard configuration of a server managed through an administration workstation. The procedures also apply to configurations that do not separate the server from the administration workstation.

The following high-level task list provides an overview of the procedures necessary to install SecureLogin in a Microsoft Active Directory environment.

1. Uninstall any Novell® SecureLogin version prior to 3.5.*x*
2. Ensure that Microsoft Management Console (MMC) Active Directory plug-ins are installed on the administration workstation.
3. Extend the directory schemas for Novell SecureLogin version prior to 6.1.
4. If the application type is single sign-on enabled, install Citrix or Terminal Services clients.
5. Install Sun Java Runtime Engine version 1.3 or later, or Oracle JInitiator 1.3.1 or later on the server and workstations, if single sign-on to Java applications is required.
6. Install Novell SecureLogin on the administration workstation.
7. Create test users on the administration workstations.
8. Define and configure the Novell SecureLogin user environment, including enabling the required applications for single sign-on.
9. Copy the test users’ configuration to relevant objects.
10. Deploy the Novell SecureLogin application on user workstations.

NOTE: Secure Workstation is not supported in Active Directory installation of Novell SecureLogin.

You must install JRE version 1.4 or later to enable single sign-on to Java applications or JavaScript* logins on the workstation.

5.2 Microsoft Active Directory

This section has the following information:

5.2.1 Novell SecureLogin on Windows

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

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

If an error appears during an attempted login immediately after you install Novell 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.

5.2.2 LDAP Mode

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

To extend the Microsoft Active Directory schema and assign user rights, see Section 4.2.2, “Extending The LDAP Directory Schema,” on page 35.

5.2.3 ADAM

Novell SecureLogin supports deployment in an ADAM instance. For more information, see Chapter 6, “Installing in an ADAM Environment,” on page 77.

5.3 Installing

This section provides the following information:

5.3.1 Extending The Active Directory Schema

Novell SecureLogin leverages the directory to store and manage Novell SecureLogin data. Novell SecureLogin extends the directory schema to add six Novell SecureLogin schema attributes where Novell SecureLogin data is stored.

After you extend the directory schema, you must give permissions to objects including group policy, organizational units, and containers. These implement Novell SecureLogin to access the attributes. Authorizing read or write rights to the Novell SecureLogin directory schema attributes is referred to as *assigning user rights*.

These are the six Novell SecureLogin attributes that are added to the Directory schema:

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

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

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

IMPORTANT: Keep the following information in mind as you extend the schema:

- If Novell SecureLogin version 3.5.*x* is installed, you do not need to extend the directory schema, because the attributes are the same. However, any new directory objects for example organizational units still require you to assign rights.
- If the Microsoft Active Directory instance is deployed by copying and running the `adsscheme.exe` file from another location, you must copy the entire folder containing the Microsoft Active Directory Schema and configuration files to the new preferred location. The Microsoft Active Directory Schema and configuration files must be located in the same folder in order for the Active Directory instance to successfully deploy.

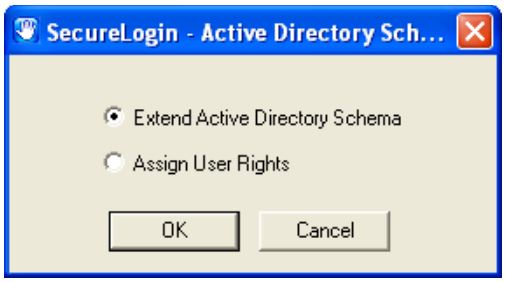
The following instructions apply to the configuration of the Microsoft Active Directory instance stored and administered on a separate server from the Active Directory server domain controller.

1. Log in to the server as an administrator.
2. Click *Schema Extension Tools* > *Active Directory Extension*.

   or,

   If you are installing from the Novell SecureLogin installer package, locate the `Tools` folder and double-click `adsschema.exe`.

   The Novell SecureLogin Active Directory Schema dialog box is displayed.



3 Select *Extend Active Directory Schema*.

4 Click *OK*. A confirmation message is displayed.

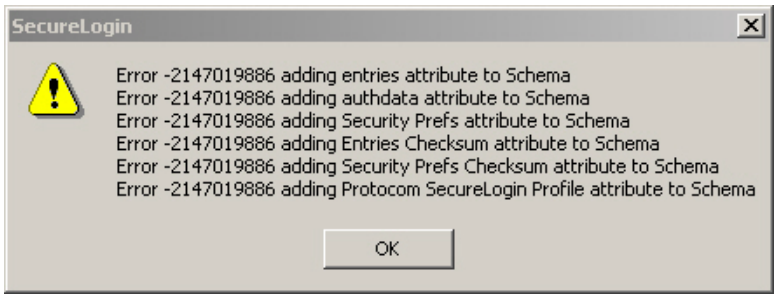
5 Click *OK* to return to the Active Directory Schema dialog box.

Now that you have extended the schema, you need to assign access rights to the relevant containers and organizational units.

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

---

6 Ignore this message and click *OK*.



5.3.2 Assigning User Rights

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

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

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

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

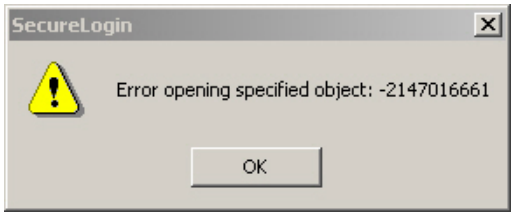
In the above figure, rights are assigned to the Users container.

The Users container definition is:
`cn=users, dc=www, dc=training, dc=com`
To assign rights to an organizational unit, for example Marketing, in the domain www.company.com, the definition is:
`ou=marketing, dc=www, dc=company, dc=com`

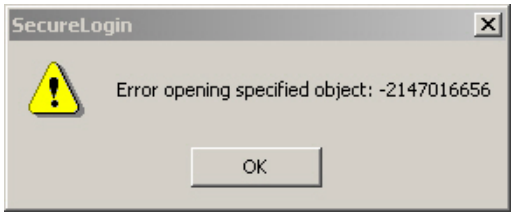
3 Specify your container or organizational unit definition in the *Assign rights to this object* field. The confirmation dialog box appears.

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

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



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



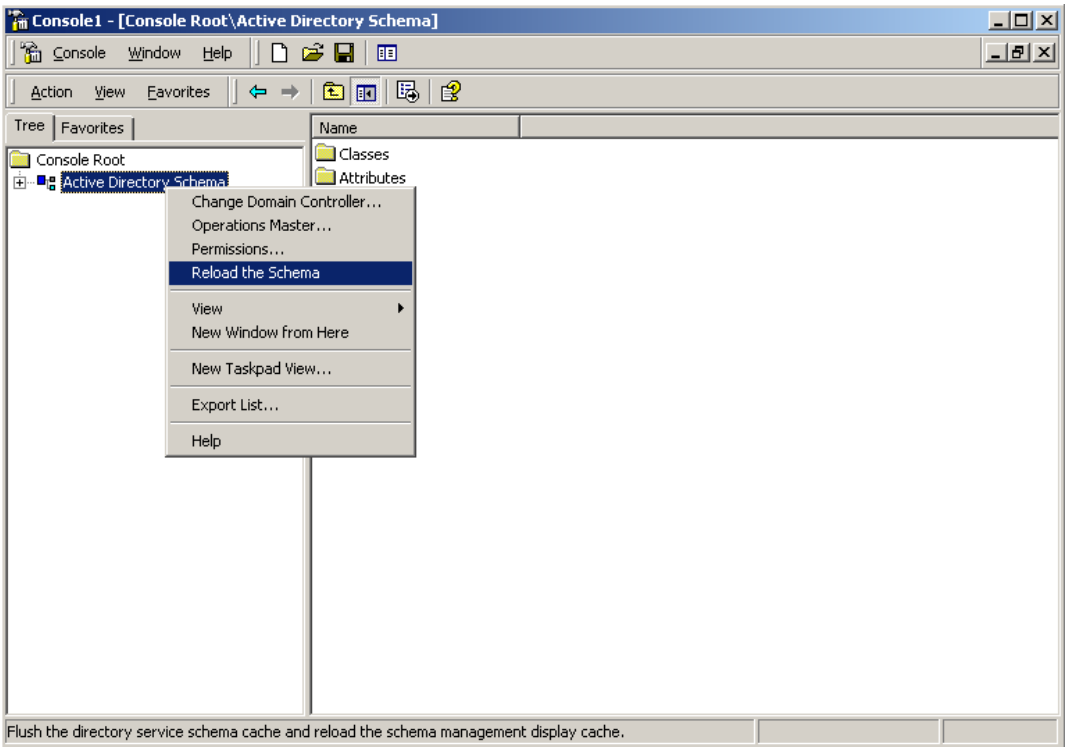
If the above error message is displayed, you have attempted to assign rights to an object that does not exist on this directory. Check your punctuation, syntax, and spelling, and repeat the procedure.

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

7 Click *Cancel.*

5.3.3 Refreshing the Directory Schema

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



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

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

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

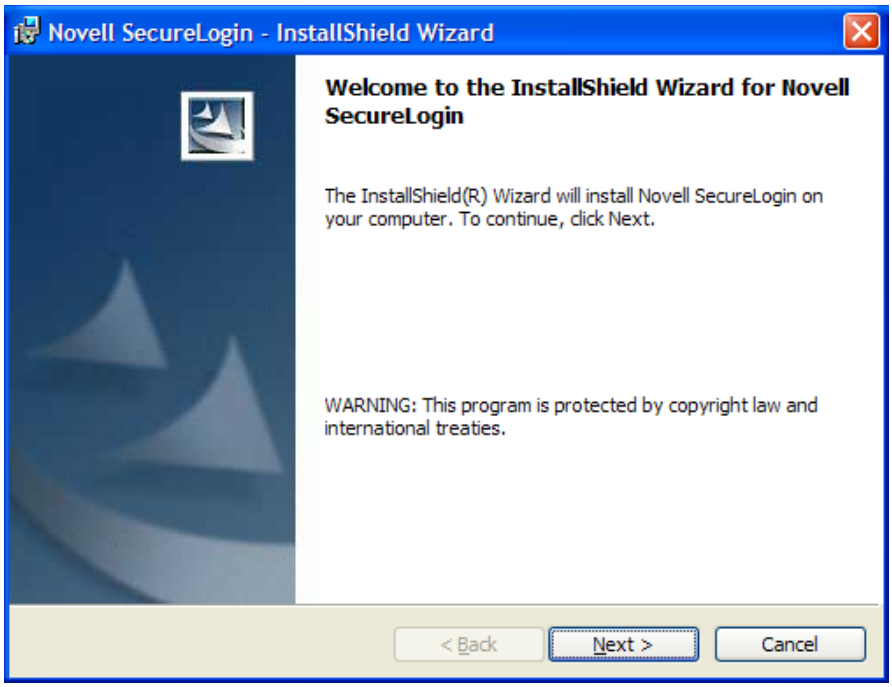
NOTE: You can extend rights to objects at any time after the schema is extended. If you add organizational units, then you need to rerun the `adschema.exe` tool and assign rights to the new object to permit Novell SecureLogin data to write to the directory.

5.3.4 Installing on the Administration Workstation

After you have extended the Active Directory schema and assigning permissions to the required directory objects, install the Novell SecureLogin application on the administration and user workstation.

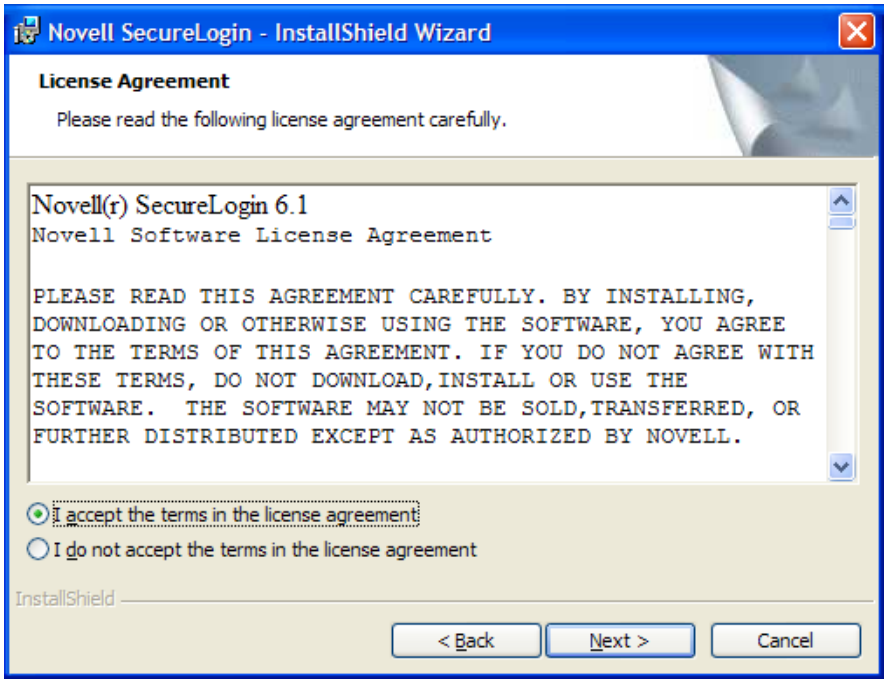
1 Log in to the workstation as an administrator.

2 If you are installing from the product installer package, double-click the `Novell SecureLogin.msi` that is available in `SecureLogin\Client` directory of the installer package. The Welcome page is displayed.

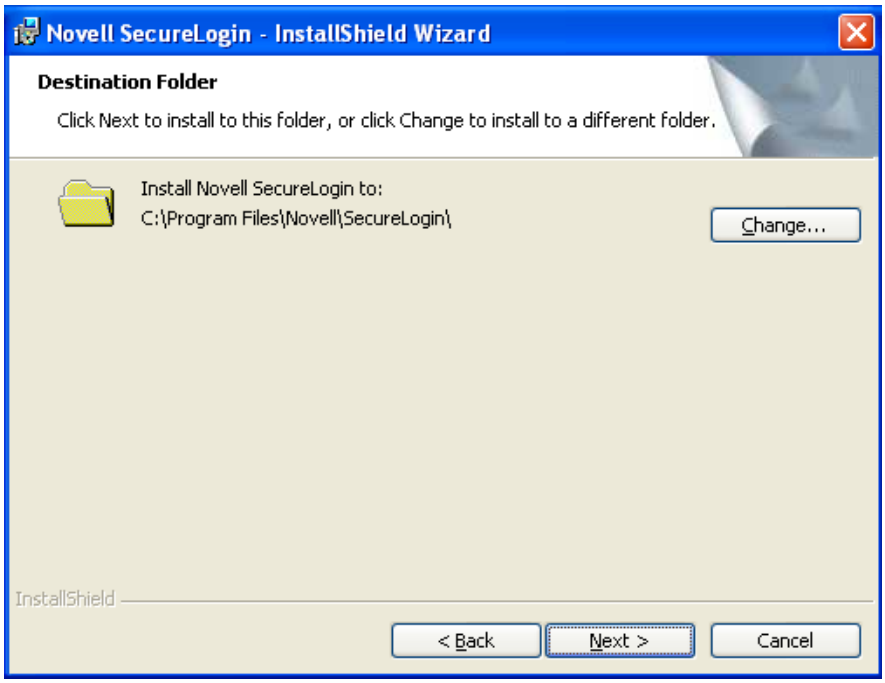


3 Click *Next*. The License agreement page is displayed.

4 Read the license agreement. Select *I accept the terms in the license agreement* if you want to proceed with the execution of the license agreement. If you do not want to proceed with the execution of the license agreement, click *Cancel* to quit the setup.



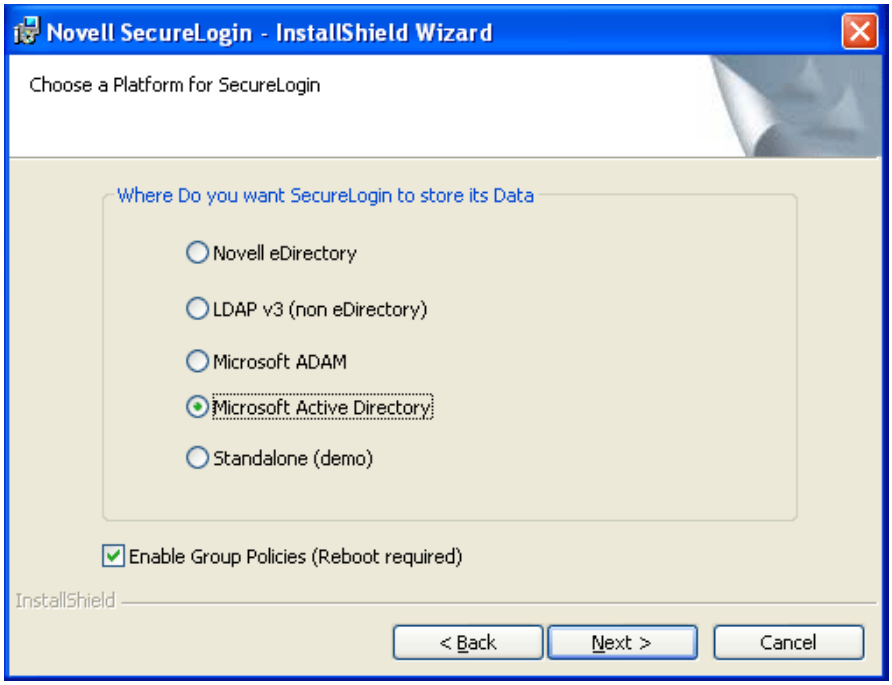
5 Click *Next*. The program location folder is displayed. The default location for Novell SecureLogin is, `..\Program Files\SecureLogin\`. If you want to change the location, click *Change* and select an alternative location for Novell SecureLogin on the drive.



6 Click *Next*. The installation environment page is displayed.

7 Select *Microsoft Active Directory*.

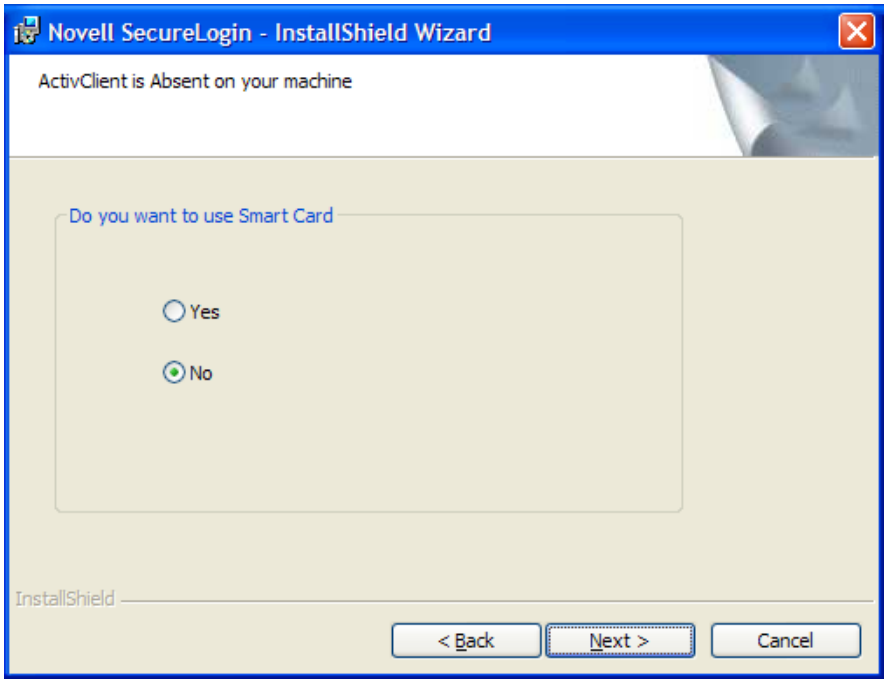
IMPORTANT: There are no additional installation or configurations required when running Microsoft Active Directory in LDAP mode. The only variation is in selecting the installation environment. You select the *LDAP directory* instead of the *Microsoft Active Directory*.



8 (Optional) Select *Enable Microsoft Active Directory Group Policies*.

9 Click *Next*. The smart card support page is displayed.

The ActivClient card settings are used if they are detected.

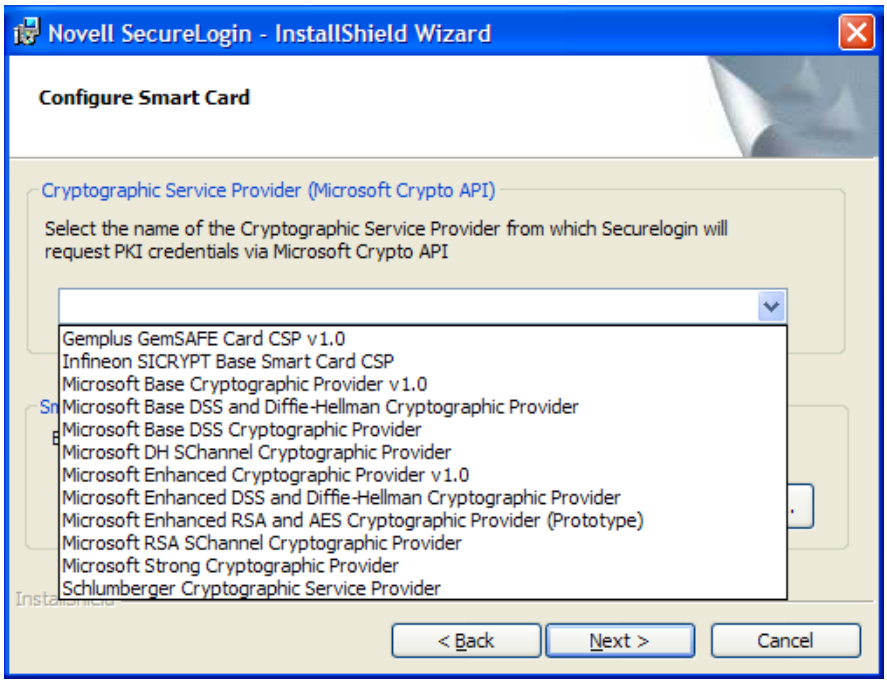


10 Select *Use smart card or cryptographic token*.

NOTE: This option is based on whether you want to have Novell SecureLogin users use their smart cards to store single sign-on data to encrypt the users' directory data by using Public Key Infrastructure (PKI) tokens.

11 If you are not using the *ActivClient smart card* option, or you want to change the smart card or cryptographic token, select the *Use ActivClient smart card settings* option. This is the recommended setting.

12 From the *Cryptographic Service Provider (Microsoft Crypto API)* drop-down list, select the appropriate cryptographic service provider.

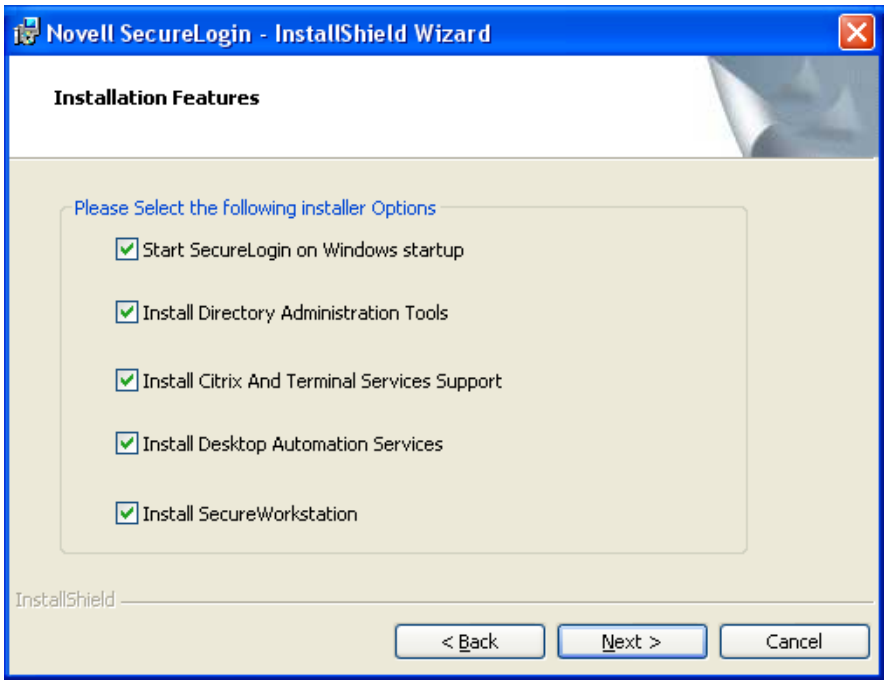


13 Browse to locate and select the appropriate *Smart card (PKCS#11) library* link (`.dll`) file.

14 Manually configure the third-party smart card PKCS#11 link library assumes a high level of understanding of the cryptographic service provider's product, so, we recommend that you use the ActivClient smart card support.

15 Click *Open*.

16 Click *Next*. The installation features page is displayed.



Select the startup options.

We recommend you to select the *Start SecureLogin at Windows startup* option. However, depending on your enterprises's operating environment, you can opt to have Novell SecureLogin start at Windows startup or at user login.

Select *Install Directory administration tools*.

The Directory administration tools are provided for corporate environments to manage users centrally at the directory. In the LDAP mode, Novell SecureLogin installs the Administrative Management utility.

If applicable, select *Install Citrix and Terminal Services support*.

This is highly recommended to enhance the performance of Novell SecureLogin in a Citrix environment.

17 Click *Next*. The cache location folder page is displayed.

If you want to change the location of the cache folder, select *Custom Location* > *Browse* and locate the an alternative folder.

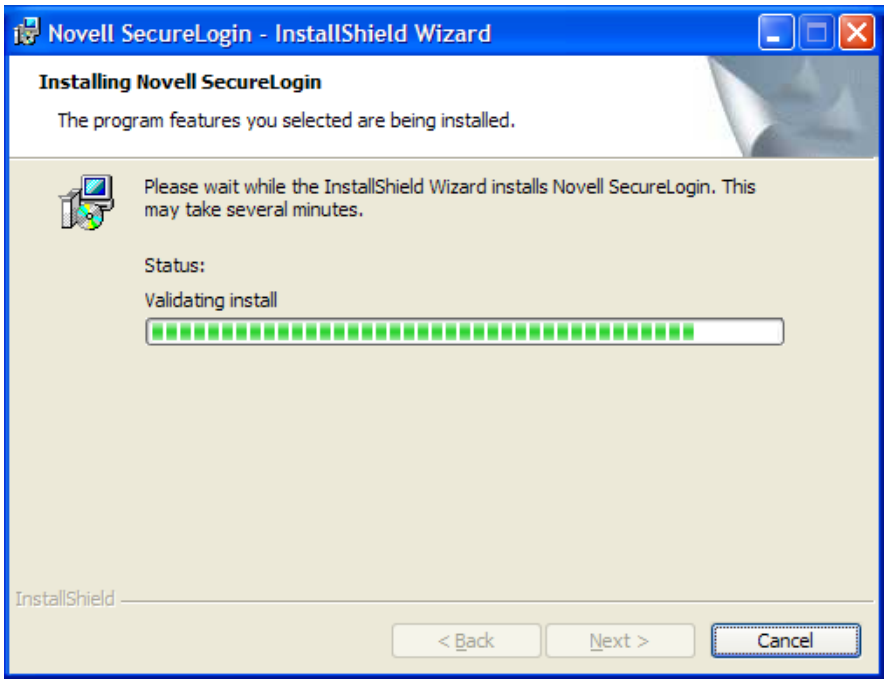
IMPORTANT: Consider the following information before changing the cache location:

- The user's application data folder is the Triple DES or optionally AES encrypted repository for all Novell SecureLogin user data, which includes credentials, preferences, password policies, preconfigured applications, and application definitions.
- By default, Novell SecureLogin data is stored in both your organization's corporate directory and in the Novell SecureLogin offline cache on your workstation's hard drive. The data in the directory and the local cache are synchronized to ensure user data is always current.
- When the smart card is used to store application credentials, the credentials are stored on the smart card and directory only. The cache and directory contain the application definitions, policies, and settings for single sign-on.
- If smart cards are not used in the LDAP implementation, you can turn off the cache using an administrative preference so that the users access their single sign-on data from the directory only. This option has an impact on system performance.

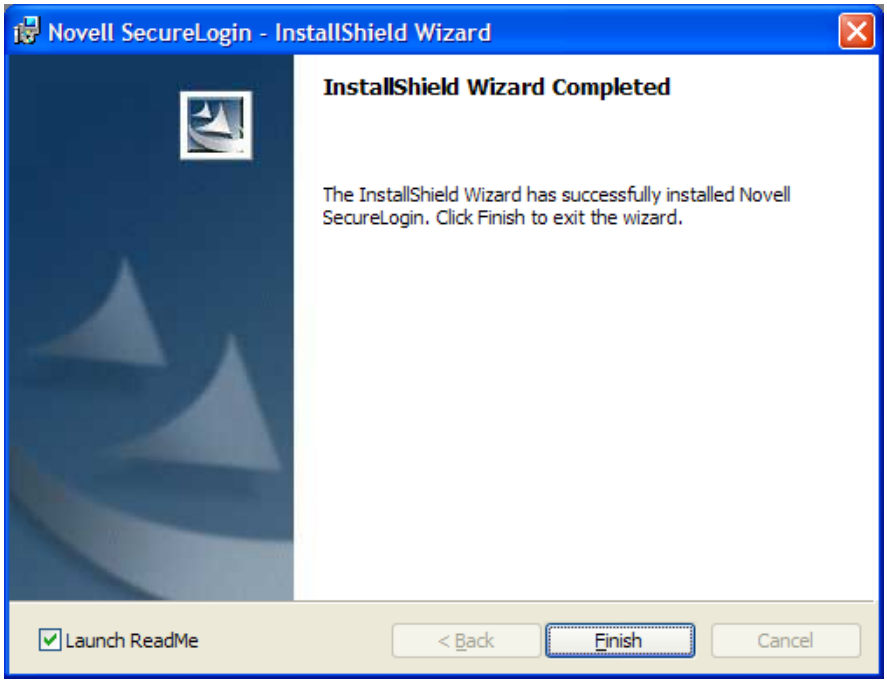
---

18 Click *Next*. The Ready to install the program page is displayed.

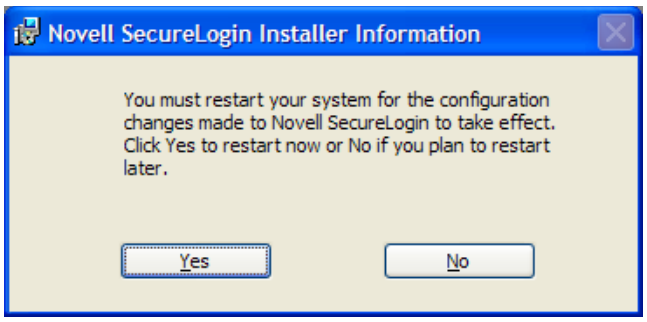
19 Click *Install*. The installation process takes a few minutes. A confirmation message appears after the installation is complete.



20 Click *Finish*.



21 If you are prompted for a restart, click *Yes*. The computer is automatically restarted.

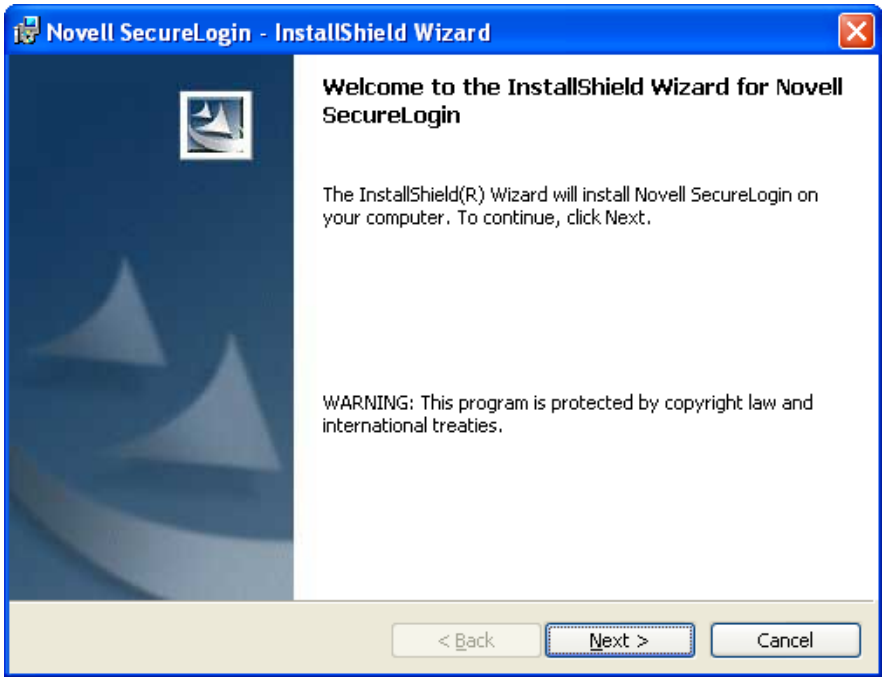


On login or restart, the Novell SecureLogin launches automatically and the Novell SecureLogin icon is displayed in the Windows notification area.

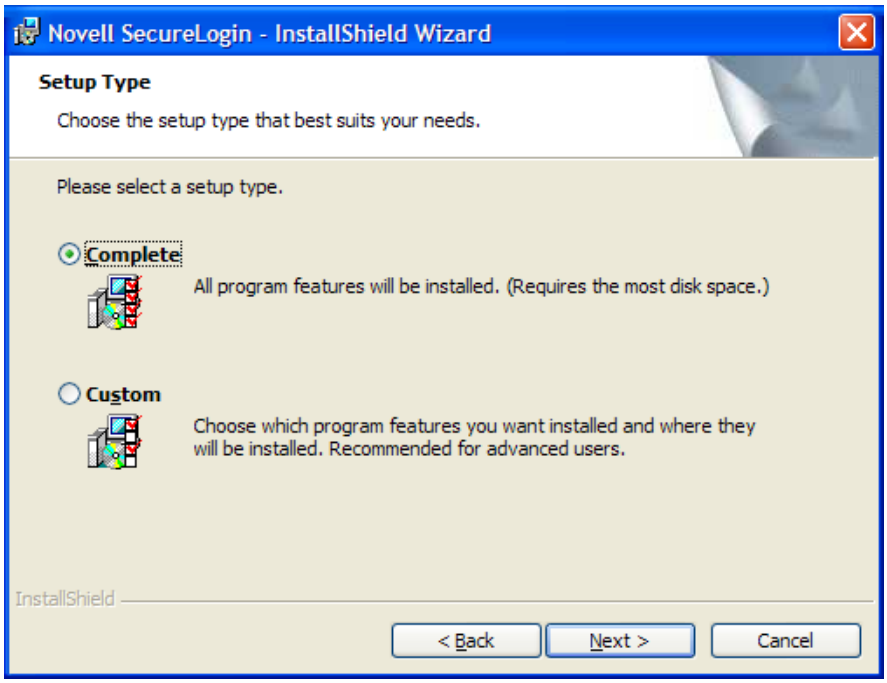
5.3.5 Using the Complete Option for Active Directory

The *Complete* option uses default values and installs Novell SecureLogin in `c:\program files\novell\securelogin`. Refer to Section 5.3.6, "Using the Custom Option for Active Directory," on page 71 for options available through the *Custom* option.

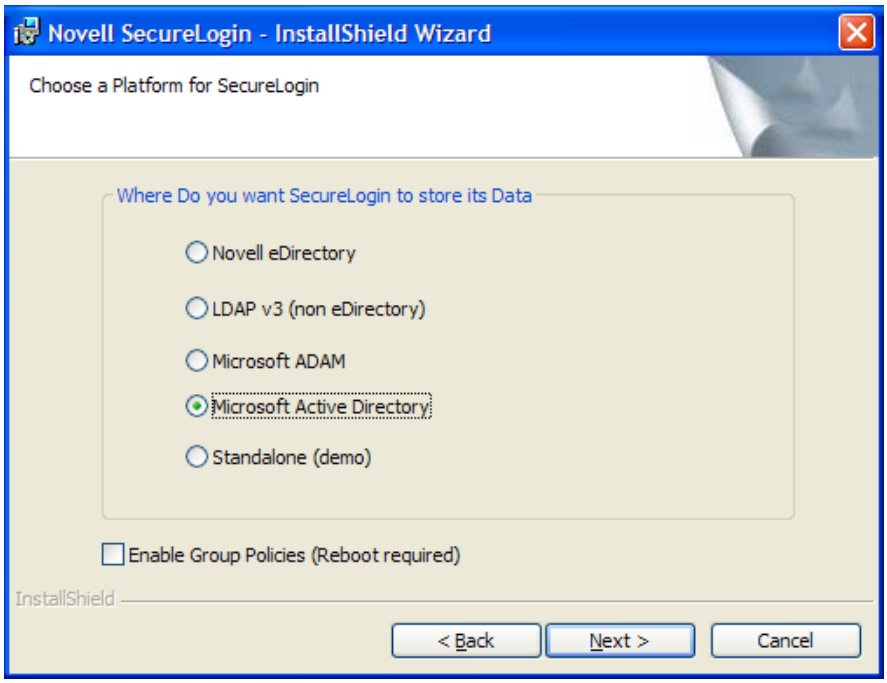
1 Run `Novell SecureLogin.msi` found in the `securelogin/client` directory.



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



3 Select *Microsoft Active Directory* as the platform where SecureLogin stores its data, then click *Next*.



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

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

5a (Conditional) If you want to use smart card and if ActiveClient is not detected in your system.

5b Select *Yes,* then click *Next.*

5c (Optional) Select a cryptographic service provider from which SecureLogin will request PKI credentials via the Microsoft Crypto API.

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

This specifies the location of the Cryptographic Token Interface installed as part of the smart card vendor's software. These API files are used by SecureLogin to communicate with the smart card.

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

For more information and instructions on smart card settings and cryptographic tokens, see the *Novell SecureLogin 6.1 SP1 Administration Guide*.

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

5.3.6 Using the Custom Option for Active Directory

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

1 Specify a path for Novell SecureLogin's local cache.

The user profile directory is the default path.

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

User profiles for Windows Vista are in `c:\users username`.

2 Select Novell SecureLogin components. The Description panel provides information about a component that you select.

3 Select options for starting Novell SecureLogin.

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

5.4 Deploying

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

5.4.1 Configuring a User's Environment List

Configuring a user's Novell SecureLogin environment includes:

- Setting preferences.

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

NOTE: We recommend that you configure Novell SecureLogin on a test user account before deploying.

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

Table 5-1 *Deploying and Distribution Options*

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

5.4.2 Installing On a User Workstation

It is recommended that you use industry standard application distribution packages such as Microsoft IntelliMirror, System Management Server, or Novell ZENWorks® to deploy and manage Novell SecureLogin across large enterprises.

Novell SecureLogin can be installed, configured, and features can be added and removed using Microsoft Windows Installer command-line options and parameters types from the command line or provided through a batch file.

Prior to installing Novell SecureLogin that ensure the LDAP certificate file is saved in the default certificate location of the LDAP log, for example, `securelogin\rootcert.der`.

The procedure explained here applies to manual installation, and is also applicable to installing on small number of workstations and laptop computers.

1. Log in to the workstation as an administrator.
2. Run the `Novell SecureLogin.msi`.

   The Welcome page is displayed.
3. Click *Next*. The License agreement page is displayed.
4. Read the license agreement. Select *I accept the terms in the license agreement* if you want to proceed with the execution of the license agreement. If you do not want to proceed with the execution of the license agreement, click *Cancel* to quit the setup.
5. Click *Next*. The program location folder is displayed. The default location for Novell SecureLogin is, `..\Program Files\SecureLogin\`. If you want to change the location, click *Change* and select an alternative location for Novell SecureLogin on the drive.
6. Click *Next*. The installation environment page is displayed.

7 Select *Microsoft Active Directory*.

IMPORTANT: There are no additional installation or configurations required when running Microsoft Active Directory in LDAP mode. The only variation is in selecting the installation environment. You select the *LDAP directory* instead of the *Microsoft Active Directory*.

---

8 Click *Next*. The smart card support page is displayed.

The ActivClient card settings are used if they are detected.

9 Select *Use smart card or cryptographic token*.

NOTE: This option is based on whether you want to have Novell SecureLogin users use their smart card to store single sign-on data to encrypt the users' directory data by using a Public Key Infrastructure (PKI) token.

---

10 If you are not using *ActivClient smart card* option, or you want to change the smart card or cryptographic token, select *Use ActivClient smart card settings* option. This is the recommended option.

11 From the *Cryptographic Service Provider (Microsoft Crypto API)* drop-down list, select the appropriate cryptographic service provider.

12 Browse to locate and select the appropriate *Smart card (PKCS#11) library* link (`.dll`) file.

Manually configuring the third-party smart card PKCS#11 link library assumes a high level of understanding of the cryptographic service provider's product. Hence, we recommend that you use the ActivClient smart card support.

13 Click *Open*.

14 Click *Next*. The installation features page is displayed.

15 We recommend you to select the *Start SecureLogin at Windows startup* option. However, depending on your enterprises's operating environment, you can opt to have Novell SecureLogin start at Windows startup or at user login.

16 Select *Install Directory administration tools*.

The Directory administration tools are provided for corporate environments to manage users centrally at the directory. In the LDAP mode, Novell SecureLogin installs the Administrative Management utility.

17 If applicable, select *Install Citrix and Terminal Services support*.

18 Click *Next*. The cache location folder page is displayed.

IMPORTANT: Consider the following information before changing the cache location:

- The user's application data folder is the Triple DES or optionally AES encrypted repository for all Novell SecureLogin user data, which includes credentials, preferences, password policies, preconfigured applications, and application definitions.
- By default, Novell SecureLogin data is stored in both your organization's corporate directory and in the SecureLogin offline cache on your workstation's hard drive. The data in the directory and the local cache are synchronized to ensure user data is always current.

- When the smart card is used to store application credentials, the credentials are stored on the smart card and directory only. The cache and directory contain the application definitions, policies, and settings for single sign-on.
- If smart cards are not used in the LDAP implementation, you can turn off the cache using an administrative preference so that the users access their single sign-on data from the directory only. This option has an impact on system performance.

---

19 If you want to change the location of the cache folder, select *Custom Location* > *Browse* and locate the an alternative folder.

20 Click *Next*. The Ready to install the program page is displayed.

21 Click *Install*. The installation process takes a few minutes. A confirmation message appears after the installation is complete.

22 Click *OK*.

23 Click *Finish*.

24 If you are prompted for a restart, click `Yes`. The computer is automatically restarted.

5.4.3 Setting Up a Passphrase

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

During installation, the passphrase security is enabled to enforce passphrase setup during the initial login. You can disable the passphrase policy by deselecting *Use Passphrase Policy* option in the *Advanced Settings* pane of the Administrative Management utility.

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

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

WARNING: Remember the passphrase answer. If you forget the answer, it cannot be accessed.

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

After installing Novell SecureLogin successfully, when you attempt to log in to the workstation, you are prompted to set your passphrase question and answer.

1 Specify a question in the *Enter a question* field.

2 Specify an answer in the *Enter the answer* field.

3 Specify the answer again in the *Confirm the answer* field.

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

NOTE: When you upgrade, SecureLogin stores all users data, including the user's passphrase question and response, from the previous version, so you do not need to re-create the passphrase.

You can create passphrase questions for users to select from in a directory environment; however, because you are the first SecureLogin user, you must create your own passphrase question.

5.4.4 Installing for Mobile Users and Notebook Users

Installing Novell SecureLogin for mobile and remote users use the same procedure as Section 5.4.2, "Installing On a User Workstation," on page 72.

However, it is important to ensure that the cache is saved locally, or users cannot access applications when they are disconnected from the network. The *Enable cache file* setting in the *Preferences* option is set to *Yes* by default. You can set this at either the Organization Unit level or on a per-user basis.

5.4.5 Configuring Roaming Profiles

Enterprises often create roaming profiles for specific groups of users, defined by their organizational role or function. For example, field engineers connecting from remote locations or accounting staff working at different locations setting the path to the target user's profile path.

For more information on creating roaming profiles in an Active Directory environment, see the Microsoft Support Web site. (http://support.microsoft.com/kb/314478)

NOTE: During loading, the Novell SecureLogin loads the user's profile effectively locking that profile and preventing the user's credential data from being copied to their roaming profile.

To prevent the Novell SecureLogin from causing problems with the existing user roaming profiles, you must manually force the Novell SecureLogin not to encrypt the user's credential data by using the Microsoft's Data Protection API (DPAPI).

Configuring the Novell SecureLogin for use with roaming profiles requires additional support for a successful deployment. Contact Novell Support for assistance.

Installing in an ADAM Environment

6

Active Directory Application Mode (ADAM) is an LDAP directory service that runs as a user service, rather than as a system service. This section contains information on installing SecureLogin in an ADAM environment.

This section contains information on the following:

6.1 Using Active Directory and ADAM

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

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

6.2 Prerequisites

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

NOTE: If the ADAM instance is deployed by using the `adamconfig.exe` file that has been copied from the Novell SecureLogin installer package, then administrators will need to copy the entire folder containing the ADAM Schema and Configuration files to their preferred location. The ADAM Schema and configuration files must all be located in the same folder, for ADAM instance to successfully deploy.

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

6.3 Using Active Directory and ADAM

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

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

For information about ADAM, see the Microsoft Web site. (http://www.microsoft.com/windowsserver2003/adam/default.mspx)

6.4 Installation Overview

Before proceeding with installing Novell SecureLogin in ADAM mode, make sure that the following prerequisites are in place.

- Install Windows 2003 or Windows XP, including Active Directory.
- Assign permissions to a Network Service Account.
- Create an ADAM instance.
- Back up the Active Directory server.
- n multi-directory environments you need to identify the domain controller in order to determine which directory to synchronize Novell SecureLogin user data with and to determine the order of replication.

NOTE: Secure Workstation is not supported in ADAM installation of Novell SecureLogin.

If the ADAM instance is deployed by copying and running the `adamconfig.exe` file from another location, you need to copy the entire folder containing the ADAM schema and configuration files to the their preferred location. The ADAM Schema and configuration files must all be located in the same folder for the ADAM instance to successfully deploy.

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

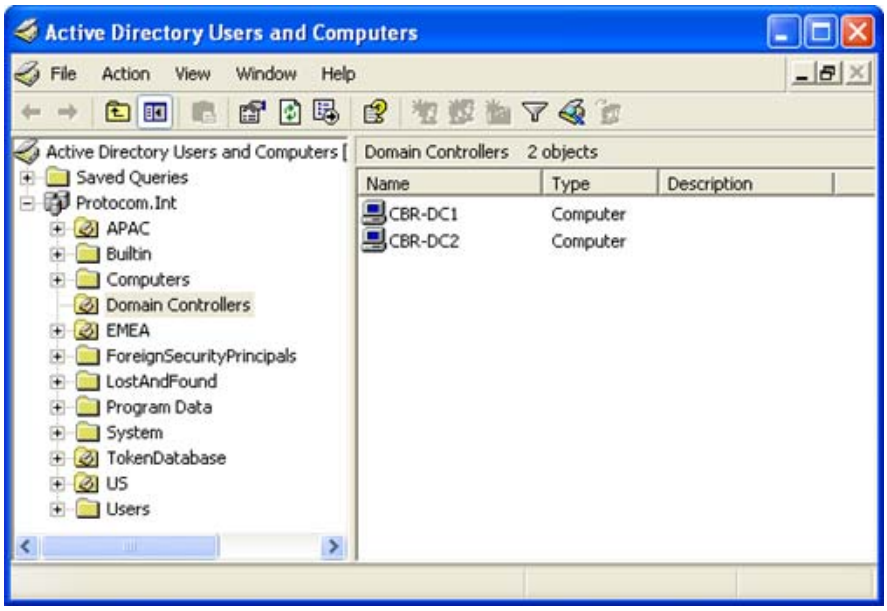
6.4.1 Creating a Network Service Account and Assigning Permissions to It

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

Creating a Network Service account enables the ADAM instance. For information on creating the ADAM instance, see Section 6.5.1, "Creating an ADAM Instance," on page 80.

To create a Network Service account and assign permissions to it:

1. Click *Start* > *All Programs* > *Administrative Tools* > *Active Directory Users and Computers*. The Active Directory Users and Computers page is displayed.



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

NOTE: Selecting *Delete All Child Objects* has no effect for Novell SecureLogin, but allows the ADAM instance to be cleaned properly when it is uninstalled.

9 Click *OK* to close the [Domain] Properties dialog box.

6.4.2 Configuring the ADAM Schema

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

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

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

For more information about the Novell SecureLogin schema attributes, see the *Novell SecureLogin 6.1 SP1 Administration Guide*.

6.5 Creating and Configuring an ADAM Instance

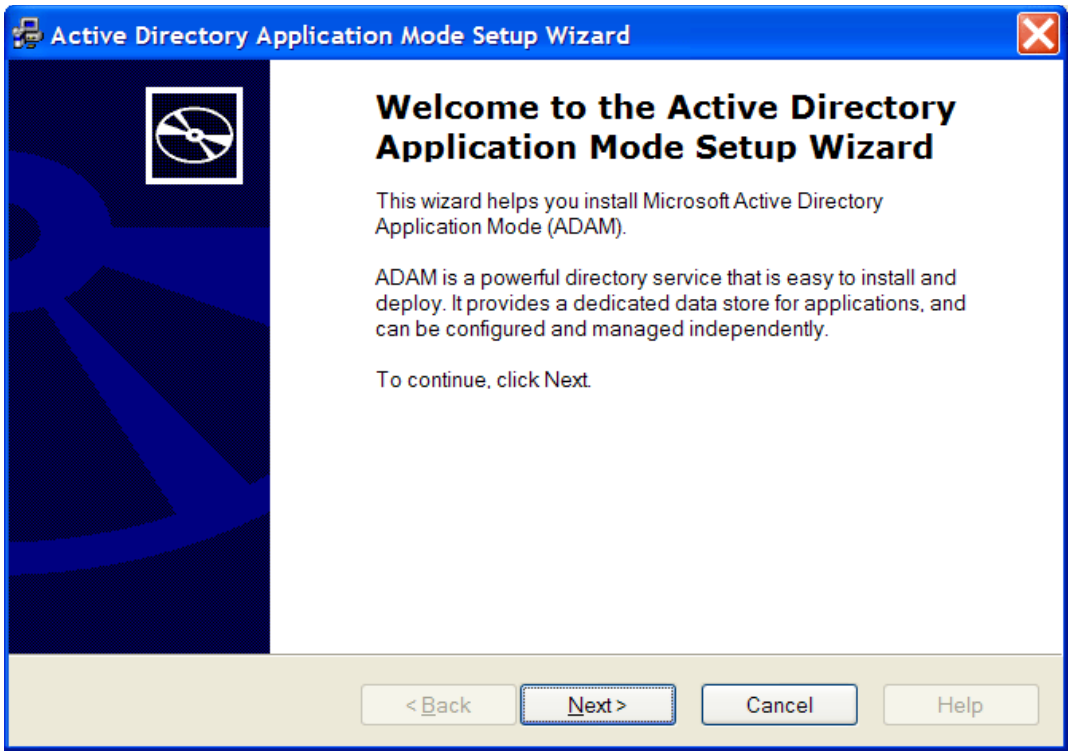
This section contains information on the following:

6.5.1 Creating an ADAM Instance

The ADAM setup files are provided in the `Tools` folder of the Novell SecureLogin installer package.

To create an ADAM instance for Novell SecureLogin:

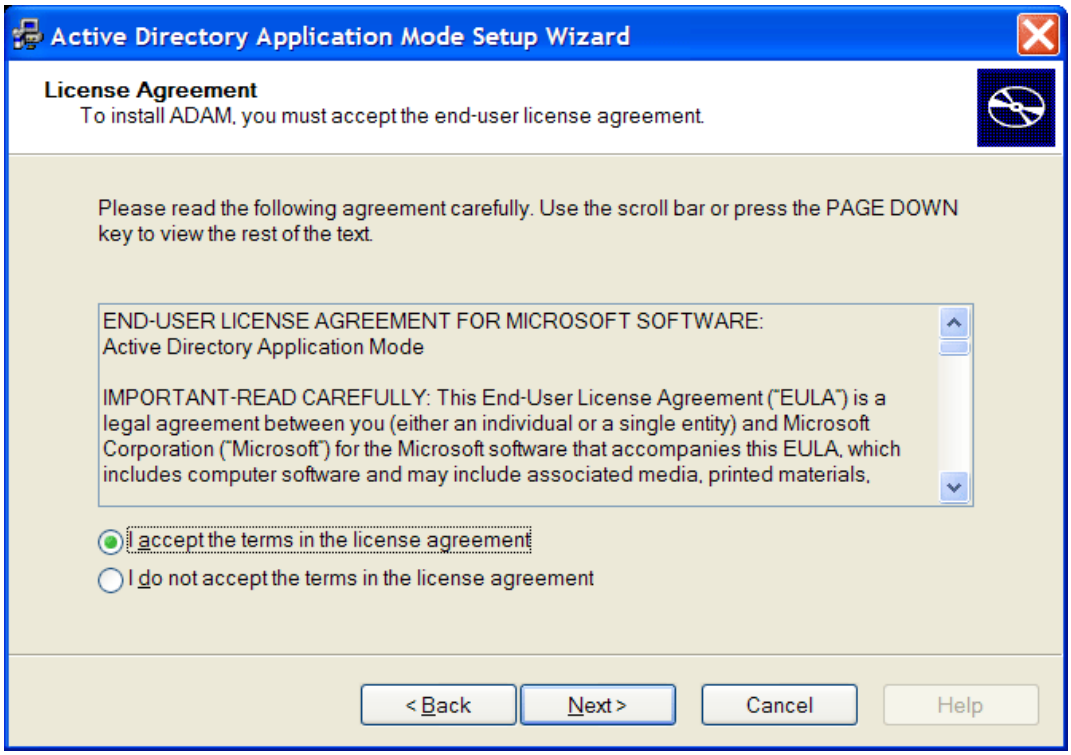
1 Double-click the `adamsetup.exe` file. The Active Directory Application Mode Setup Wizard is displayed.



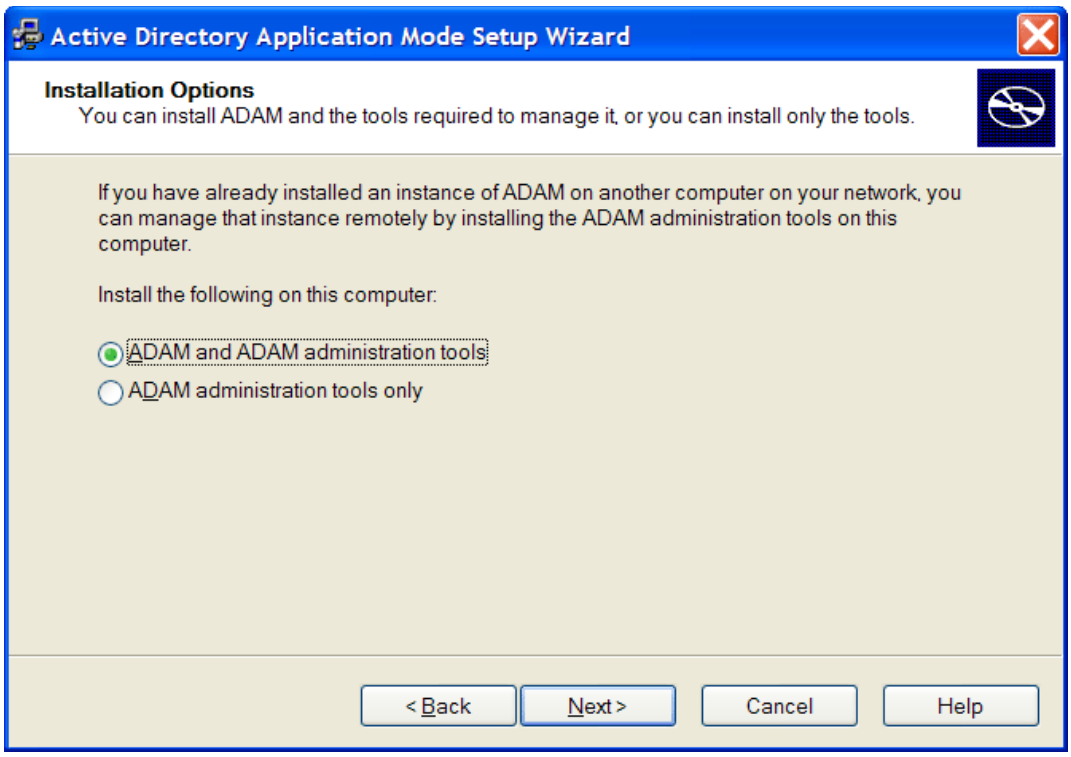
2 Click the *Next* button. The License Agreement dialog box is displayed.

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

The Installation Options dialog box is displayed.

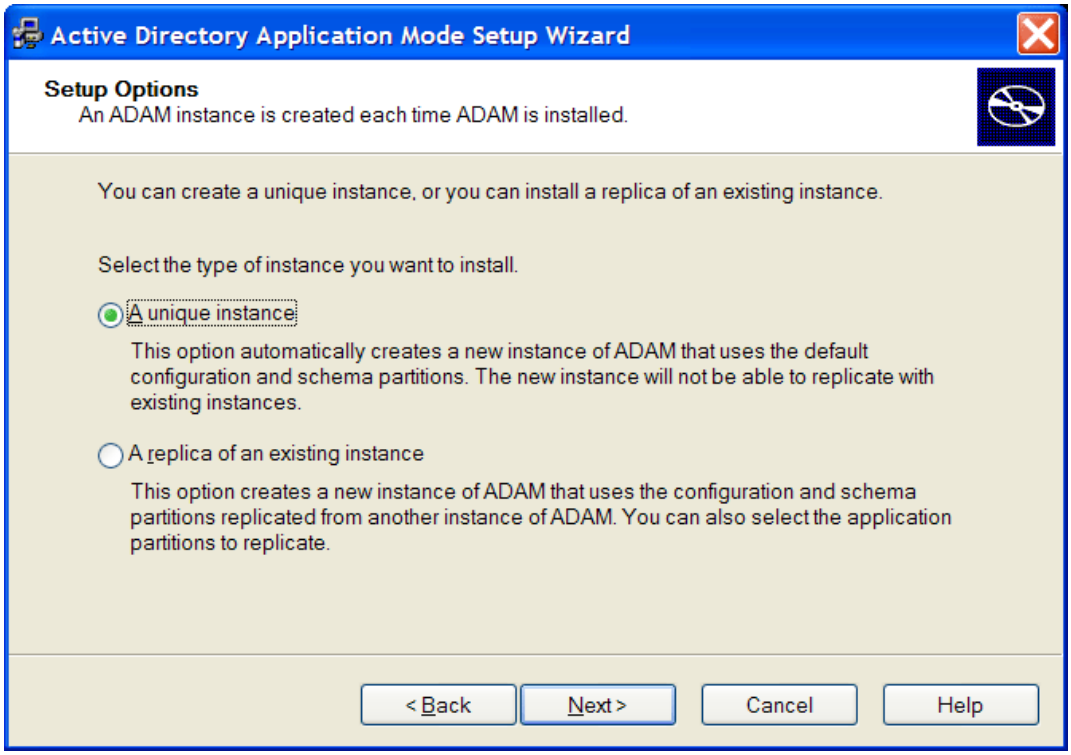


4 Select the *ADAM and ADAM administration tools* option.



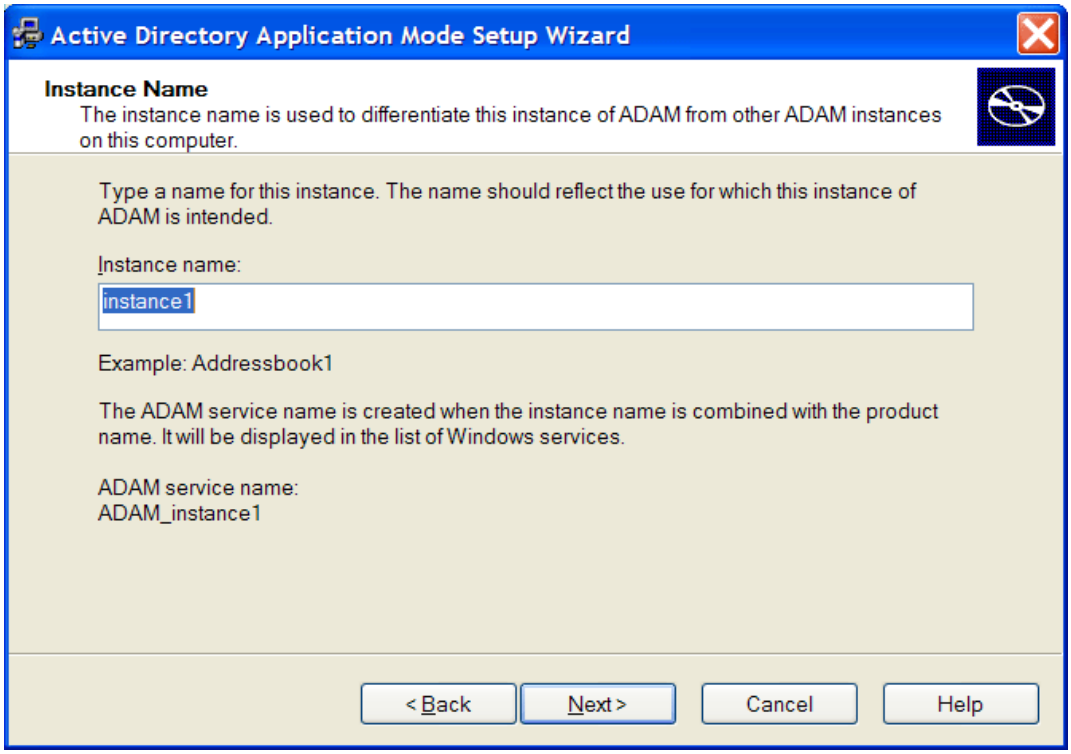
5 Click *Next*. The Setup Options dialog box is displayed.

6 Select the *A unique instance* option.



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

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

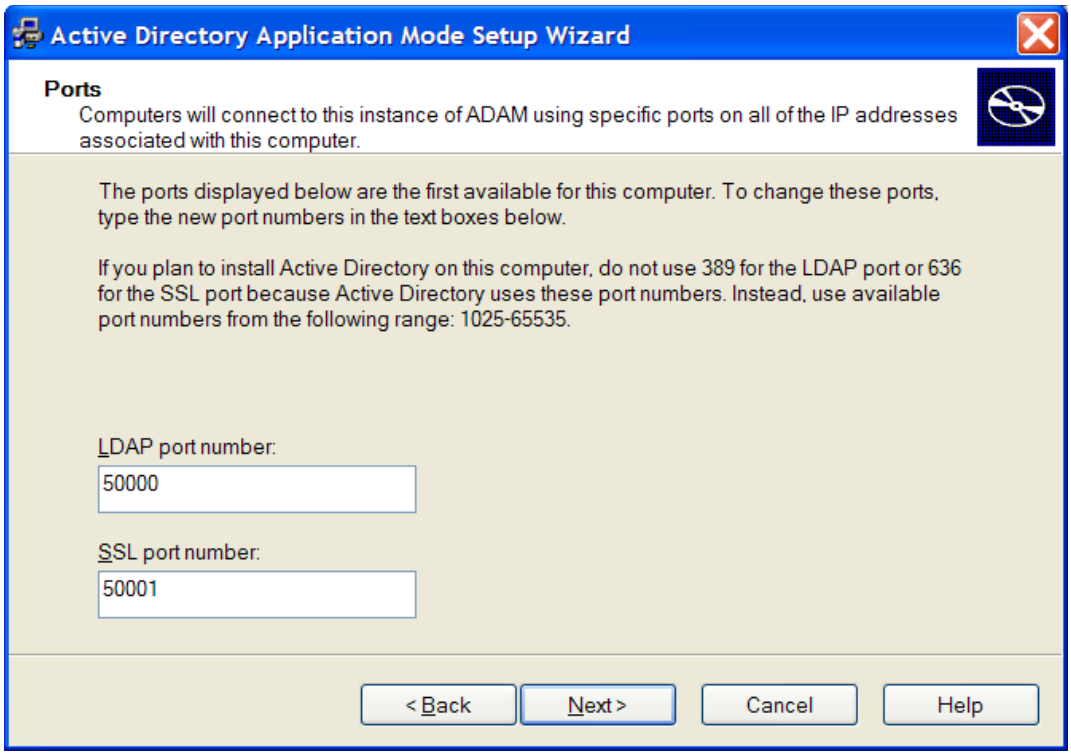


9 Click *Next*. The Ports page is displayed.

10 Specify the ADAM instance port number in the LDAP port number field and specify the ADAM instance SSL port number in the SSL port number field.

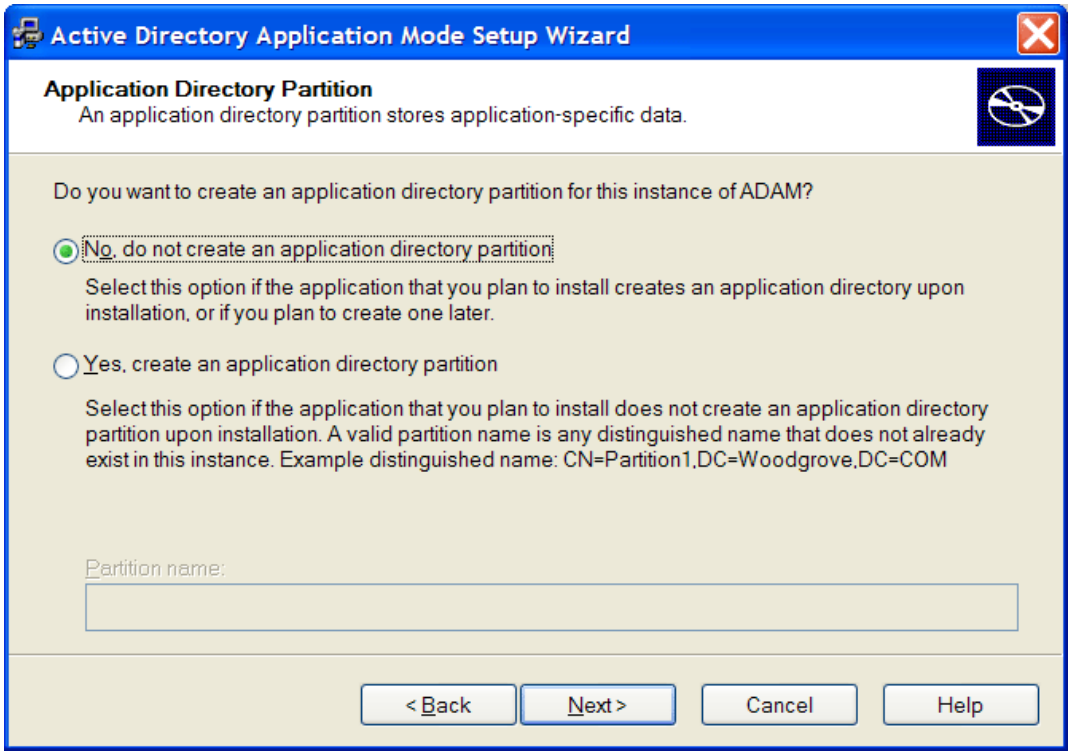
The default LDAP port number is 50000 and the SSL port number 500001. If Active Directory is not installed on the computer, the default will be LDAP port number 389 and SSL port number 636. The default values are recommended; however, the port numbers can be manually configured.

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



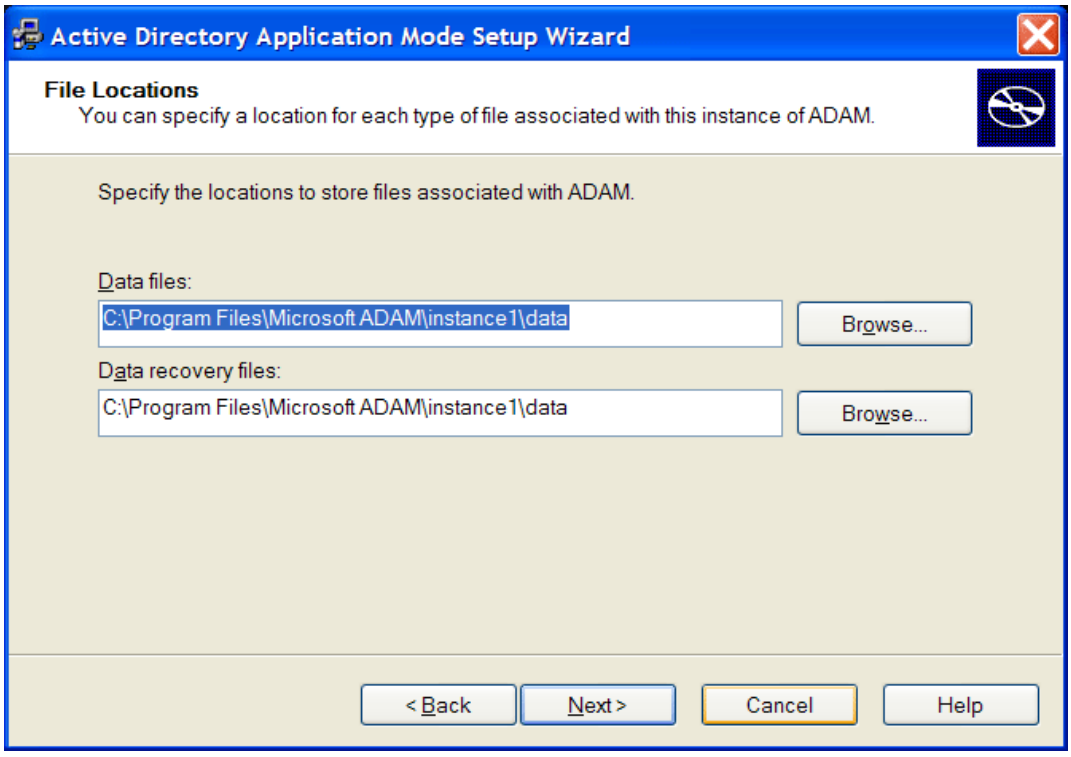
11 Click *Next*. The Application Directory Partition page is displayed.

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



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

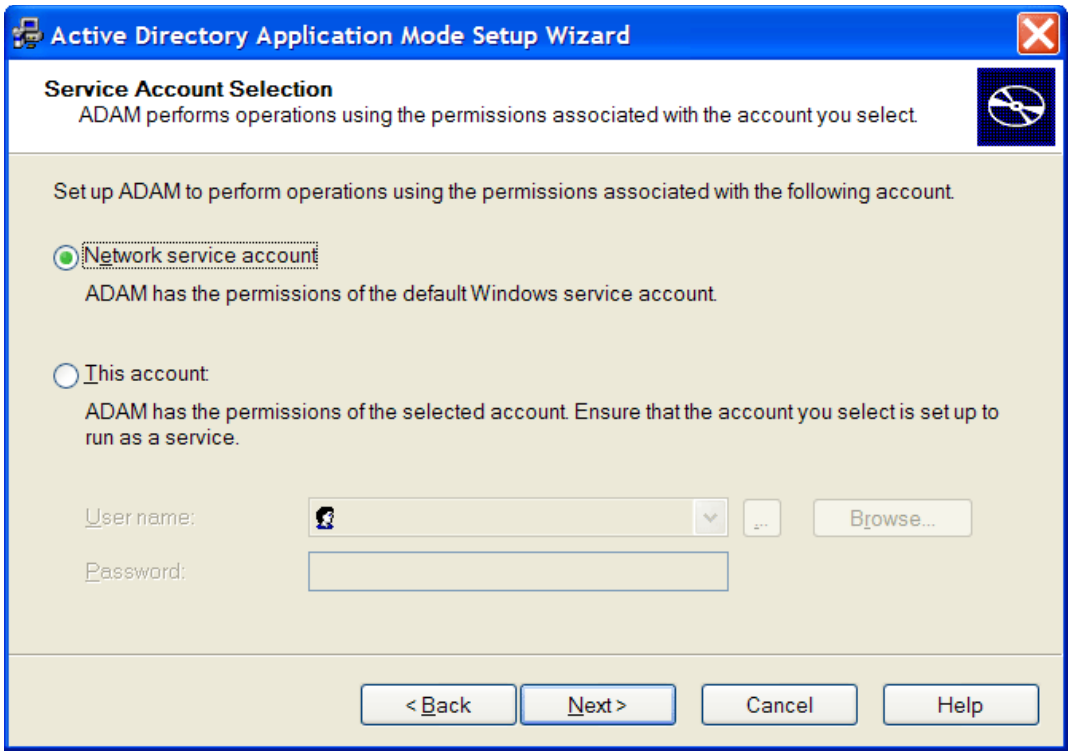
14 Specify alternative locations for ADAM files in the *Data files* and *Data recovery files* fields, or accept the default values.



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

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

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

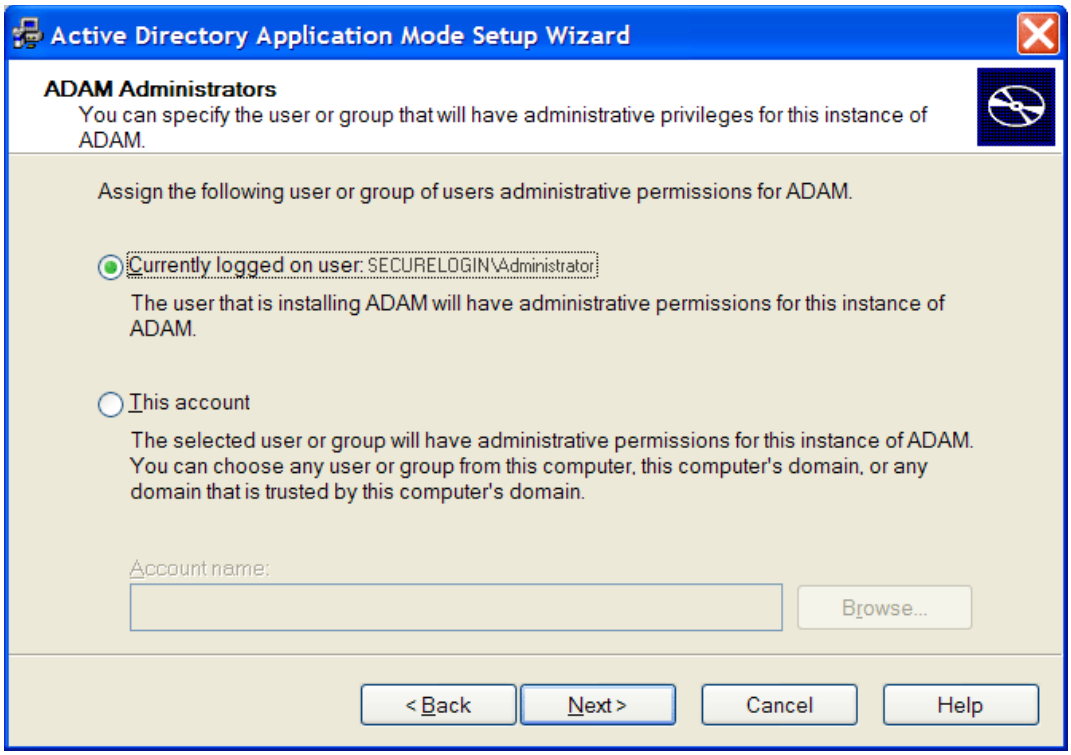


17 Click *Next*. The ADAM Administrators page is displayed.

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

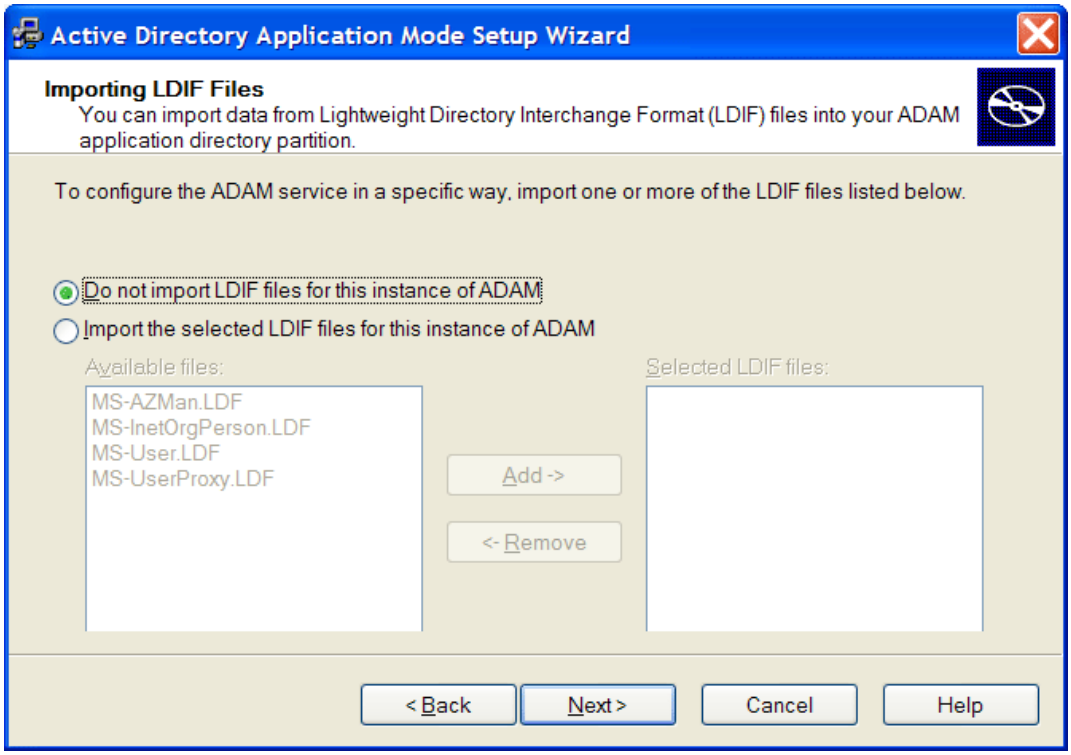
The account selected needs administrator level permissions for the ADAM instance. In this example, the default is selected as the current user, so the Administrator will administer this ADAM instance.

If an alternative account or group is preferred, select and provide the account or group name and credentials.



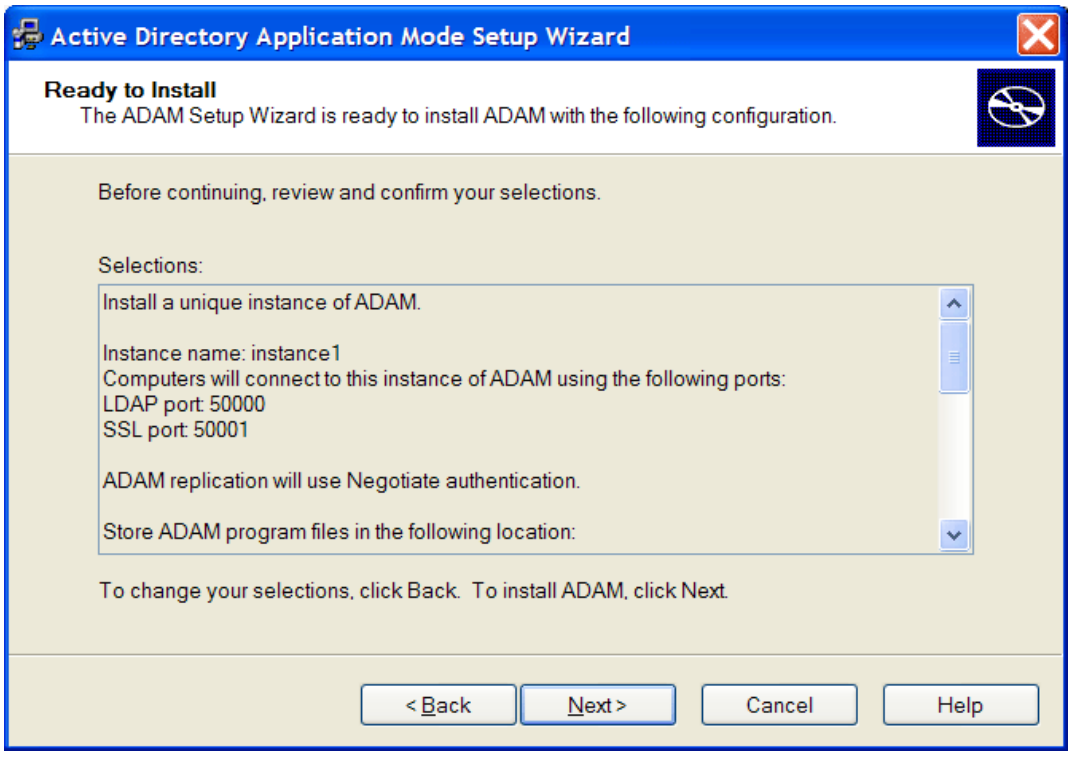
19 Click the *Next* button. The Importing LDIF Files page is displayed.

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



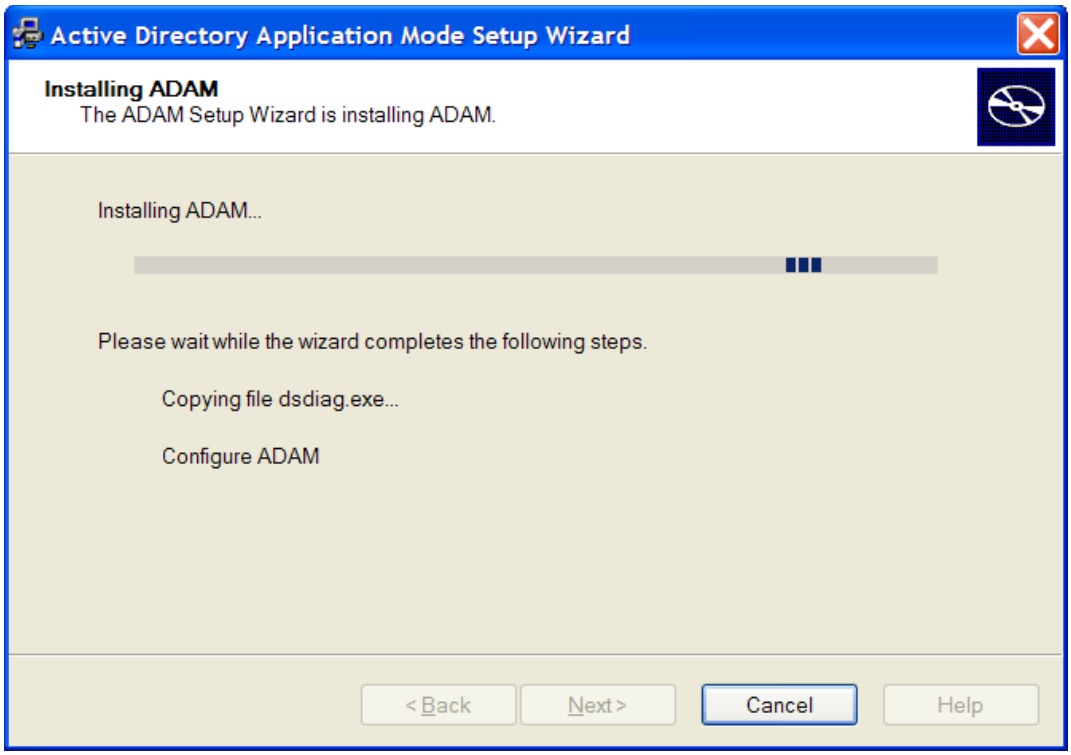
21 Click *Next*. The Ready to Install page is displayed.

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

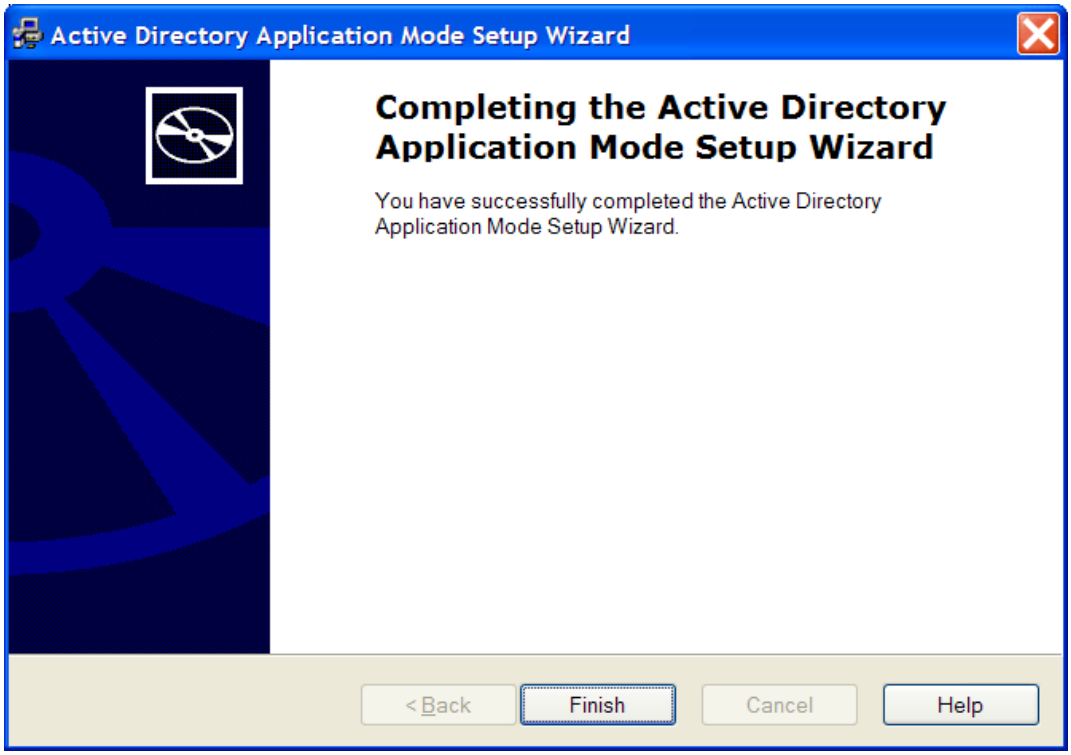


22 Click *Next* to continue or *Back* to change selected options.

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



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



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

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

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

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

6.5.2 Using the ADAM Configuration Wizard

Before executing the Novell SecureLogin ADAM Configuration Wizard:

1 Navigate to the `SecureLogin\Tools` folder of the Novell SecureLogin installer package.

2 Copy the `ADAMconfig` folder to your local drive

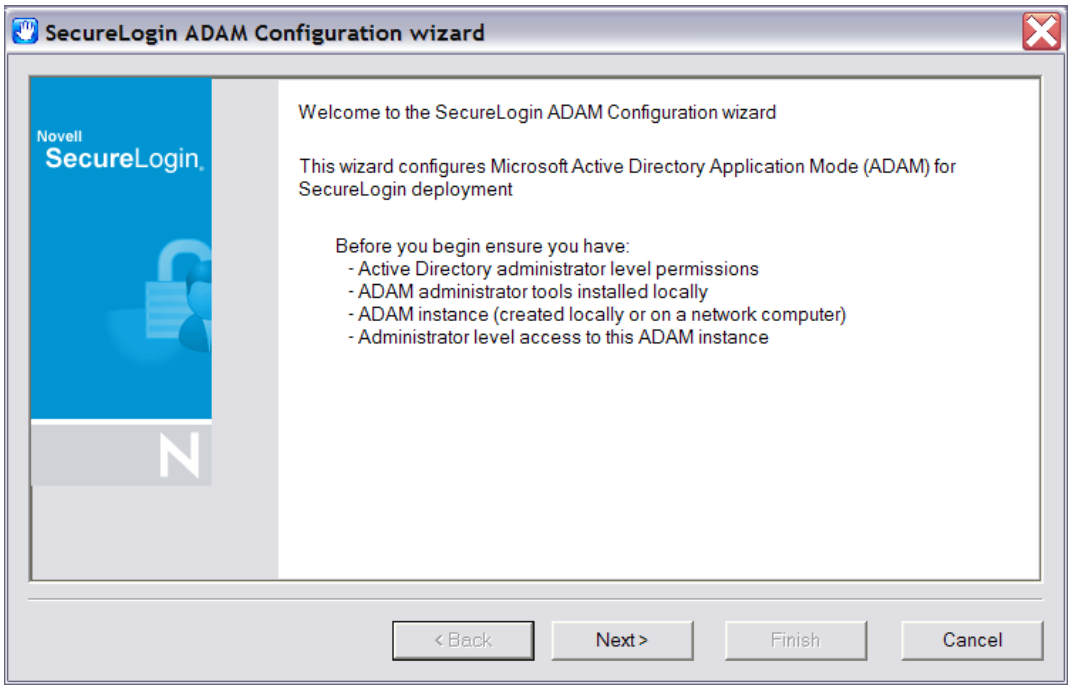
The Novell SecureLogin ADAM Configuration Wizard extends the ADAM Directory Schema with Novell SecureLogin Single Sign-On attributes, creates ADAM partitions, and assigns selected directory objects Read and Write permissions to the Novell SecureLogin attributes. The Wizard creates corresponding user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

To run the Novell SecureLogin ADAM Configuration Wizard:

1 Log in to the ADAM instance or server or to the administration workstation if it is a separate machine or as a user with Administrator access.

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

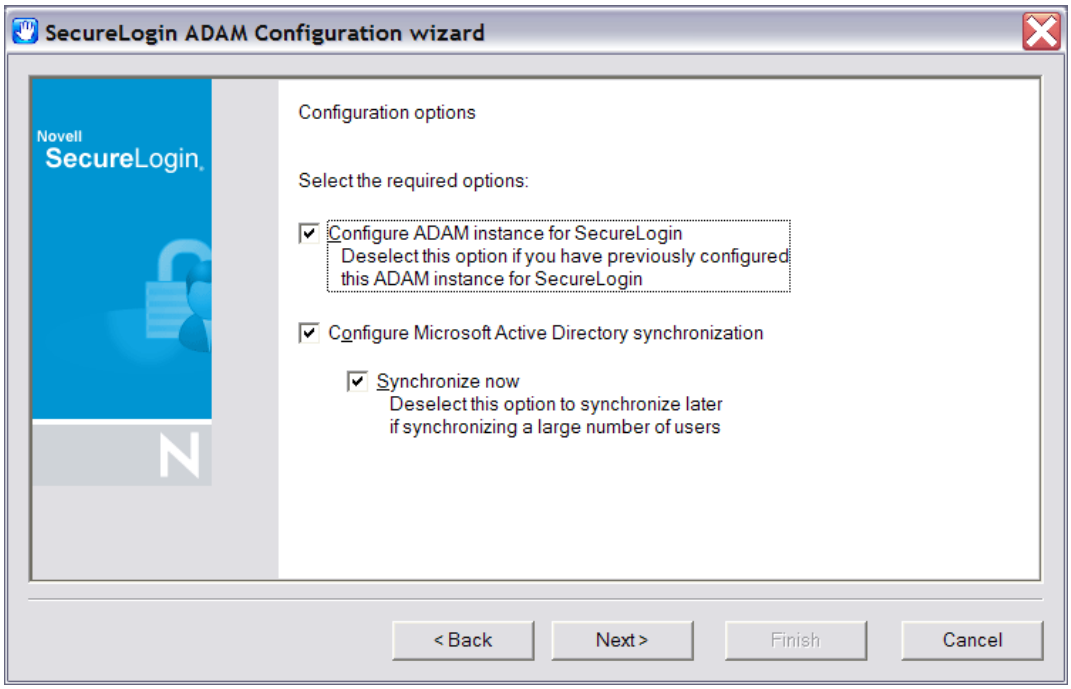
The Welcome to the Novell SecureLogin ADAM Configuration Wizard page is displayed. Ensure that you have all the required Active Directory and ADAM Administrator account details selected during ADAM instance creation.



3 Click *Next.*

The ADAM schema can be extended manually at the command line using the `MS-UserProxy.LDF` and `sso-adam-schema.LDF` files. These files are located in the `Tools` folder of the Novell SecureLogin installer package. We recommend that you perform this procedure with the assistance of our consultants.

4 Select the *Configure ADAM instance for Novell SecureLogin* option on first execution of the Novell SecureLogin ADAM Configuration Wizard.



Although configuration is required only once, you can select this option again with no adverse affects.

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

Directory synchronization of a large number of users can adversely affect network performance. Make sure you select a time to run the Novell SecureLogin ADAM Configuration Wizard when the network is less busy, in order to minimize these effects.

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

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

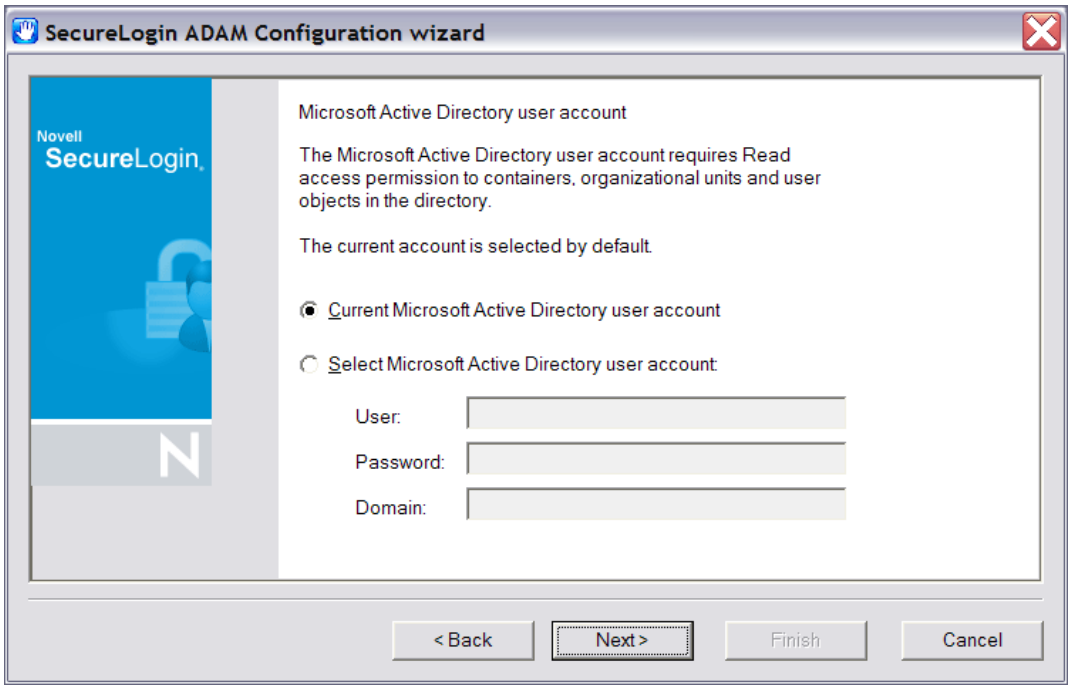
6 Select the *Synchronize now* check box if necessary.

Each time a new organizational unit is created in Active Directory, the Novell SecureLogin ADAM Configuration Wizard or the `SyncAdam.cmd` command file must be executed to synchronize with the ADAM Instance and assign Read and Write permissions. For more information refer to section Section 6.5.4, “Synchronizing Data from Active Directory to an ADAM Instance,” on page 96.

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

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

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



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

9 Accept the default values or specify the alternative Server and Port values as required, then click *Next*.

- The default server value is localhost. Select an alternative server if you are hosting your ADAM instance on another computer.
- The default port is 50000. Specify an alternative port number if this is not the ADAM instance server port.

The Microsoft Active Directory containers/organizational units dialog box is displayed.

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

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

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

12 Click *OK*.

13 The ADAM Configuration error message box is displayed if the distinguished name of the domain, container or organizational unit specified is invalid. If this occurs, click the *OK* button. Specify the correct name in the *Enter distinguished name of domain, container or organizational unit* field and click *OK*.

14 Click *Next* when all required objects are added to the list. The Configuration summary dialog box is displayed

Review your selected configuration options.

15 Click *Back* to change details or click *Finish* finish the configuration.

The Novell SecureLogin ADAM Configuration - Termination dialog box is displayed if the configuration was not able to complete successfully. If this occurs, review the text box to investigate cause of termination. If a solution to the problem is determined, click *Close* and repeat execution of the Novell SecureLogin ADAM Configuration Wizard.

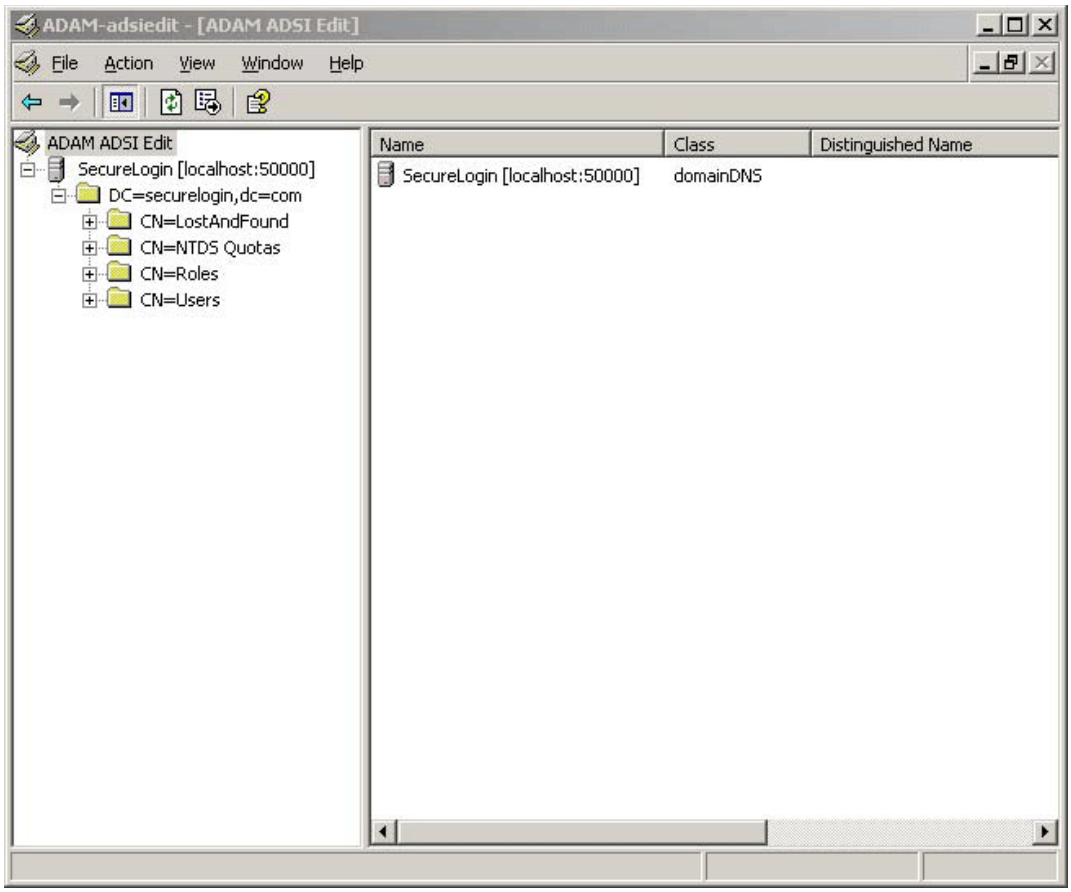
When configuration is complete, the Novell SecureLogin ADAM configuration - Finished dialog box is displayed.

16 Click *Close*.

6.5.3 Using the ADAM ADSI Edit Tool

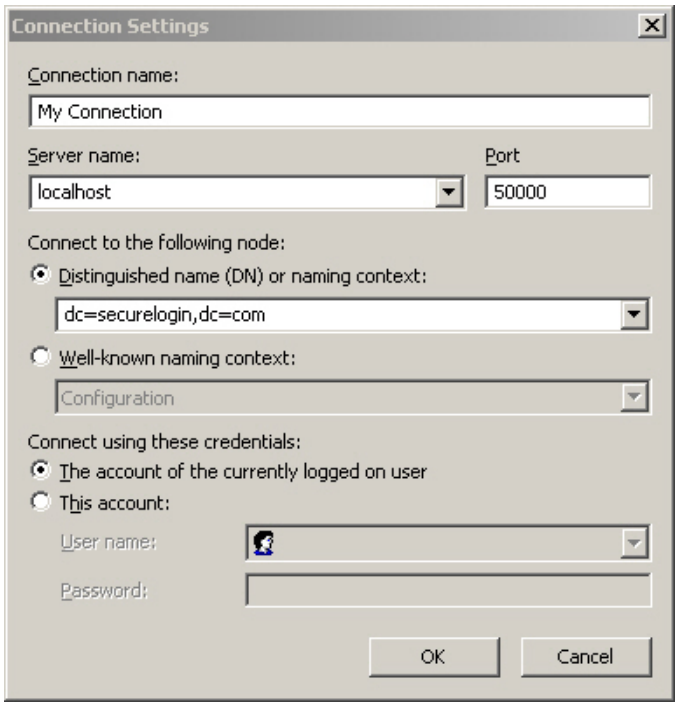
The ADSI Edit tool is an MMC plug-in used to view all objects in the directory (including schema and configuration information), modify objects, and set access control lists on objects. You can use it to check and review the Novell SecureLogin ADAM configuration.

1 Click *Start* > *Programs* > *ADAM* > A*DAM ADSI Edit*. The ADAM ADSI Edit tool is displayed.



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

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



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

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

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

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

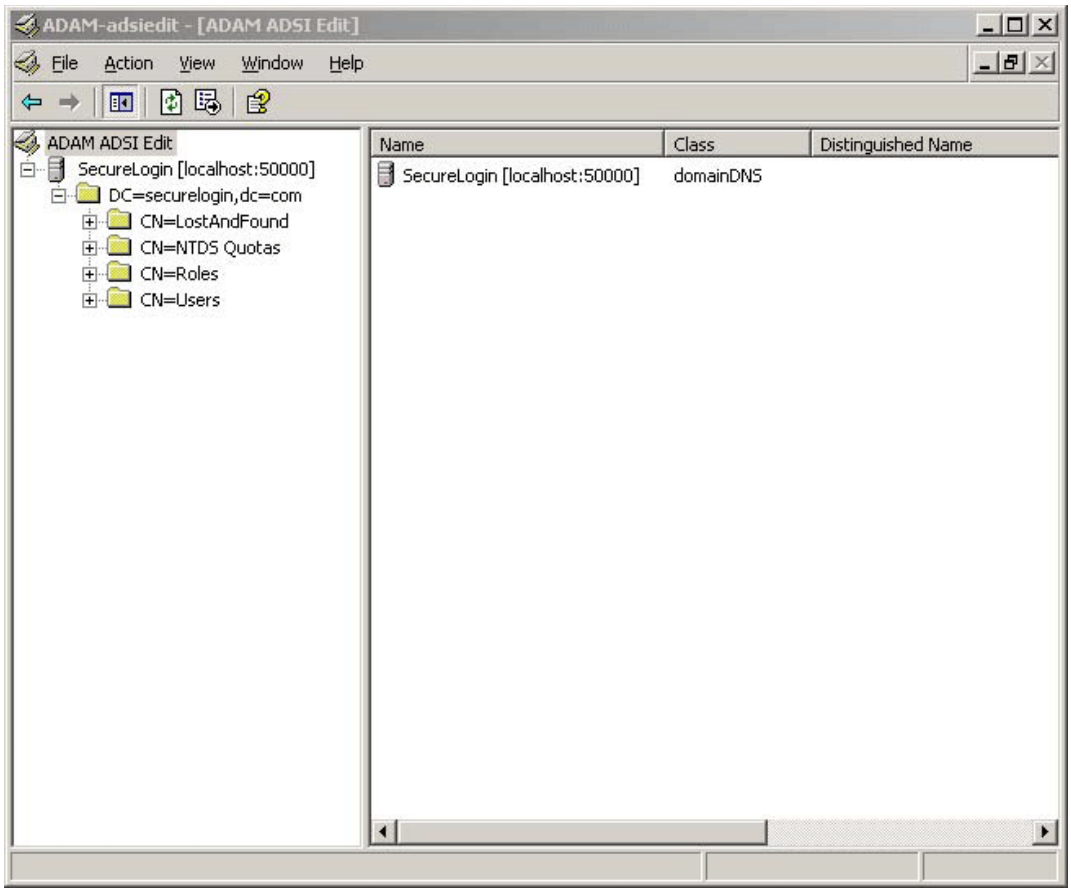
8 Specify the Distinguished Name in the *Distinguished name* (DN) or naming context field.

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

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

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

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



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

12 To confirm that the schema attributes have been added successfully, scroll down the Attributes table window to display the six single sign-on attributes.

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

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

Contact Novell Support for assistance if required.

6.5.4 Synchronizing Data from Active Directory to an ADAM Instance

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

To synchronize data from Active Directory to an ADAM instance:

1. Open the folder where you copied the ADAM files, then double-click the `syncadam.cmd` file. It is advisable to run the synchronization method on a regular basis, or when Active Directory users are changed. One way to do this is to add the process to the Windows Scheduled Tasks.
2. When the synchronization is complete, check the `SyncAdam.log` log file to make sure that the process was successful.

The following processes are automatically synchronized:

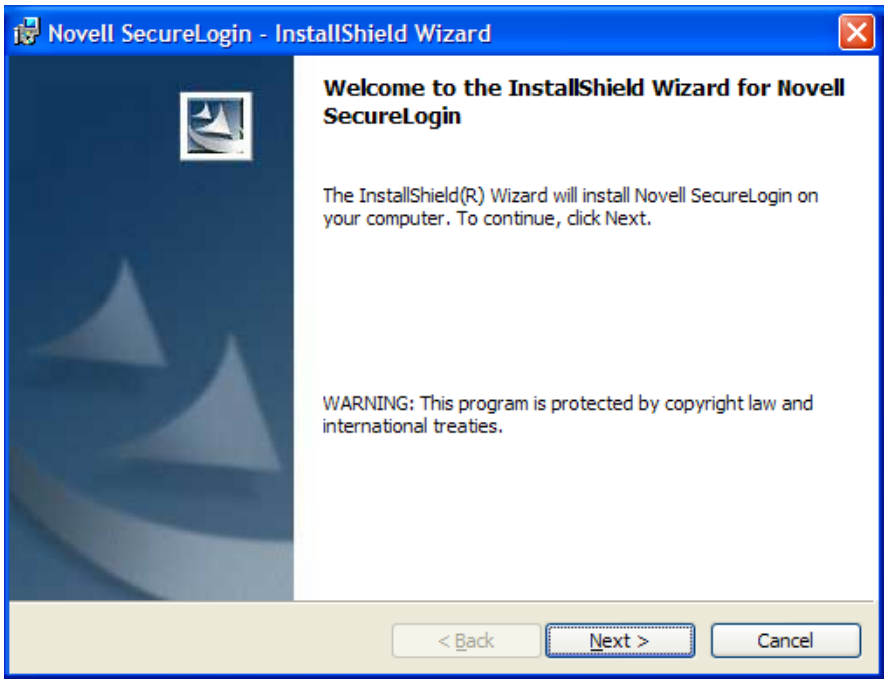
- A new container or organizational unit in Active Directory is created as a corresponding container in ADAM.
- A new user in Active Directory is created as ADAM user proxy.
- A renamed user object in Active Directory causes the corresponding user proxy to be renamed in ADAM.
- A moved user object in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

The following processes are not automatically synchronized:

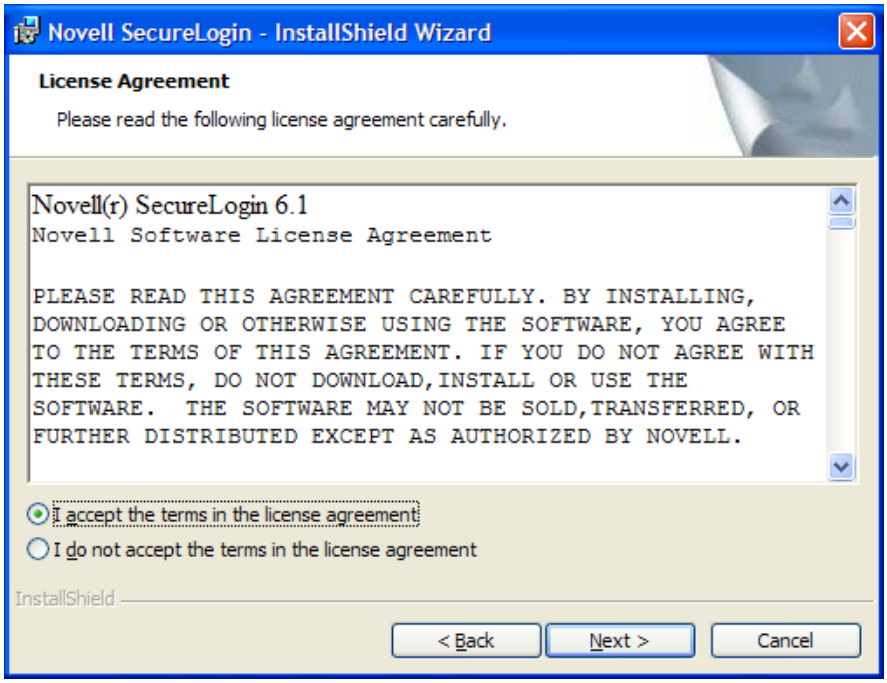
- Deleted user objects in Active Directory are not deleted in ADAM by default. This is because od security concerns. You can override this by manually editing `SyncAdam.config`. However, this is not recommended unless there is a good reason because username might conflict with a ‘zombie’ user, or performance issues.
- Deleted, moved, or renamed containers and organizational units in Active Directory are not synchronized to ADAM. Changes to existing container or OU objects in Active Directory must be manually synchronized to ADAM by using the ADSI Edit tool or any other directory editor. For example, if an OU is renamed in Active Directory, it must be renamed in ADAM. Because of security concerns, synchronization does not run if existing containers and OUs do not match in Active Directory and ADAM.

6.6 Installing Novell SecureLogin in the ADAM Environment

1. Run `Novell SecureLogin.msi`, found in the `\Securelogin\Client` directory of the installer package. The Welcome page is displayed.



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



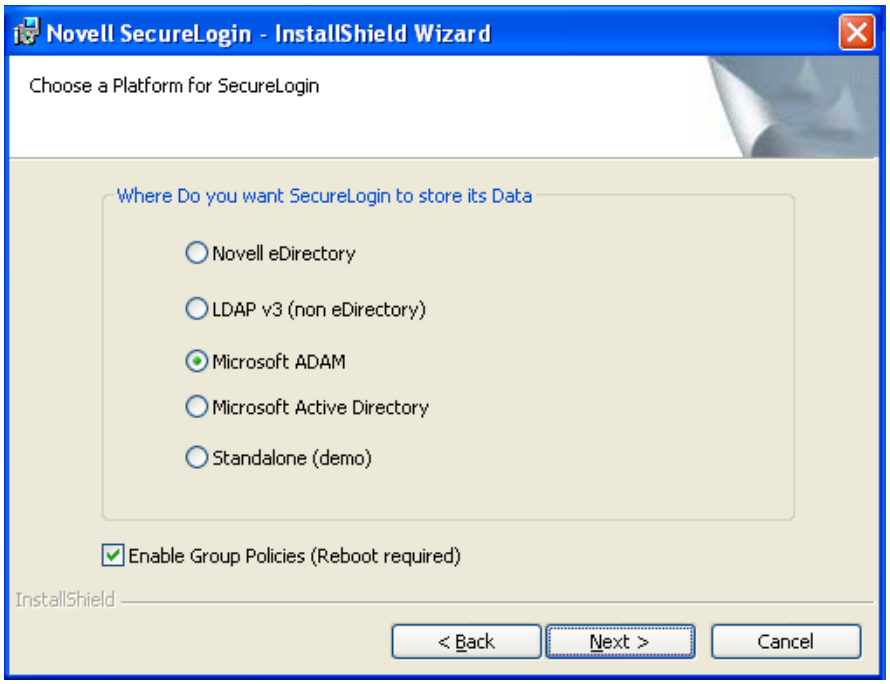
3 Select setup type, then click *Next*.

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

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

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

6 Click *Microsoft ADAM* > *Next*.



7 (Optional) Select *Enable Microsoft Active Directory Group Policies*.

NOTE: The group policies option is used where the ADAM directory is working along with Microsoft Active Directory or if Microsoft Active Directory is utilized for Novell SecureLogin in LDAP mode.

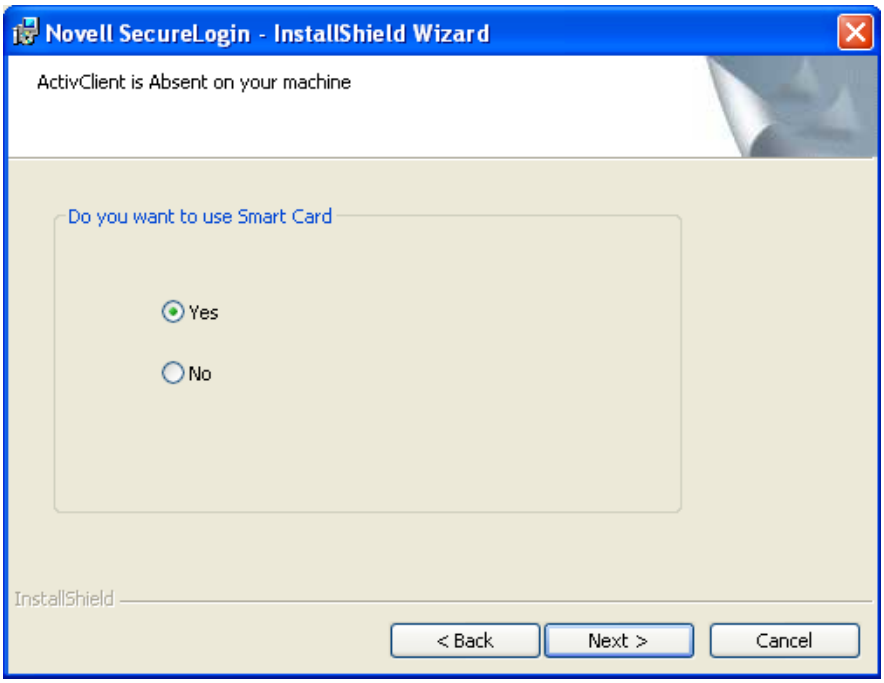
---

8 In the *Do you want to use smart card* dialog box, select *No*.

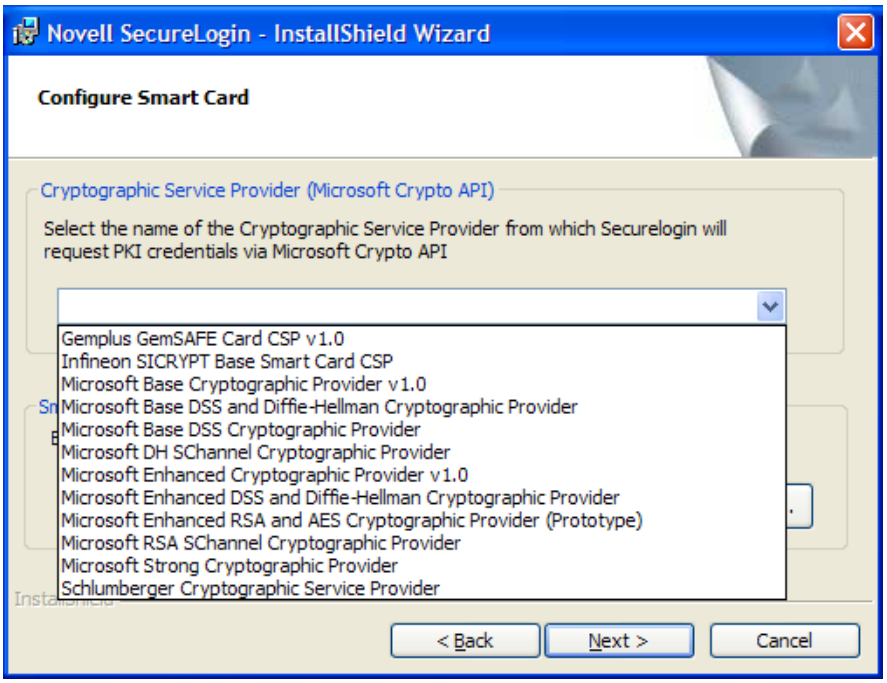
9 (Conditional) If you want to use smart card and if ActiveClient is detected in your system, select *Yes*, *Click*, then continue with Step 10.

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

10a Select *Yes*, Click *Next*.



10b (Conditional) Select a cryptographic service provider from which Novell SecureLogin will request PKI credentials via Microsoft Crypto API.



10c Click *Browse* and select a PKCS#11 compatible library required for accessing the smartcard, then click *Next*.

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

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

For more information and instructions about smartcard settings and cryptographic tokens, see the *Novell SecureLogin 6.1 SP1 Administration Guide*.

---

11 (Conditional) The Installation options dialog box is displayed if you have selected the *Custom* setup option.

Specify where you want Novell SecureLogin to store its local cache.

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

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

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

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

15 Select *Install Directory administration tools*.

The Directory administration tools are provided for corporate environments to manage users centrally at the directory.

16 If applicable, select *Install Citrix and Terminal Services support*.

This is highly recommended to enhance the performance of Novell SecureLogin in a Citrix environment.

17 Click *Next*. The cache location folder page is displayed.

IMPORTANT: Consider the following information before changing the cache location:

- The user's application data folder is the Triple DES or optionally AES encrypted repository for all Novell SecureLogin user data, which includes credentials, preferences, password policies, preconfigured applications, and application definitions.
- By default, Novell SecureLogin data is stored in both your organization's corporate directory and in the Novell SecureLogin offline cache on your workstation's hard drive. The data in the directory and the local cache are synchronized to ensure user data is always current.
- When the smart card is used to store application credentials, the credentials are stored on the smart card and directory only. The cache and directory contain the application definitions, policies, and settings for single sign-on.
- If smart cards are not used in the LDAP implementation, you can turn off the cache using an administrative preference so that the users access their single sign-on data from the directory only. This option has an impact on system performance.

---

18 If you want to change the location of the cache folder, select *Custom Location* > *Browse* and locate the an alternative folder.

19 Click *Next*. The Ready to install the program page is displayed.

20 Click *Install*. The installation process takes a few minutes. A confirmation message appears after the installation is complete.

6.7 Setting Up a Passphrase

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

During installation, the passphrase security is enabled to enforce passphrase setup during the initial login. You can disable the passphrase policy by deselecting *Use Passphrase Policy* option in the *Advanced Settings* pane of the Administrative Management utility.

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

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

WARNING: Remember the passphrase answer. If you forget the answer, it cannot be accessed.

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

After installing Novell SecureLogin successfully, when you attempt to log in to the workstation, you are prompted to set your passphrase question and answer.

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

6.8 Deploying

This section consists of information on the following:

6.8.1 Configuring a User’s Environment

Configuring a user’s Novell SecureLogin environment includes:

- Setting preferences
- Creating password policies (optional)
- Enabling required applications on Novell SecureLogin
- Creating of passphrase questions for user selection (optional)

It is recommended that Novell SecureLogin configuration is installed on test user accounts prior to deployment. For more information, see the *Novell SecureLogin 6.1 SP1 Administration Guide*.

Novell SecureLogin provides a range of options for deployment and distribution of user configurations. For more information, see the "Distributing Configurations" in the *Novell SecureLogin 6.1 SP1 Administration Guide.*

6.8.2 Managing Novell SecureLogin in an ADAM Instance

Novell SecureLogin users are managed in the Administrative Management utility. For more information on Novell SecureLogin administration, refer to the *Novell SecureLogin 6.1 SP1 Administration Guide*. The Administrative Management utility which is accessed via the *Start* menu, manages users at the container, organizational unit, and user object levels.

1. Access the Administrative Management utility.

   Refer section Section 10.1, "Accessing iManager," on page 145 for information on accessing the Administrative Management utility.
2. Specify the distinguished name of the required object. For example, CN=*users*, dc=*SecureLogin*, dc=*com*.
3. The Administrative Management utility options are displayed.

6.8.3 Installing Novell SecureLogin for Mobile Users and Notebooks

To install Novell SecureLogin for mobile and remote users, follows the procedure found in Section 6.6, "Installing Novell SecureLogin in the ADAM Environment," on page 97.

It is important that you save the cache locally. Otherwise, users who are disconnected from the network are unable to access the applications. By default, the *Enable cache* in the *Preferences properties* table option is set to *Yes*. You can set this at either the organizational unit level or on a per-user basis.

Installing on Standalone Workstations

7

This section provides information for installing Novell SecureLogin on a standalone workstation.

The instructions and examples given in the following sections apply to Microsoft Windows 2000 and 2003 Active Directory environments with a directory server managed through an administration workstation.

7.1 Installation Overview

The Novell SecureLogin standalone mode operates on a user’s workstation, which is independent of a network or, corporate directory system. In addition to providing a platform for Novell SecureLogin review and testing, the standalone mode is intended to provide Novell SecureLogin for individual workstations.

NOTE: You must have administrator access to the workstation.

---

1. Backup the existing workstation directory.
2. Uninstall any Novell SecureLogin version prior to 3.5.*x*.
3. Ensure that the Microsoft Management Console’s Active Directory plug-ins are installed on the administration workstation.
4. Define and configure the Novell SecureLogin environment, including enabling single sign-on of the required applications.
5. Copy test user configurations to relevant objects.
6. Install the Novell SecureLogin application on user workstation.

7.2 Microsoft Active Directory

This section has the following information:

7.2.1 LDAP Mode

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

To extend the Microsoft Active Directory schema and assign user rights, see Section 5.3.1, "Extending The Active Directory Schema," on page 59.

7.2.2 ADAM

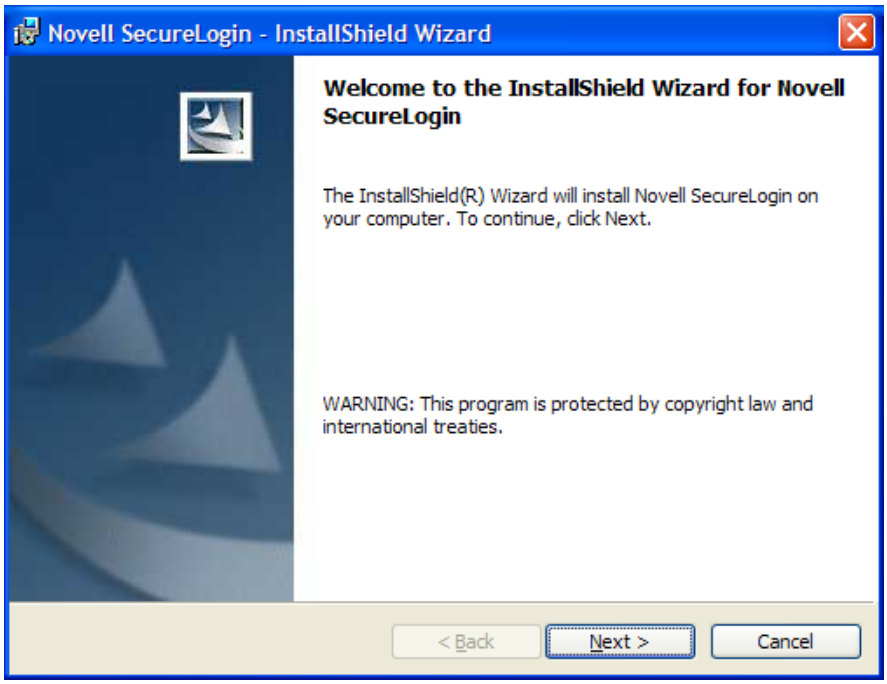
Novell SecureLogin supports installation in ADAM instance. For information, see *Novell SecureLogin 6.1 SP1 Administration Guide*.

7.3 Using the Complete Option to Install SecureLogin on a Standalone Workstation

Novell SecureLogin standalone operates on the workstation, independent of a network or corporate directory system.

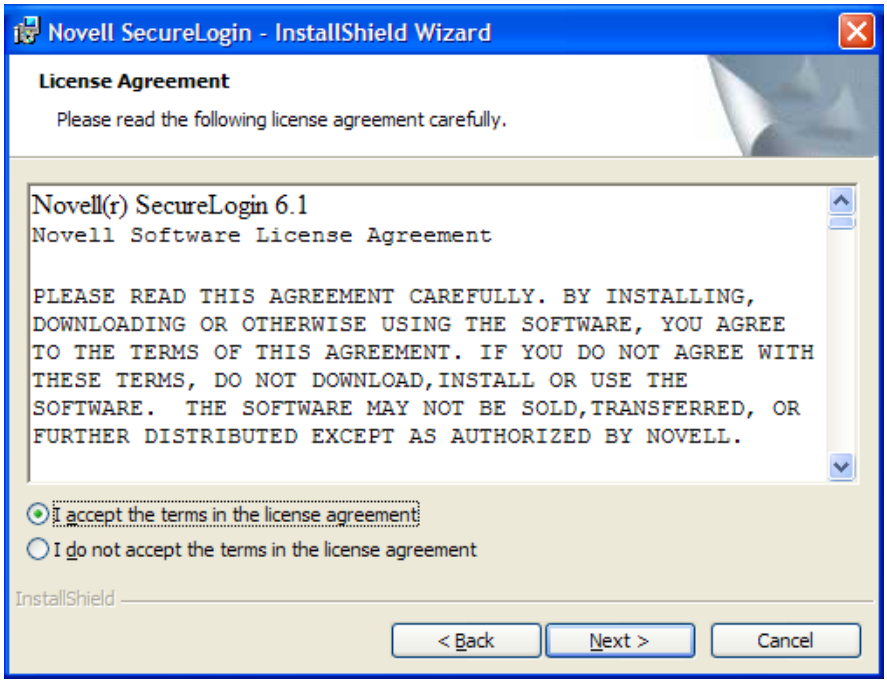
If you are installing Novell SecureLogin for the first time, follow the instructions given below:

1. Log in to the workstation as an administrator.
2. Run the `Novell SecureLogin.msi` file available in the `SecureLogin\Client` directory of the installer package. The Welcome page is displayed.



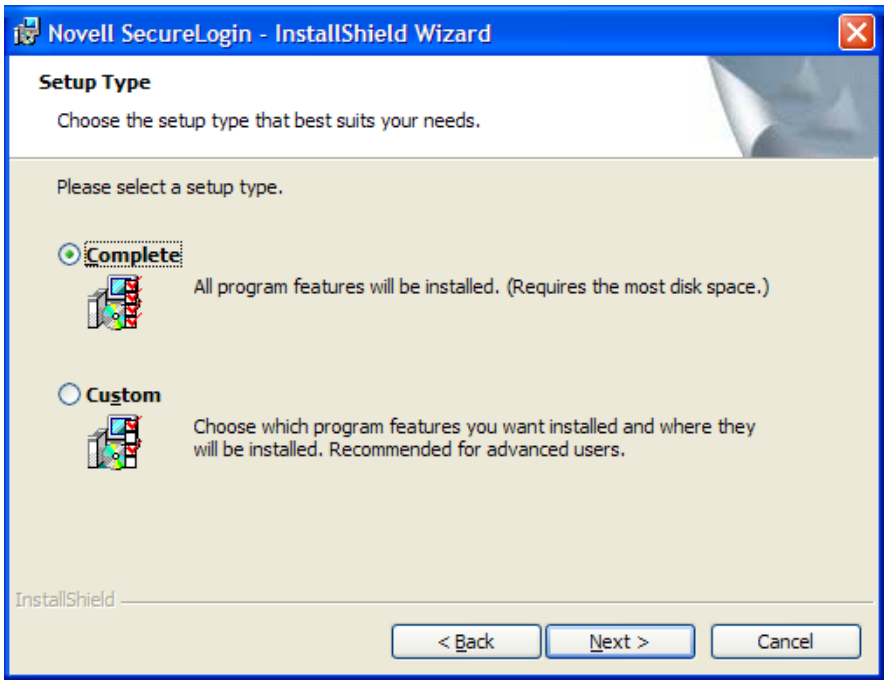
3. Click *Next*. The License agreement page is displayed.

4 Read the license agreement. Select *I accept the terms* in the license agreement if you want to proceed with the execution of the license agreement. If you do not want to proceed with the execution of the license agreement, click *Cancel* to quit the setup.

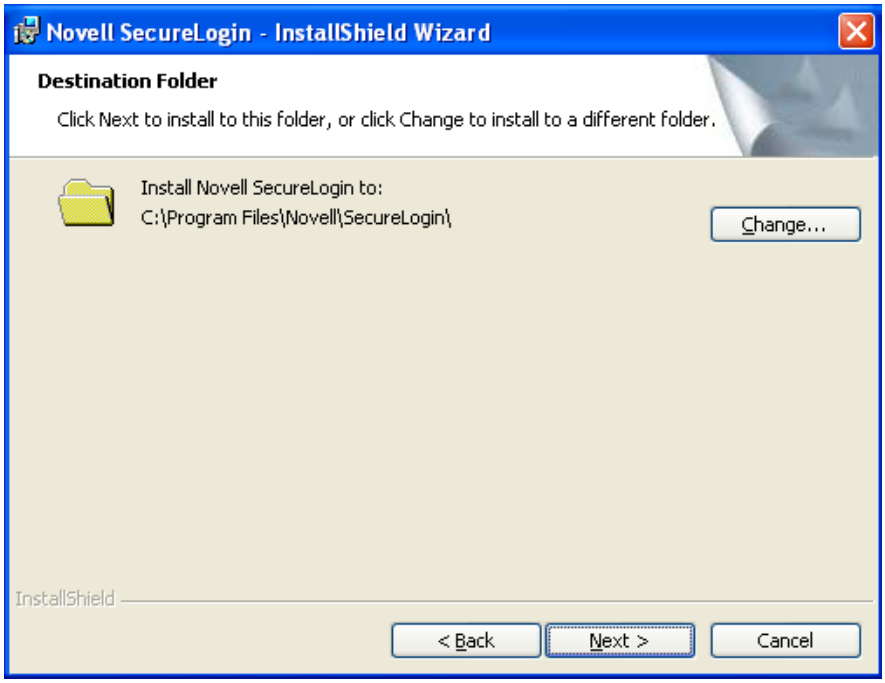


The *Complete* option uses default values and installs SecureLogin in *c:\program files\novell\securelogin*. For options available through the *Custom* option, see Section 7.4, "Using the Custom Option to Install SecureLogin on a Standalone Workstation," on page 111.

5 Click *Complete* > *Next*.

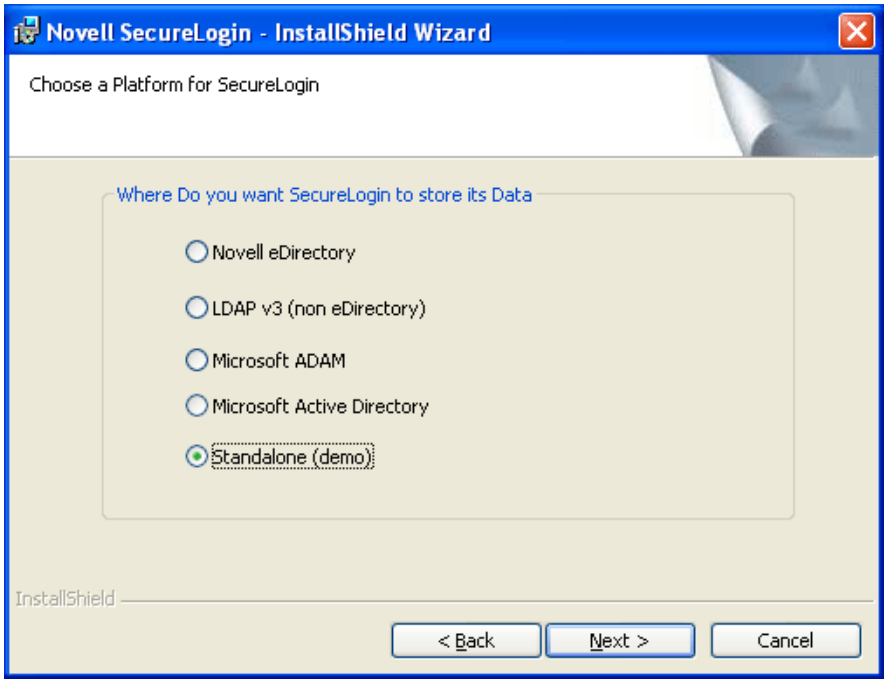


6 Click *Next*. The program location folder is displayed. The default location for Novell SecureLogin is, ..*Program Files**SecureLogin*\. If you want to change the location, click Change and select an alternative location for Novell SecureLogin on the drive.



7 Click *Next*. The installation environment page is displayed.

8 Select *Standalone*.



9 Click *Next*. The installation features page is displayed.

10 Select *Start SecureLogin at Windows startup*.

11 Click *Next*.The cache location folder page is displayed.

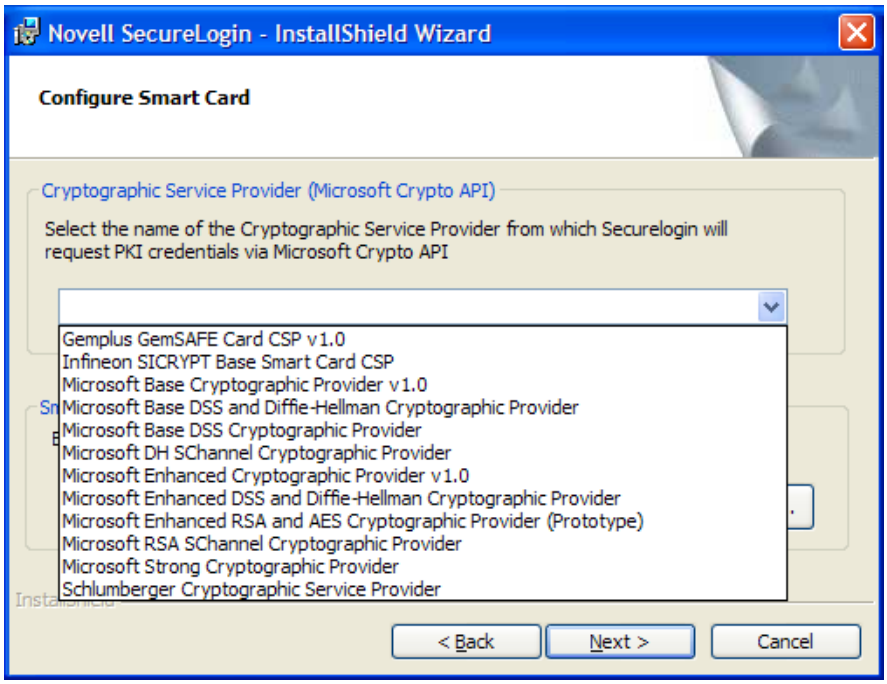
IMPORTANT: Consider the following information before changing the cache location:

- The user's application data folder is the Triple DES or optionally AES encrypted repository for all Novell SecureLogin user data, which includes credentials, preferences, password policies, preconfigured applications, and application definitions.
- By default, for standalone installations, Novell SecureLogin user data is stored in the offline cache on the local hard drive of the workstation.

---

12 If you want to change the location of the cache folder, select *Custom Location* > *Browse* and locate an alternative folder.

13 (Optional) Select a cryptographic service provider from which SecureLogin requests PKI credentials via the Microsoft Crypto API.



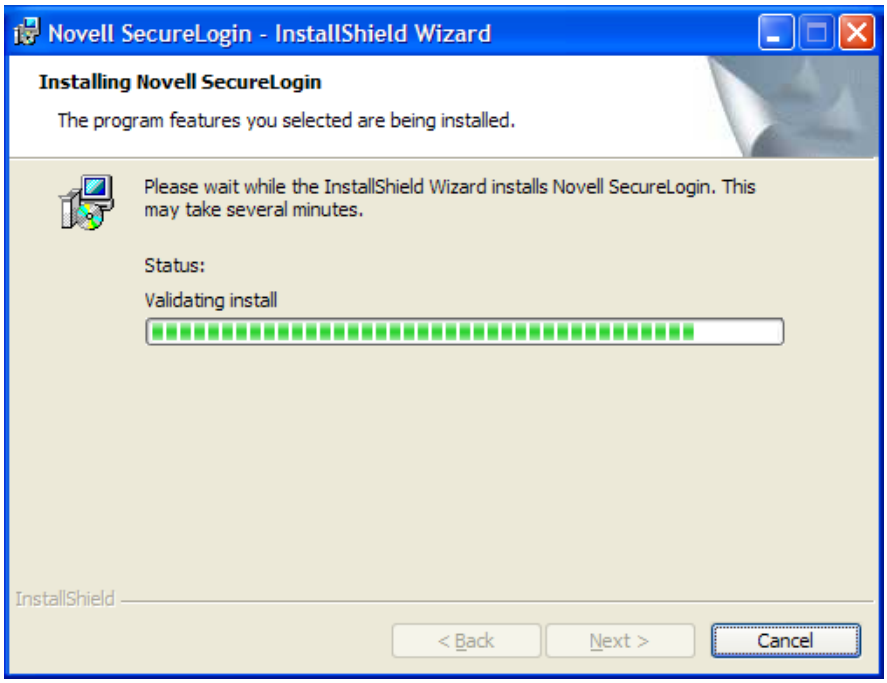
14 Click *Browse* and select a *PKCS#11 compatible library* required for accessing the smart card, then click *Next*.

This specifies the location of the Cryptographic Token Interface installed as part of the smartcard vendor's software. These API files are used by SecureLogin to communicate with the smart card.

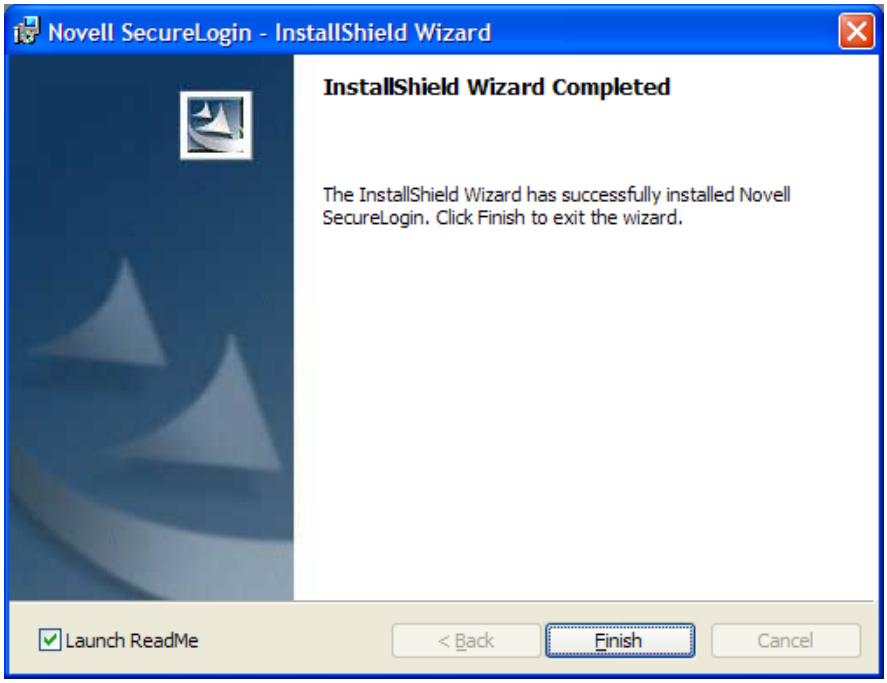
Manually configuring the third-party smart card PKCS library assumes a high level of understanding the Cryptographic Service Provider's product.

15 Click *Next*. The Ready to install the program page is displayed.

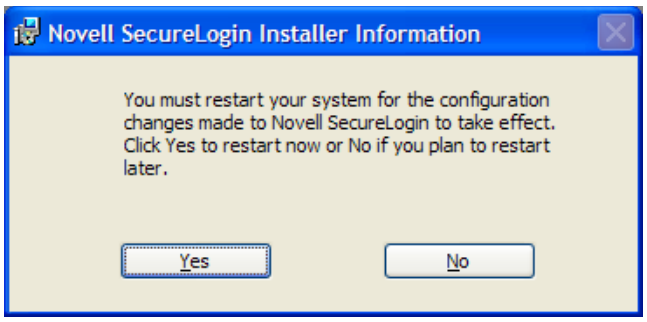
16 Click *Install*. The installation process takes a few minutes. A confirmation message appears after the installation is complete.



17 Click *Finish*. By default, the *Launch ReadMe* option is selected.



If you are prompted for a restart, click *Yes*. The computer is automatically restarted.



On login or restart, the Novell SecureLogin launches automatically and the Novell SecureLogin icon is displayed in the Windows notification area.

If you are upgrading from a previous version of Novell SecureLogin, follow the instructions given in Section 12.3, “Upgrading Novell SecureLogin,” on page 159.

7.4 Using the Custom Option to Install SecureLogin on a Standalone Workstation

The *Custom* option, which is the same as the procedure explained in the previous section, Section 7.3, “Using the Complete Option to Install SecureLogin on a Standalone Workstation,” on page 106. This type of installation provides the same defaults as does the *Complete* option, but enables you to do the following:

- Specify where SecureLogin files are stored.

  You can use the default path or specify a different one.
- Specify a path for to store the SecureLogin local cache.
- Select SecureLogin components.

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

7.5 Setting Up a Passphrase

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

During installation, the passphrase security is enabled to enforce passphrase setup during the initial login. You can disable the passphrase policy by deselecting *Use Passphrase Policy* option in the *Advanced Settings* pane of the Administrative Management utility.

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

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

WARNING: Remember the passphrase answer. If you forget the answer, it cannot be accessed.

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

After installing Novell SecureLogin successfully, when you attempt to log in to the workstation, you are prompted to set your passphrase question and answer.

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

NOTE: When you upgrade, SecureLogin stores all users data, including the user's passphrase question and response, from the previous version, so you do not need to re-create the passphrase.

You can create passphrase questions for users to select from in a directory environment; however, because you are the first SecureLogin user, you must create your own passphrase question.

7.5.1 Upgrading when Using Passphrases

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

7.5.2 Creating Passphrase Question for Users

You can create passphrase questions for users that they can select from a directory environment. However, because you are the first Novell SecureLogin user, you must create your own passphrase question and answer.

7.6 Installing for Mobile Users and Laptops

Installing Novell SecureLogin for mobile users and on laptops is the same as with the regular installation, which is explained in the earlier sections: Section 7.3, "Using the Complete Option to Install SecureLogin on a Standalone Workstation," on page 106 and Section 7.4, "Using the Custom Option to Install SecureLogin on a Standalone Workstation," on page 111.

7.6.1 Saving the Cache Locally

It is important that you save the cache locally. Otherwise, users are unable to access the applications when they are disconnected from the network.

By default, the *Enable cache file* setting in the *Preferences properties* table is set to *Yes*. You can set this at either the organizational unit level or on a per user basis.

7.7 Installing Novell SecureLogin Upgrade

Novell SecureLogin previously supported the creation of multiple Novell SecureLogin accounts for a single workstation log in. Novell SecureLogin operates in a seamless stand-alone mode. This mode uses the workstation log in to identify the user and therefore eliminating the previous need for the user to log in to Novell SecureLogin in addition to logging in to the workstation.

Because logging in to the Novell SecureLogin occurs at log in to the workstation, a seamless stand-alone does not support multiple accounts for the same user workstation log in.

To maintain backward compatibility, Novell SecureLogin supports users created in previous versions.

The first time Novell SecureLogin is launched after installation, you are prompted with options to continue using multiple accounts or to select one of your accounts and migrate to a seamless stand-alone mode. If you have been operating the Novell SecureLogin stand-alone with one account, you are automatically migrated to a seamless stand-alone mode after specifying your username and password in the first log in.

The installation procedure is the same as with the regular installation, which is explained in the earlier sections: Section 7.3, “Using the Complete Option to Install SecureLogin on a Standalone Workstation,” on page 106 and Section 7.4, “Using the Custom Option to Install SecureLogin on a Standalone Workstation,” on page 111.

7.7.1 Managing Novell SecureLogin after Upgrade

For mobile and notebook users, the Novell SecureLogin is managed through the Personal Management utility. To launch the Personal Management utility, double-click the Novell SecureLogin icon  on the notification area, or right-click the icon and select *Manage Logins*.

If you had earlier operated the Novell SecureLogin with one user account, proceed to Section 7.7.2, “Setting Up Single Novell SecureLogin User Account,” on page 113.

7.7.2 Setting Up Single Novell SecureLogin User Account

If you are upgrading from Novell SecureLogin 3.5.*x* or later, Novell SecureLogin automatically updates the single account to the workstation log in and the Novell SecureLogin icon is displayed on the notification area.

Installing Manually

8

Novell SecureLogin can be installed, configured, features can be added and removed without user intervention by using the Microsoft Windows Installer (msiexec.exe). The installer command-line options and parameters are provided directly from the command line or, supplied through a batch file.

The range of the available command-line options and parameters depend on the version of the Windows installer.

Silent Install

A silent install provides InstallShield Wizard with instructions for installing Novell SecureLogin. To use a silent install, you have to use a response file.

The response file is created during installation in `<WidowsVolume>\NSLFiles\responsefile.ini`. It captures your responses to the dialogs that you encounter during the installation. This is later used as an input for silent installation.

Proceed with the silent installation in either of the following two methods:

- Place the response.ini file in the same folder where the Novell SecureLogin.msi file is stored. Run the `Novell SecureLogin.msi`. Silent installation takes place.

  or,

- Run the silent installation through the command line. To do this, click *Start* > *Run* and at the command prompt, type

  ```
  Msiexec /i "Novell SecureLogin.msi" /qn PATHTOISS="absolute path to
  responsefile.ini"
  ```

  IMPORTANT: During silent install, the PATHTOISS property must contain the absolute path to `responsefile.ini`. If it is a relative path or if the file path is invalid, then Novell SecureLogin installation is aborted.

Logging

During the install, the log file `nslinstalllog.txt` is created in `C:\NSLFiles`.

This section contains information on the following:

Novell SecureLogin can be installed, configured, features can be added and removed without user intervention by using the Microsoft Windows Installer (`msiexec.exe`). The installer command-line options and parameters are provided directly from the command line or, supplied through a batch file.

The range of the available command-line options and parameters depend on the version of the Windows installer.

NOTE: The examples provided in this section are based on Windows installer version 3.0.

8.1 Windows Installer Command Line Options

The following are basic Windows Installer command-line options used to manually install, uninstall; and configure software and components:

Command	Usage
`/i`	Installs or configures a product.
`/f`	Repairs a product.
`/a`	Installs or configures a product on a network.
`/x`	Uninstalls a product.
`/p`	Applies a patch to a product.
`/q`	Sets the user interface (UI) level during the installation of a product.

The following are the standard Windows installer command line options that can also be used to install, uninstall software and components:

Command	Usage
`/help`	Displays the help and quick reference options.
`/quiet`	Installs without user interaction.
`/passive`	Installs with a progress bar.
`/norestart`	No restart after installation.
`/forcerestart`	Always restarts after installation.
`/promptrestart`	Prompts user to restart after installation.
`/uninstall`	Uninstalls an application.
`/log`	Writes a log file after installation.
`/package`	Installs or configures an application.
`/update`	Installs one or multiple patches.

For details of Microsoft Windows Installer command line options and parameters, refer the MSDN Library. (http://msdn2.microsoft.com/en-us/library/aa372024.aspx)

8.2 Novell SecureLogin Installer Properties

The following private properties are authored in the Novell SecureLogin installer package (`.msi` file) and can be used to manually install, configure, or install Novell SecureLogin.

The following installer properties also function during the manual installation of Novell SecureLogin 6.*x* or later.

`INSTALLDIR` specifies Novell SecureLogin installation directory.

Examples

- `INSTALLDIR=C:\Program Files\Novell\SecureLogin`
- `X_RUNATSTARTUP` - Runs Novell SecureLogin at system startup.
- :`X_RUNATSTARTUP="1"` (Yes) or `X_RUNATSTARTUP=""` (a blank string) (No)`msiexec /i` path to file\filename`.msi`
- `ADDLOCAL=MAD X_RUNATSTARTUP=”” /qn`
- The default value of `INSTALLDIR` is `<Program Files>\Novell\SecureLogin`

  Similarly you can install the other components of Novell SecureLogin. Use the following examples as references to install other components:

  ```
  ..\SecureLogin\Client\x64>msiexec.exe /i "Novell SecureLogin.msi" /qb
  ADDLOCAL=SecureLogin,SecretStore,SmartCard  X_INSTALLTYPE=EDIR
  PROTOCOLFOREDIR=NDS IS_SECRETSTORE=1 X_SMARTCARD=Yes
  X_SMARTCARDLIB=C:\Windows\System32\avrt.dll X_CSP="Microsoft Enhanced RSA
  and AES Cryptographic Provider" /l*v madgpo.log
  ```

- **To install Citrix** `msiexec.exe /qn /i "..\Novell Securelogin.msi" X_INSTALLTYPE="MAD" X_INSTALLCITRIX="Yes" X_ISCITRIXCLIENT="Yes"`

Use the `ADDLOCAL` property to add the features of Novell SecureLogin. Some of the values that you can add are:

Table 8-1 *ADDLOCAL property values and description*

Value	Description
`ADDLOCAL=SecureLogin`	Adds the core features of Novell SecureLogin. It contains all important binaries.
`ADDLOCAL=GPO_MergeModule`	Adds the Group Policy Object feature.
`ADDLOCAL=Firefox_MergeModule`	Adds Firefox feature.
`ADDLOCAL=Citrix_MergeModule`	Adds Citrix feature.
`ADDLOCAL=SmartCard_MergeModule`	Adds smart card feature.
`ADDLOCAL=Admin_MergeModule`	Adds the administrative tools.
`ADDLOCAL=DAS`	Adds Desktop Automation Services feature.
`ADDLOCAL=SecretStore`	Adds SecretStore feature.

Cache Properties

X_CACHEDIR - Use nonstandard cache directory.

For example:

X_CACHEDIR="C:\My Cache".

If you do not set the cache directory path, it defaults to %APPDATA%, which is the user profile directory.

8.3 Novell SecureLogin Property Values

The following list of property values can be used to manually install, configure, or uninstall Novell SecureLogin mode and configure components and features.

8.3.1 Install Mode Values

Install Mode	Value
MAD	Microsoft Active Directory mode.
ADAM	Microsoft Active Directory Application mode.
EDIR	Novell NDS or eDirectory mode.
LDAP	LDAP Directory mode.
STANDALONE	Standalone mode.

NOTE: These install mode values are mutually exclusive and only one mode can be installed at any time. If no mode is specified, then Novell SecureLogin is installed in STANDALONE mode by default.

8.3.2 Smart Card Properties

- X_SMARTCARDLIB - Specifies the PKCS#11 encryption library to use. The value is supplied as the name of the desired DLL file.

  For example: X_SMARTCARDLIB="C:\Resourses\acpkcs201rc.dll"
- X_CSP - Cryptographic service provider. Typically a string constant from HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider.

NOTE: For all parameters, unless otherwise specified, use = "1" to enable that option or "0" to disable the option.

8.3.3 Citrix and Terminal Server Specific Options

This section contains information on the following:

- "Citrix Client" on page 119

Citrix Client

Citrix Client is used to capture credentials from the Workstations and send the credentials through a virtual channel when an ICA session is established, known as GINA to GINA pass through. The CitrixClient component facilitates this GINA to GINA pass through.

The CitrixClient components install the following files:

- `pcpxcitc.dll` Citrix Virtual Channel Driver for NMAS pcProx.
- `nmascitc.dll` Citrix Virtual Channel Driver for NMAS.
- `nswcitc.dll` Citrix Virtual Channel Driver for Secure Workstation.
- `vdslsso.dll` (Novell SecureLogin Virtual Channel Driver for ICA Client) - This library file serves as a virtual channel to pass the captured credentials from the workstation to the Citrix Server GINA.
- `module.ini` (Configuration file in the ICA client directory) - This initialization file is modified so that the ICA client can use the Novell SecureLogin Virtual Channel driver.

Terminal Services Client

TerminalServicesClient is used to capture credentials from the Workstations and send the credentials through a virtual channel when a Terminal services session is established, known as GINA to GINA pass through. The TerminalServicesClient component facilitates this GINA to GINA pass through.

The TerminalServicesClient component installs the following file:

- `tsslsso.dll`

Citrix Client

- The Novell SecureLogin GINA to Novell GINA pass through is different.
- The Novell SecureLogin GINA for Microsoft GINA component is only installed on Novell workstations with the ICA client installed.

CitrixServer

The Novell SecureLogin published application component consists of `SLLauncher.exe` used as a wrapper to launch published applications that are enabled with Novell SecureLogin.

MicrosoftCitrixServer

This Microsoft GINA component uses the Novell SecureLogin GINA Extension (`tsgina.dll`) and a registry entry to accommodate the GINA to GINA pass through.

CitrixServer

This Novell GINA component uses the Novell SecureLogin GINA Extension (`tsgina.dll`) and a registry entry to accommodate the GINA to GINA pass through.

8.4 Installer Options

There are other options and many parameters that can be used that may better suit the corporate or enterprise environment. Where administrators like to keep control away from the users yet still allow the user see the product being installed then the following installation command-line options may be relevant:

Install Options	Parameters
`/qn`	Displays no user interface. This option will install and reboot the application and show nothing to the user to indicate the installation is taking place. A user cannot cancel the installation.
`/qb`	Displays a basic user interface. This option will install and prompt the user to reboot the application indicating the installation has taken place. A user can cancel the installation.
`/qr`	Displays a reduced user interface with a modal dialog box displayed at the end of the installation.
`/qf`	Displays the full user interface with a modal dialog box displayed at the end.
`/qn+`	Displays no user interface, except for a modal dialog box displayed at the end.
`/qb+`	Displays a basic user interface with a modal dialog box displayed at the end.
`/qb-`	Displays a basic user interface with no modal dialog boxes

IMPORTANT: It is recommended that you do not modify the `responsefile.ini`. If you want to specify new values, refer "Providing Property Through the Command Line" on page 120.

The following example installs Novell SecureLogin in Microsoft Active Directory mode with Admin tools, Smart card support, Firefox and Group policies features added. Novell SecureLogin is launched at the completion of the installation. The process is completely invisible to the user.

`msiexec.exe /i "c:\Novell SecureLogin.msi" /qn` PATHTOISS = <absolute path to `responsefile.ini`>

`msiexec.exe /i "c:\Novell SecureLogin.msi" /qn` <all property with values>

Providing Property Through the Command Line

If you do not want to use the `responsefile.ini` and want to provide a new values to the install options, we recommend you to use the command line options to provide the property values.

For example,
`msiexec.exe /i "c:\Novell SecureLogin.msi" /qn`
X_INSTALLTYPE = "STANDALONE" X_RUNATSTART UP = "Yes"
X_CACHEDIR = "C:\SecureLogin\cache..." X_INSTALLADMIN = "Yes"

Table 8-2 *Properties and Values*

Properties	When to use	Values
X_INSTALLTYPE	Use this property to specify the install type. Specify whether to install in eDirectory, LDAP, Active Directory, ADAM, or Standalone modes.	EDIR/LDAP/MAD/ADAM/ STANDALONE
X_USEGPO	Use this property to use the group policy object option. This is applicable only in Active Directory and ADAM modes of installation.	Yes **NOTE:** Works only with MAD and ADAM values. Do not set any value if you do not want to use the GPO.
X_CACHEDIR	Use this property to set the cache path.	cache path
IS_SECRETSTORE	Use this property to set the secretstore.	1 Do not set any value if you do not want to use SecretStore.
PROTOCOLFOREDIR	Use this property to set the protocol for eDirectory. **NOTE:** You can set to NDS only if Novell Client is present on the workstation.	NDS LDAP
INSTALLDIR	Use this property to set the target directory path.	target directory path
LDAPMODE	Use this property to install in LDAP mode. The options are GINA, application mode, and credential mode.	GINA/APP/CRED
LDAPCREDASSOC	This property applies only to LDAP credential mode. The options are either Window, Client32, or none of these.	NONE/WINDOWS/CLIENT32 Applies only to LDAP credential mode.
LDAPSERVERADDRESS	Use this property to specify the LDAP server address.	server address
LDAPPORT	Use this property to specify the LDAP port address.	provide port address
PCPROX	Use this property to install pcProx.	1 Do not set any value if you do not want to use pcProx.

Properties	When to use	Values
X_SMARTCARD	Use this property to specify the use of smart card.	Yes Do not set any value if you do not want to use smart card.
X_CSP	Use property to populate the dll path of the cryptographic service provider.	populate with cryptographic service provider dll path
X_SMARTCARDLIB	Use this property to populate the the PKCS#11 encryption library.	name of the dll file.
X_RUNATSTARTUP	Use this property to specify when Novell SecureLogin must be launched, that is, whether is must be launched at the startup or not.	Yes Do not set any value if you do not want Novell SecureLogin at startup.
X_INSTALLADMIN	Use this property to specify the installation of administration tools.	Yes Do not set any value if you do not want to install any administration tools.
X_INSTALLCITRIX	Use this property to specify the installation of Citrix.	Yes Do not set any value, if you do not want to install Citrix.
SW_INST	Use this property to specify the installation of Secure Workstation.	Yes Do not set any value if you do not want to install SecureWorkstation.

Disabling Java Module Installation

This release of SecureLogin has introduced:

- A command line option in the installer to disable Java module installation when running Novell SecureLogin.
- Another set of command line option that allows users to unregister and re-register Javasso, post installation during runtime.

The two command line options are

- **slproto /javereg:** /javareg registers Javasso hook.

  /javareg retrieves a list of all JRE currently installed in the system and also the Jinitiator.

  For each JRE it edits or creates two properties files, register the Javasso hook, copies jacess.jar and javasso.jar files to the JRE.
- **slproto /javaunreg:** /javaunreg unregisters Javasso hook. For this, the sljava.dll must be available in SecureLogin installation directory.

  /javaunreg does not remove jaccess.jar because it is a common module for accessibility. It removes the JavaSSO key in the registry.

NOTE: The two command are mutually exclusive of each other. If you specify both the command line options, only one is executed. In this case, `/javareg` is executed.

8.5 Switches Supported By SLProto.exe

The switches explained in the following table applied to all versions of Novell SecureLogin and modes of install.

Table 8-3 *Switches*

Switch	Usage
/displaymenu	Displays the system menu of Novell SecureLogin from the notification area icon.
/shutdown	Shuts down Novell SecureLogin, if it is running.
/nochange	Does not watch for user changing in eDirectory or SecretStore mode.
/reload	Reloads Novell SecureLogin.
/runstartup	Starts the startup scripts configured as part of Novell SecureLogin client.
/writereg	Writes to the registry after reload. **NOTE:** Use this with the reload switch.

8.6 UnInstall Options

The Windows installer uninstall option requires `/x` instead of `/i` switch.

The following example uninstalls Novell SecureLogin. The process is completely invisible to the user.

```
msiexec /x "Novell SecureLogin.msi" /qn
```

Installing, Configuring, and Deploying Desktop Automation Services

9

Desktop Automation Services (DAS) is a software component service that runs locally on the workstation to handle unique use cases associated with workstations or kiosks (multiple users using the same workstation during the day or during other shifts).

DAS provides a way to execute selective and configurable lists of user operations from virtually any scripting or programming medium on the Microsoft Windows operating system. This allows you to change the behavior of the workstation based on how you work, instead of how a computer works. This provides you the best and most flexible computing experience while saving time and mouse clicks, and adding some productivity improvements.

9.1 Installing DAS

This section covers the following topics:

9.1.1 Overview

DAS provides a way to execute selective and configurable lists of user operations from virtually any scripting or programming medium on the Microsoft Windows operating system. This allows you to change the behavior of the workstation based on how you work, instead of how a computer works. This provides you the best and most flexible computing experience while saving time and mouse clicks, and adding some productivity improvements.

You can install, configure, and use DAS in Novell eDirectory environment.

The `ARS.exe` is the center of DAS. You can configure this object with an independent set of instructions by using an XML document that is obtained through an entry in the Windows registry. The XML document can be obtained either locally on the workstation or through the directory services. The XML document is called the action file and the file is named `actions.xml`.

Each action is a set of configurable user-level operations such as mapping a drive, testing for establishing an authenticated connection to a directory, and running or shutting down an application. The flexibility of the code to test for conditions or have the action triggers such as hot keys provides tremendous flexibility to change the behavior of the workstation to fit your needs.

You can start `ARSControl.exe` either by using the Run prompt or by running ARSControl.exe, directly. The `ARSControl.exe` then parses the `actions.xml` file and stores the configuration in memory. All actions performed by the `ARS.exe` and `ARSControl.exe` are recorded in a `DASlog.txt` log file at different configurable levels of details.

After you have configured the `ARS.exe` object, its actions are available individually or in combination from any scripting interface that is available on Windows, for example, VBScript*, JavaScript*, login scripts, and batch files.

With this release of Novell SecureLogin, you can choose to install DAS (DAS) along with Novell SecureLogin.

Previously, DAS (DAS 2.0) was released as a standalone component and you had to downloaded it separately for use with Novell SecureLogin. With this release, you can install DAS during the installation process of Novell SecureLogin.

Install Desktop Automation Services is one of the options displayed on the Installation Features during the installation of Novell SecureLogin.

If you have installed earlier version of DAS or ARS installed on your workstations, uninstall these versions prior to installing the new version of DAS, which is available with the Novell SecureLogin installer package. The install location of DAS has changed as a sub directory of Novell SecureLogin.

9.1.2 Prerequisite

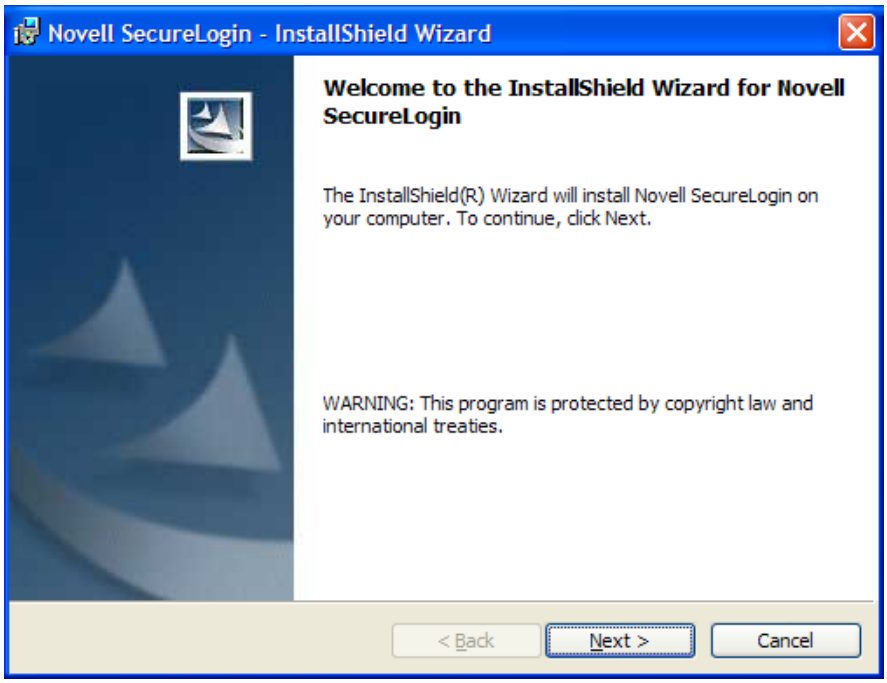
If you are installing DAS on Microsoft Windows 2000, ensure that you have Microsoft XML Parser (MSXML) 3.0 SP7

9.1.3 Changes from the Previous Version

In comparison to the previous version of DAS (version 2.0, which was a standalone release), some of the install options: *Disk Cost* and *Install Desktop Automation Services for yourself, or for anyone who uses this computer* are handled internally in this release.

9.1.4 Installing in Novell eDirectory Environment

1. Log in to the workstation as an administrator.
2. Run `Novell SecureLogin.msi`, found in the `Securelogin\Client` directory of the installer package.

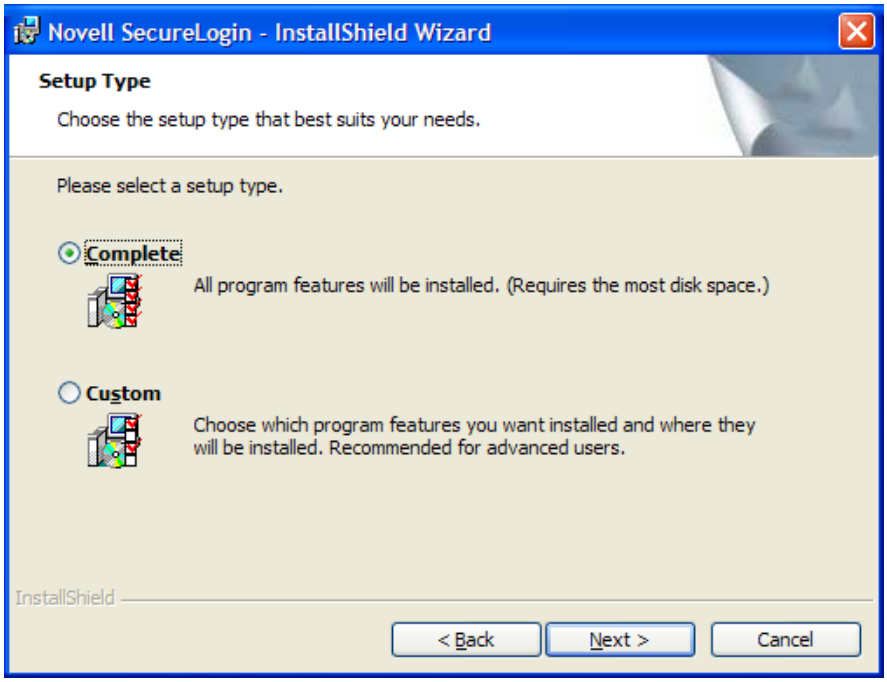


3 Accept the license agreement, then click *Next*.

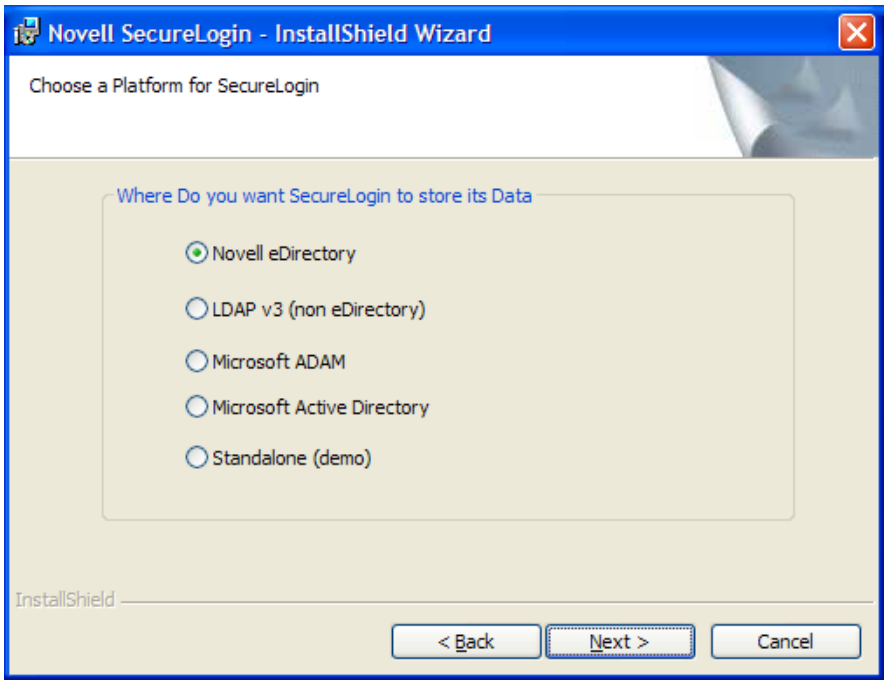
4 Select the setup type.

We recommend that you select *Complete*.

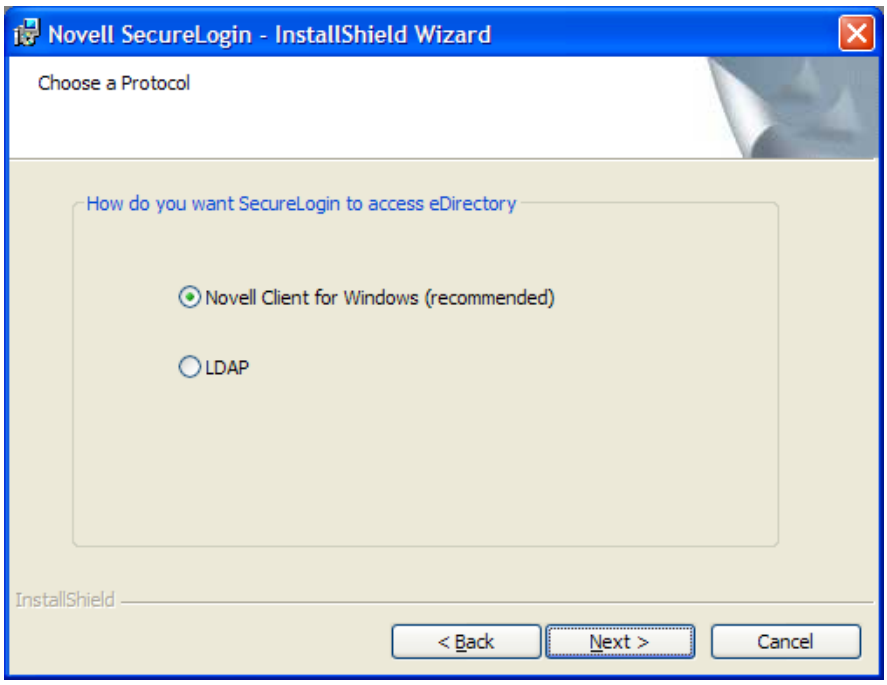
NOTE: If you select *Custom*, you are prompted to choose a destination folder to install Novell SecureLogin.



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



6 Select how you want Novell SecureLogin to access eDirectory.

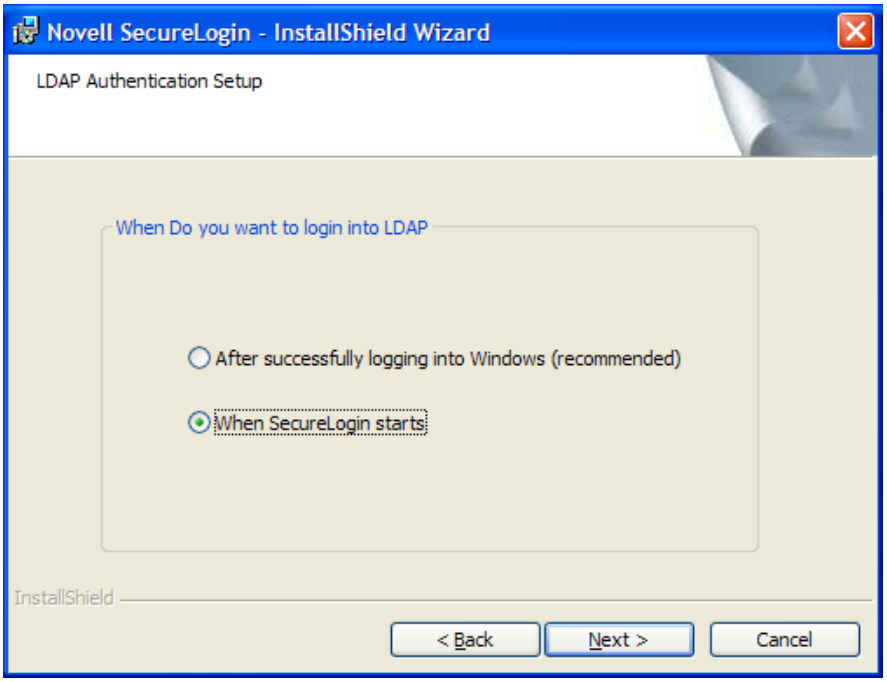


If the Novell Client™ is installed, the installation program recommends the Novell Client for Windows option. Otherwise, LDAP is recommended.

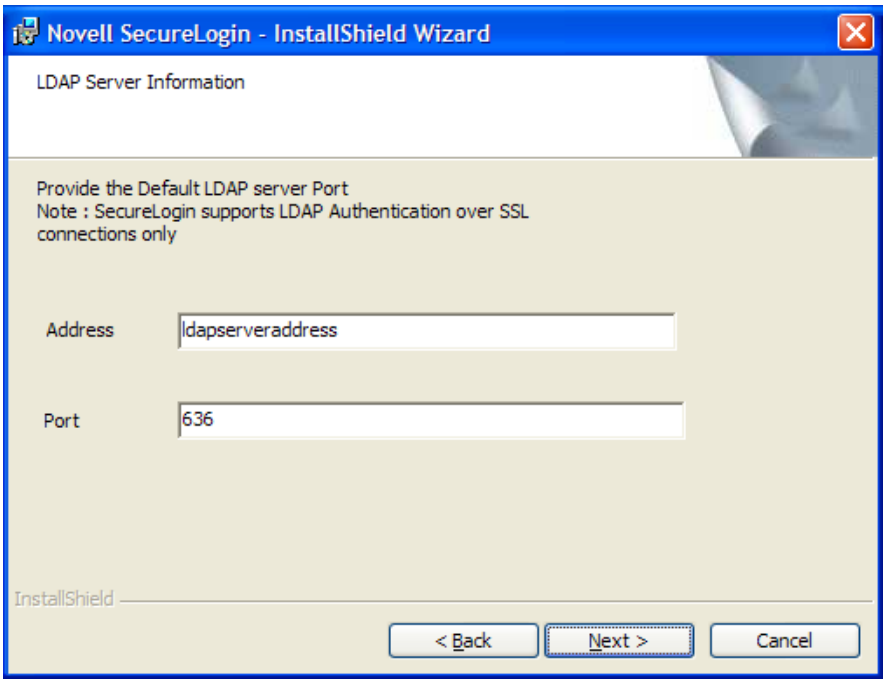
NOTE: The above dialog box is displayed only if you have Novell Client for Windows installed on your machine. Otherwise, LDAP is auto-selected as the protocol.

Proceed to Step 7.

6a If you have selected LDAP, choose when you want to log in to LDAP.



6b Specify the LDAP server information.

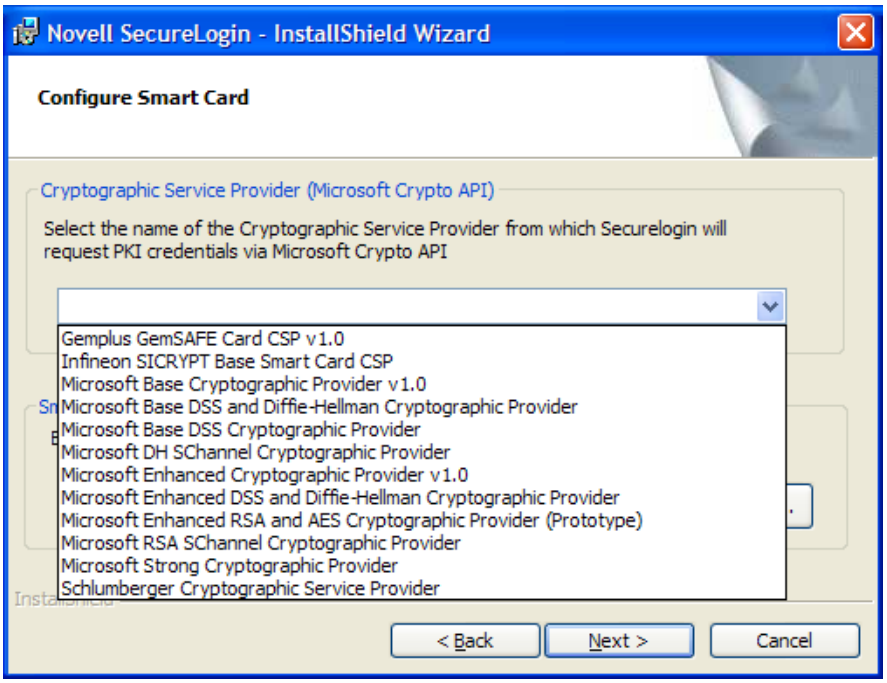


6c Proceed to Step 7.

7 Click *Next*. The smart card option page is displayed.

8 Click *Yes* if you want to use smart card. Else, proceed with Step 10.

8a Select a cryptographic service provider from which Novell SecureLogin requests PKI credentials through a Microsoft Crypto API.



8b Select a PKCS#11 compatible library required for accessing the smart card, then click *Next*.

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

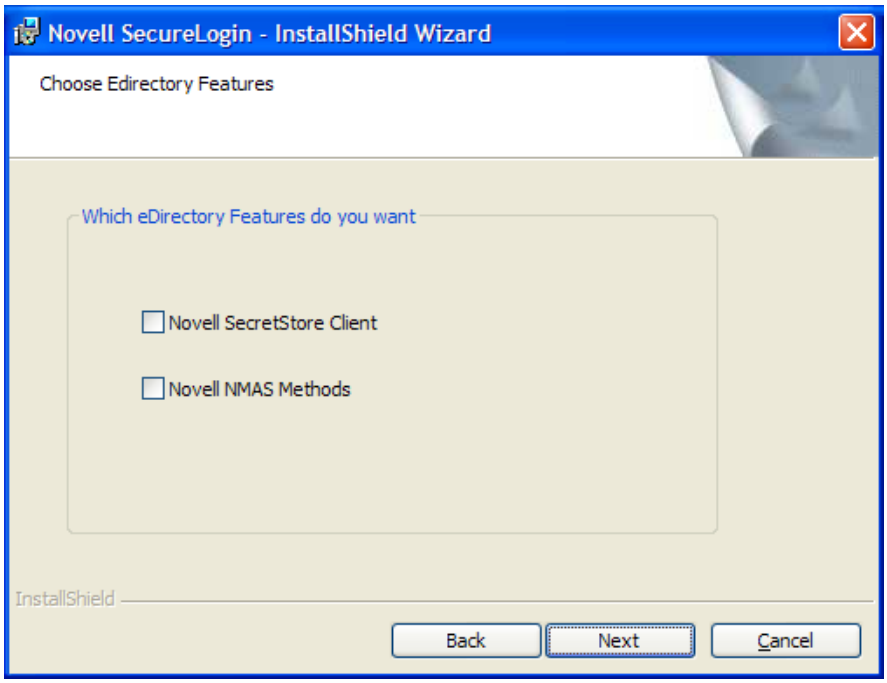
Manually configuring the third-party smart card PKCS library assumes a high level of understanding the Cryptographic Service Provider's product.

---

9 Click *No* if do not want to use smart card support. Proceed with Step 10.

10 Select the eDirectory features that you want to install, then click *Next*.

You can select both Novell SecretStore Client and Novell NMAS Methods.

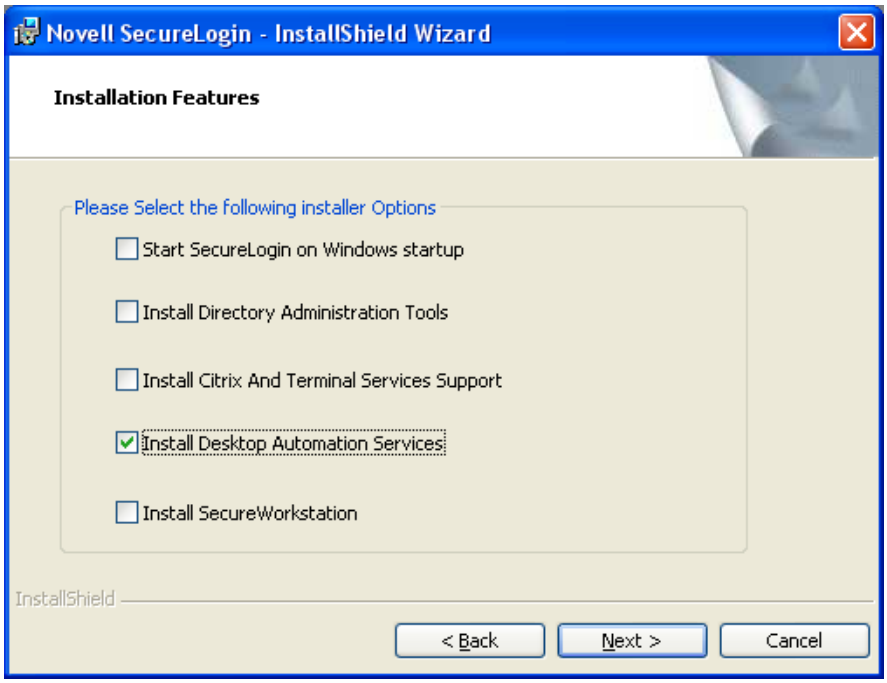


11 Click *Next*. Select the client login pcProx method.

12 Select the NMAS Methods *pcProx*.

13 Click *Next*. The installation features page is displayed.

14 Select *Install Desktop Automation Services*.

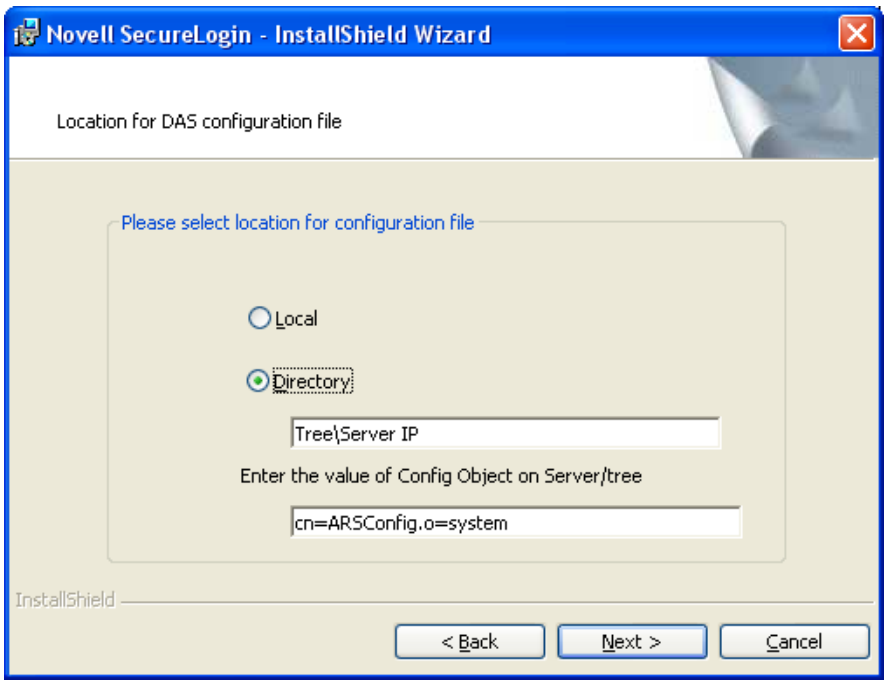


NOTE: If you are installing DAS on a kiosk or shared desktop, de-select *Start SecureLogin on Windows startup*. By default, this option is selected.

DAS handles starting and stopping of Novell SecureLogin.

15 Click *Next*. The location for DAS configuration file page displayed.

16 Select the location for the configuration file.



If you choose Local, the registry settings set for ARS.exe use the actions.xml file located in the `Program Files\Novell\SecureLogin\Desktop Automation Services` folder of the workstation.

If you choose eDirectory, the actions.xml file is managed through eDirectory as described in Section 9.2.3, "Managing the actions.xml File Through eDirectory and iManager," on page 139.

17 Click *Next*. The program is ready to install.

18 Click *Install*.

19 Click *Finish*. By default, the *Launch ReadMe* option is selected

20 You are prompted to restart your system. Select *Yes* to restart the system for Desktop Automation Services to take effect.

9.1.5 Installing in Other LDAP Environment

1 Log in to the workstation as an administrator.

2 From the *SecureLogin\Client*, select the appropriate install package and double-click it to begin the install process. The InstallShield Wizard is Novell SecureLogin is displayed.

3 Click *Next*. The License Agreement page is displayed.

4 Select the setup type.

We recommend that you select *Complete*.

NOTE: If you select *Custom*, you are prompted to choose a destination folder to install Novell SecureLogin.

---

5 Select *LDAP v3 (non eDirectory)* as the directory where Novell SecureLogin stores its data.

6 Click *Next*. The protocols page is displayed

7 Select how you want Novell SecureLogin to access LDAP directory.

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

8 Click *Next*. The smart card option page is displayed.

9 Click *Yes* if you want to use smart card. Else, proceed with Step 11.

9a Select a cryptographic service provider from which Novell SecureLogin requests PKI credentials through a Microsoft Crypto API.

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

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

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

---

10 Click *No* if do not want to use smart card support. Proceed with Step 11 on page 135.

11 Select the install features that you want to install, then click *Next*.

You can select both Novell SecretStore Client and Novell NMAS Methods.

12 Click *Next*. Select the client login pcProx method.

13 Select the NMAS Methods *pcProx*.

14 Click *Next*. The installation features page is displayed.

15 Select *Desktop Automation Services* as the feature that you want to install.

NOTE: If you are installing DAS on a kiosk or shared desktop, de-select *Start SecureLogin on Windows startup*. By default, this option is selected.

DAS handles starting and stopping of Novell SecureLogin.

---

16 Click *Next*. The location for DAS configuration file page displayed.

17 Select the location for the configuration file.

If you choose Local, the registry settings set for ARS.exe use the actions.xml file located in the `Program Files\Novell\SecureLogin\Desktop Automation Services` folder of the workstation.

If you choose eDirectory, the actions.xml file is managed through eDirectory as described in Section 9.2.3, “Managing the actions.xml File Through eDirectory and iManager,” on page 139.

18 Click *Next*. The program is ready to install.

19 Click *Install*.

20 Click *Finish*. By default, the *Launch ReadMe* option is selected

21 You are prompted to restart your system. Select *Yes* to restart the system for Desktop Automation Services to take effect.

9.1.6 Installing In Active Directory, ADAM, Or Standalone Mode

With this release of Novell SecureLogin, you can install DAS in Active Directory* mode.

1 Log in to the workstation as an administrator.

2 From the *SecureLogin\Client*, select the appropriate install package and double-click it to begin the install process. The InstallShield Wizard is Novell SecureLogin is displayed.

3 Click *Next*. The License Agreement page is displayed.

4 The Destination Folder page is displayed. By default, the program is saved in `C:\Program Files\Novell\SecureLogin\`.You can accept the default folder or choose to change. To change, click *Change* and navigate to your desired folder.

5 Select the directory where Novell SecureLogin stores its data.

In this example, Microsoft Active Directory is selected.

6 Click *Next*. The LDAP Authentication Setup page is displayed.

NOTE: As an Active Directory user, you can use DAS only with local configuration. The default value for the configuration file is, Local.

---

7 Select when you want to log in to LDAP.

- If you select *After successfully logging into Windows*, you are prompted to associate the login user with your LDAP distinguished name.
- If you select *When SecureLogin starts*, you are prompted to specify the LDAP server information.

8 Click *Next*. The smart card option page is displayed

9 Click *Yes* if you want to use smart card. Else, proceed with Step 10.

9a Select a cryptographic service provider from which Novell SecureLogin requests PKI credentials through a Microsoft Crypto API.

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

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

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

---

10 Click *No* if do not want to use smart card support. Proceed with Step 10.

11 Select *Install Desktop Automation Services* as the install feature that you want to install.

NOTE: If you are installing DAS on a kiosk or shared desktop, de-select *Start SecureLogin on Windows startup*. By default, this option is selected.

DAS handles starting and stopping of Novell SecureLogin.

---

12 Click Next. The location for the DAS configuration file page displayed.

13 Select a location for the configuration file.

If you choose Local, the registry settings set for ARS.exe use the actions.xml file located in the `Program Files\Novell\SecureLogin\Desktop Automation Services` folder of the workstation.

If you choose eDirectory, the actions.xml file is managed through eDirectory as described in Section 9.2.3, "Managing the actions.xml File Through eDirectory and iManager," on page 139.

14 Click *Next*. The program is ready to install.

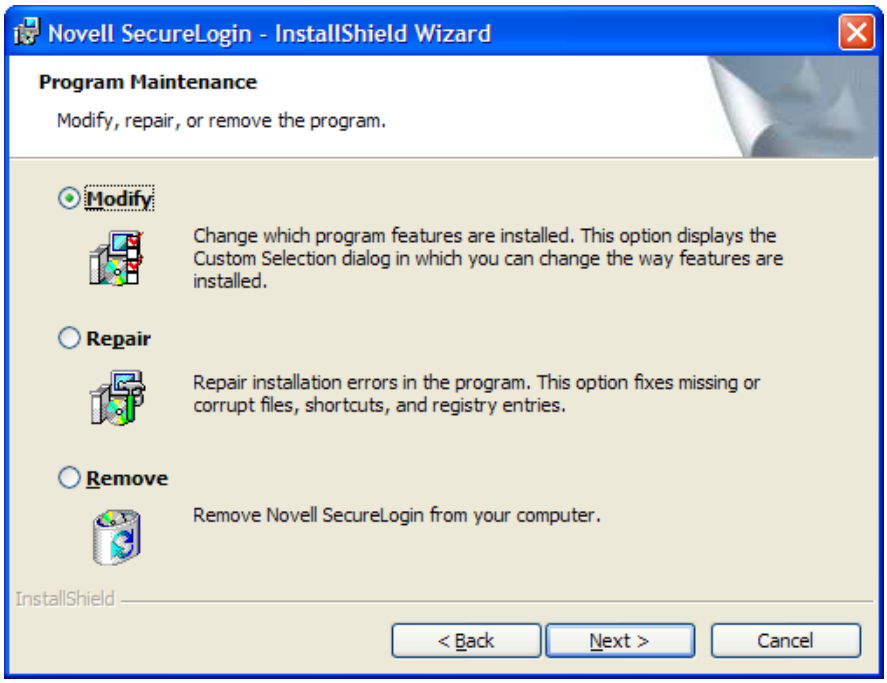
15 Click *Install*.

16 Click *Finish*. By default, the *Launch ReadMe* option is selected

17 You are prompted to restart your system. Select *Yes* to restart the system for Desktop Automation Services to take effect.

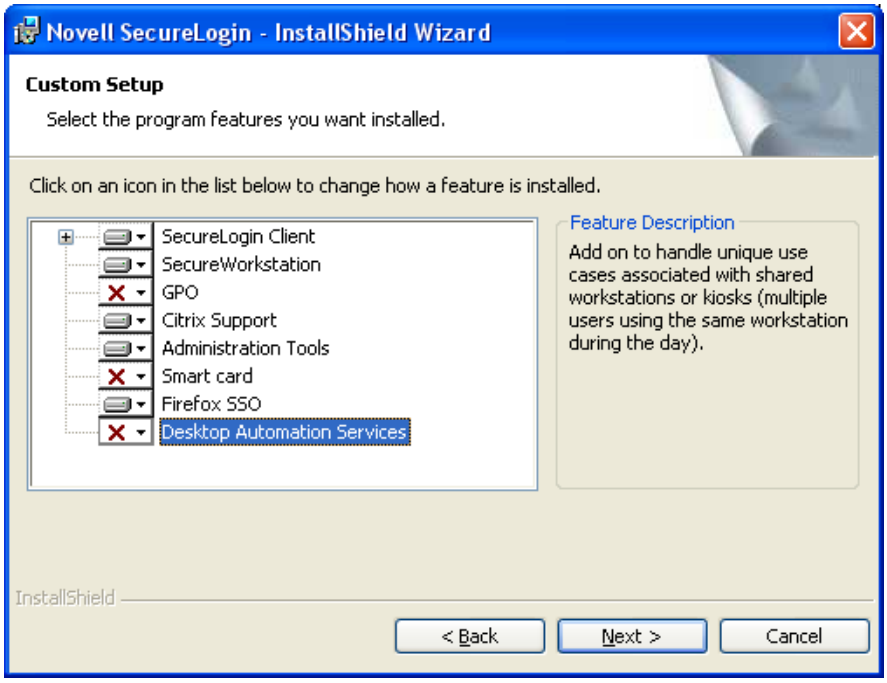
9.1.7 Installing Using the Modify Option

1 Launch Novell SecureLogin after you have successfully upgraded or installed afresh version 6.1.1 The Program Maintenance page appears.



2 Select *Modify* then click *Next*. The Custom Setup page appears.

3 Select *Desktop Automation Services* then click *Next*.



4 Click *Install*. DAS is installed.

NOTE: DAS is installed in the same folder as of Novell SecureLogin. It is typically installed at `C:\Program Files\Novell\SecureLogin\Desktop Automation Services` unless you choose a different destination folder for the installation.

After you have successfully installed DAS through the *Modify* option, DAS initializes the ConfigObject and ConfigTree registry keys, which are related to DAS network configuration.

To use the DAS XML script from the network, you must modify these registry keys.

- For information on modifying the ConfigObject registry key, see "ConfigObject" on page 137.
- For information on modifying the ConfigTree registry key, see "ConfigTree" on page 138.

9.2 Configuring

This section contains the following topics:

9.2.1 Editing Environment Registry Keys

After DAS is successfully installed, it initializes some registry keys. You must edit the registry keys to configure the system for your workstation.

To view and edit the registry keys:

1. Click *Start* > *Run*, type *RegEdit*, then click *OK*. The Registry Editor is displayed.
2. Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ARS`.
3. Modify the following keys to adapt the installation to your workstation environment:

Key Name	Value	Description
`ConfigFile`	`C:\Program Files\Novell\Securelogin\Desktop Automation Services\actions.xml` The value is the default value.	This is the pathname for the `actions.xml` file that defines the actions for the workstation. Use this key only when you are referring to an `actions.xml` file loaded locally to the workstation. If you are using a directory based `actions.xml` file, set the key value to null (blank).
`ConfigObject`	cn=ARSControl ou=ARS o=CHIP	This is the value of the fully distinguished name (DN) of an ARSControl object. This key is the object in the directory that stores the `actions.xml` file. It can be managed through Novell iManager.

Key Name	Value	Description
ConfigTree	IP address of the directory: xxx.xxx.xxx.xxx The default value is null.	This value can be the tree name or the IP address of the eDirectory tree that contains the ARSControl object. Leave the key blank if the ConfigFile key is used with a locally installed actions.xml file on the workstation. **NOTE:** The tree name must be specified for DAS to access an ARSControl object. The server on which the object is residing must be SLP enabled.
LogFilePath	C:\Program Files\Novell\Securelogin\Desktop Automation Services\DASLog.txt The value is the default value.	This is the path of DAS log file. If you do not want any log file to be generated on the workstation, set the LogFilePath to null (blank). The details of the log file are dependant on the log level that is set.
LogLevel	dword:00000001 The value is the default value.	See Section 9.2.2, "Logging and Error Notification," on page 138 for the possible settings for this value.

9.2.2 Logging and Error Notification

You can configure the ARSControl.exe application for four levels of logging. The log level is set in the Registry Editor.

1. Click *Start* > *Run*, then type RegEdit. The Registry Editor is displayed.
2. Browse to HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ARS\LogLevel.
3. Use the information in the following table to set the logging level:

Name	Value	Description
Normal	0	This produces the minimal logging. Use this level only if no errors are expected and you do not want to capture support information if an issue arises. If an error occurs, logging is not available.

Name	Value	Description
Error	1	This is the default log level. It causes ARSControl to log high-level errors. Use this only if no errors are expected and you want to capture support information if an issue arises. If an error occurs, a high-level log is recorded with a time stamp.
Action	2	ARSControl adds basic information to the log. This information records the actions created from the configuration XML parse operation.
Verbose	4	This setting produces the maximum output in the log file. Use this to only troubleshoot an existing ARSControl problem or during the development phases of a configuration file.

9.2.3 Managing the actions.xml File Through eDirectory and iManager

During the installation of DAS, the `actions.xml` file is set up to be managed locally on the workstation. You can decide to centrally manage the `actions.xml` file through eDirectory and Novell iManager.

To centrally manage the `actions.xml` file on eDirectory, do the following:

Extending the Schema for eDirectory

1. Locate the `ARSControl.sch` in `C:\Program Files\Novell\SecureLogin\Desktop Automation Services\Tools` folder.
2. Ask your eDirectory administrator to help you correctly extend the schema to add a new ARSConfig object to eDirectory.

   For a detailed procedure of the schema extension, see the *Novell eDirectory 8.8 Administration Guide* at the Novell Documentation Web site. (http://www.novell.com/documentation/edir88/index.html)

9.3 Deploying

Each deployment of DAS is unique to your use case, user target group, application mix, and other factors.

In the following sections, we list some of the best practices and some common debugging issues that you can consider during your deployment.

- Section 9.3.1, “Best Practices,” on page 140
- Section 9.3.2, “Common Debug Issues,” on page 140

9.3.1 Best Practices

When deploying DAS, we recommend that you read and follow some of the best practices listed in the following section:

- Develop specific use case scenarios with the users on the multi-user workstation.
- If your current network login scripts are use, analyze them to determine the steps that can be streamlined or determine specific actions such as mapping the drives that can be accounted.
- Prepare an inventory of all the applications and their versions on the workstation.

  Determine if there are any security policies or other technical aspects that might affect the deployment.
- Make a note of the processes running in the task manager when a user is logged in to the network. This helps to determine whether there are any applications that must be auto-launched or excluded during a log out event.
- If a use case requires applications to be shut down as part of user log out or a time-out event, access each applications carefully to ensure that Desktop Automation Service does not have any adverse effect in the application sessions. For example, terminal emulator sessions or unsaved log out (graceful log out).

  Analyze each application to determine the best way to handle a fast shut down.
- When updating `actions.xml` files, if you want to activate the latest changes without having to reboot the workstation, issue a command to the workstation to `ARS.exe` to reload the actions.xml: "`C:\Program Files\Novell\SecureLogin\Desktop Automation Services\ars.exe`" /refresh

9.3.2 Common Debug Issues

Following are some of the common debug issues that you might encounter when deploying DAS:

- The action names are case-sensitive. So, ensure that you follow a common naming convention. For example, use lowercase always.
- The DASlog.txt indicates the syntax errors (if any) in the `actions.xml` file. If the syntax errors are not indicated, run each section separately to determine the error while parsing the `actions.xml` is executed.
- Enable the log file and set the log level to 4 (verbose) on the development workstations to help debug the issues. After you have completed the testing, set the log level to zero to have minimal logging.

  Delete the DASlog.txt file after you have tested at the log level 4 as the file size is large.
- eDirectory can centrally store different workstation behavior that require different DAS configuration files.

  Configure the client in the registry to point to the desired DAS configuration object in the eDirectory.

  You can also have the different `actions.xml` files managed locally on the unique workstations and, have the other common workstations point to eDirectory.
- When forcing the ICA Client to shut down with DAS, it is recommended that you provide a pause before forcing the shutdown.

When DAS tries to shutdown the ICA Client, it sends a WM_CLOSE message to the Citrix* client. The Citrix client re-sends the message to the published application that is delivered to shutdown. If it is a time out or slow to respond, DAS quickly forces the shutdown and does not allow the Citrix application to gracefully shutdown. Adding a pause addresses the timing requirement.

- Add pauses in the `actions.xml` file if you notice any unusual behavior or observe that some use cases are not met as expected. We recommend that there might be some timing issues with certain event executions. So, ensure that you set the correct values for the serial = true or false parameters.

9.4 Accessing DAS

After you install DAS, the services are available individually or in combination through DAS executable that can be accessed from any scripting interface available on Microsoft Windows such as, VBScript, JavaScript, login scripts, and batch files.

Following are some of the ways of accessing DAS actions:

- Section 9.4.1, “Accessing Through the Command Line Utility,” on page 141
- Section 9.4.2, “Accessing Through the VBScript,” on page 141
- Section 9.4.3, “Accessing Through the JavaScript,” on page 142
- Section 9.4.4, “Accessing Through Visual Basic,” on page 142

9.4.1 Accessing Through the Command Line Utility

shortcut target = “`C:\Program Files\Novell\SecureLogin\Desktop Automation Services\ARS.exe`" startup

NOTE: If you set up the workstation to automatically log in and you want DAS to start automatically, place a DAS shortcut in the Windows Startup group under the *Start* > *Programs* > *Startup* file directory.

9.4.2 Accessing Through the VBScript

```
<SCRIPT LANGUAGE = "VBScript">

      Sub physiciansApps

      Dim as

            Set as = CreateObject(“ARS.Control”)

            ars.Execute(“Run Physicians Applications”)

      End Sub

</SCRIPT>
```

9.4.3 Accessing Through the JavaScript

You can launch a DAS action through a JavaScript* within an HTML page and launch the applications, log out, and perform other defined actions.

- To set up a link on the HTML page, specify the following:

  <a href='javascript:var ars = new ActiveXObject("ARS.Control");
  ars.Execute("Physicians_Application", null);'>Physicians Application Group

- To set up a function call in the HTML page, specify the following:

  function das_onclick_logout()

  {var ars = new ActiveXObject("ARS.Control");

  ars.Execute("logoff", null);}

NOTE: You might get an ActiveX content warning from the Internet Explorer 6.0 or later. To avoid the warning, from the Internet Explorer, select *Tools > Internet Options > Advanced*. Scroll down to the *Security* tab and select *Allow active content to run in files on My Computer*, then click *OK*.

9.4.4 Accessing Through Visual Basic

```
<Assembly: Guid("ABB6194C-DDEC-4369-8ADF-E29BB367ED0C")>

Module Module1

    Sub Main()

        Dim arsObj As ARS.IARS = New ARS.CARSControl

        arsObj.Execute("Run Physicians Applications")

    End Sub

End Module
```

9.5 Tips

Following are some tips that can help in the installation of DAS:

- You can refresh the DAS configuration through the command line using the `ARS/refresh` command. For example, `ARS.exe/refresh`, refreshes ARS.exe.

  The other way to refresh the DAS configuration is to restart the ARSControl.exe process or reboot the workstation. `The ARS/refresh` command provides a better to manage your environments and does not force a reboot when you make an update to the actions.xml file.

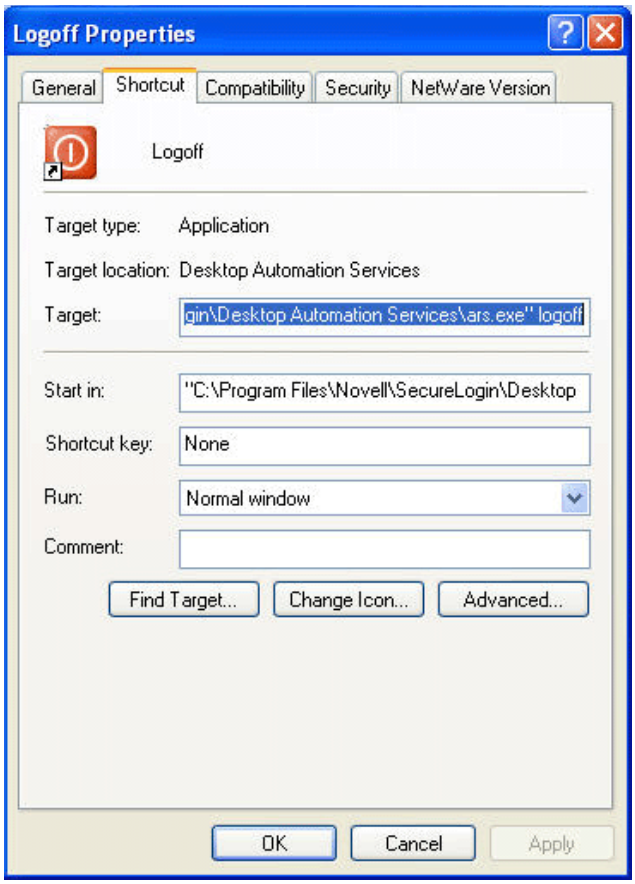
- You can close DAS through the command line using the `ARS /shutdown` command. For example, `ARS.exe /shutdown`, shuts down the `ARSControl.exe`
- Set up the `actions.xml` file by using the standard template provided in the Tools folder or modify the file based on the use case scenarios that you have developed with your users.
- You can have different `actions.xml` files managed locally on the unique workstations that have special use cases and common workstations pointing to eDirectory.

- Set up the eDirectory and iManager after you have stabilized your `actions.xml` and wish to centrally manage the configuration file. For more information, see "Extending the Schema for eDirectory" on page 139 and Chapter 10, "Accessing iManager and Installing the iManager Plug-In," on page 145.
- Set up the workstation to have auto-admin login to a local workstation ID.

  For more information, see the Novell Cool Solutions Web site. (http://www.novell.com/coolsolutions/tools/14071.html)
- Provide a logout button in the Windows quick launch tool bar and provide a logout icon on the desktop for the convenience of the users. You can also provide a hotkey combination such as Ctrl+L.

  For example, shortcut target ="`C:\Program Files\Novell\SecureLogin\Desktop Automation Services\ARS.exe`" logoff. This is your shortcut properties target setting.

Figure 9-1 *Logoff Shortcut Option*



Accessing iManager and Installing the iManager Plug-In

10

Novell SecureLogin supports iManager 2.7.2 The plug-in for iManager 2.6 are available as part of the product installer package. You can download the plug-in for iManager 2.7 from the Novell Downloads Web site. (http://download.novell.com/index.jsp)

This section contains the following information:

10.1 Accessing iManager

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

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

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

   For example:
   `http://127.0.0.1/nps/iManager.html`

   You might be redirected to an HTTPS secure page

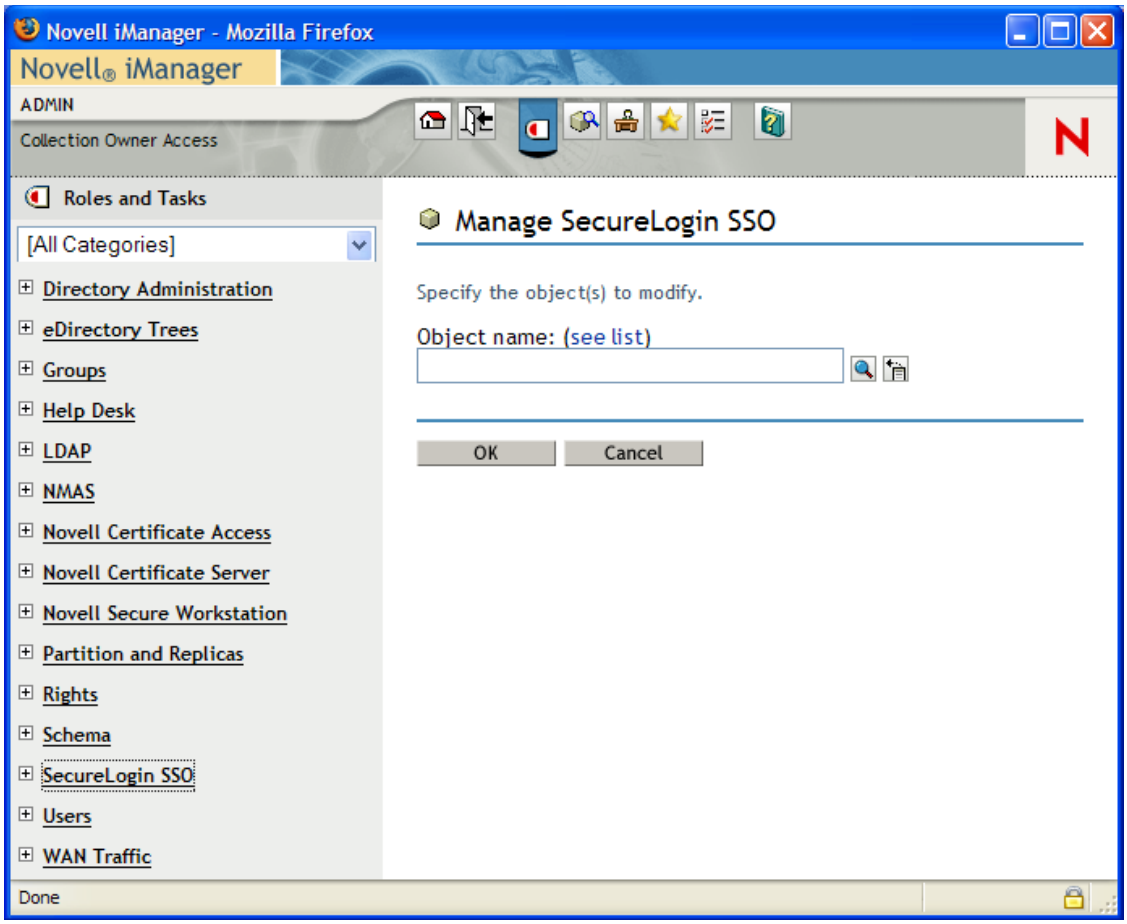
   IMPORTANT: The URL is case sensitive.

2. Log in using your username, password, and eDirectory™ tree name.

   You can substitute the IP address of an eDirectory server for the tree name.

   To have full access to all Novell® iManager features, you must log in as a user with admin-equivalent rights to the tree.

For details on accessing iManager, go to the Novell Documentation Web site for iManager 2.6 (http://www.novell.com/documentation/imanager26/index.html)



10.1.1 iManager Plug-In for Novell SecureLogin

The iManager plug-in for Novell SecureLogin are `.npm` files. The plug-in are:

- `pcprox.npm`
- `secretstore.npm`
- `sso.npm`
- `sw.npm`

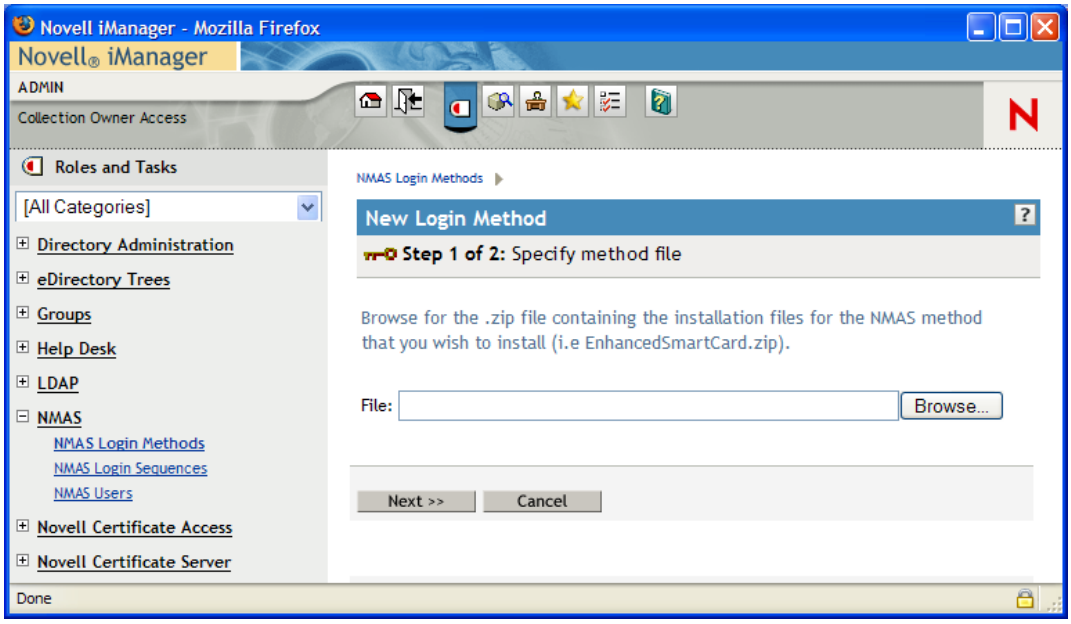
10.2 Installing the NMAS Server Methods

The `pcprox.npm` and `sw.npm` are the plug-in for NMAS server methods. These are available in a `.zip` format.

Use iManager to install these NMAS Login Methods.

1. To install, log in to iManager. Select *NMAS* > *NMAS Login Methods* > *New*. The New Login Method page opens.

2 Browse and locate the `.zip` file containing the installation files for NMAS method that you want to install. This is found in `\Nmas\NmasMethods\Novell\SecureWorkstation\SecureWorkstation.zip` that is available as part of the Novell SecureLogin installation at the Novell Download Web site. (http://download.novell.com/index.jsp)



10.3 Installing the Other Plug-In for iManager

The iManager plug-in are `.npm` files. The plug-in are:

- `secretstore.npm`
- `sso.npm`

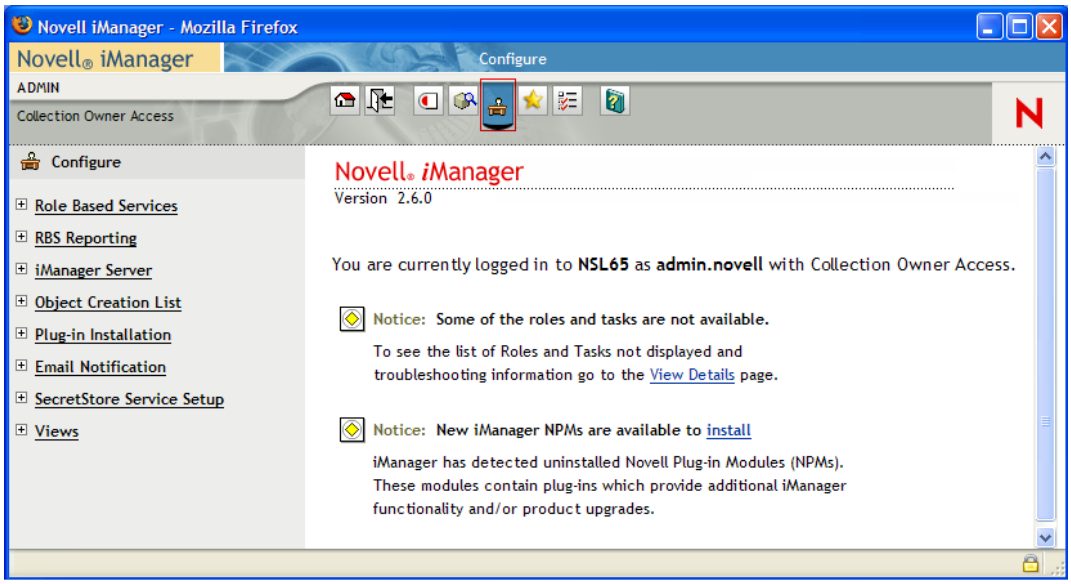
They are found in the `\imanager\snapin` directory on the Novell SecureLogin installer package.

If you want to install the PcProx plug-ins for iManager, make sure you have the following prerequisites:

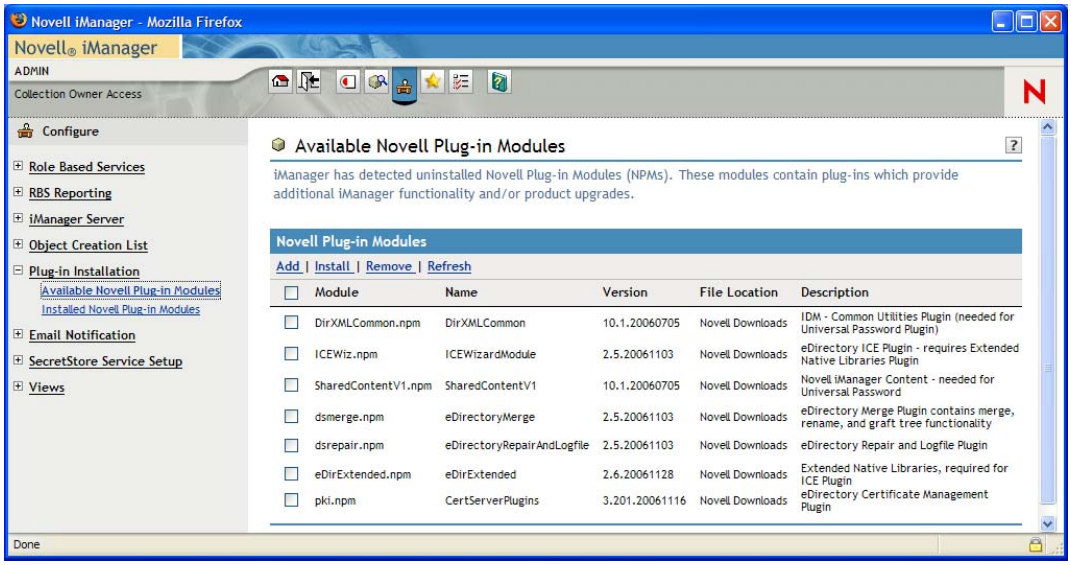
- iManager must be running on a Windows machine on which the pcProx client method is installed.
- A pcProx scanner must be connected to the same machine.

To install these `.npm` files for iManager:

1 Log in to iManager. Click the *Configure* tab.



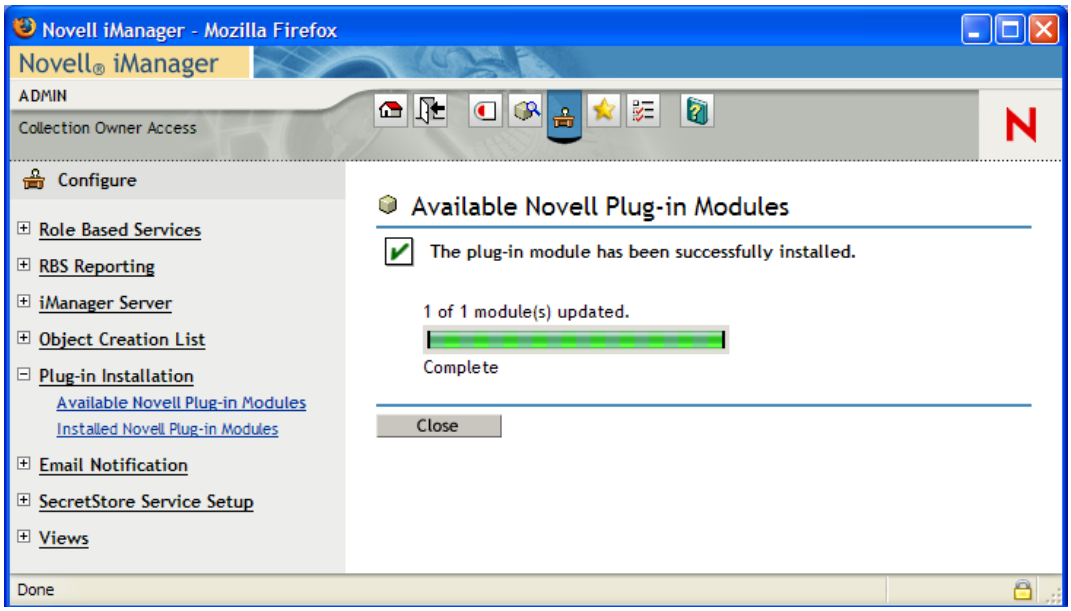
2 Click *Plug-in Installation*, then select *Available Novell Plug-in Modules*.



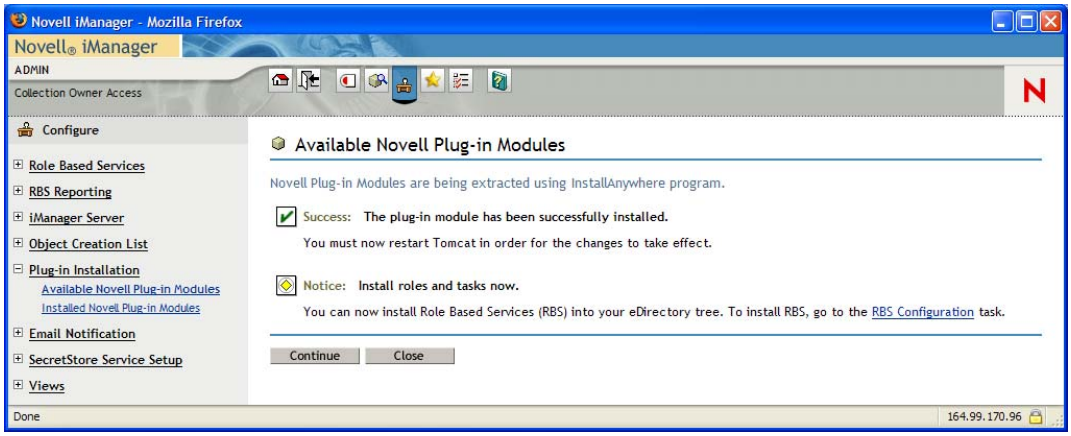
3 Select the plug-in you want to install and click *Install.* You see a confirmation message after the plug-in is successfully installed.

4 Click *Close*.

5 Repeat Step 2 to Step 4 to add the other `npm`.



6 Restart Web server after the installation is complete. This might take several minutes.



For more information on installation and Role Based Server (RBS) configuration, visit the Novell Documentation Web page (http://www.novell.com/documentation/imanager26/index.html)

NOTE: You must install the LDAP schema on the directory, after you have installed the plug-ins.

10.3.1 Configuring iManager for LDAP SSL Connection to eDirectory

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

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

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

Table 10-1 *Scenarios*

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

Installing Secure Workstation 11

This section provides information on the following:

11.1 Overview

Secure workstation helps users to secure their workstations. Secure Workstation provides a policy-based framework within which you can control locking the workstation and automatically log out of users based upon several different events, such as:

- Period of inactivity (configurable)
- Proximity card removal
- Smart card removal

Secure Workstation is available to both connected and disconnected workstations.

The policy can either be the local policy for disconnected workstation, which can be configured using Policy editor tool, or network policy for connected workstation by using Secure Workstation Post-Login Method for NMAS.

The Network policy is stored in eDirectory.

You can use iManager to configure the policy.

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.

The following two scenarios help you better understand the functioning of Secure Workstation.

Scenario 1: Inactivity Timeout. Assume that 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 2: An Authentication Device Is Removed. Assume that Secure Workstation is installed on all the workstations that Claire uses. Claire is a nurse. Claire logs in to the nursing station’s workstation by using a proximity card. She 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 Local Policy Editor
- The Secure Workstation Post-Login Method for NMAS

11.2 Installing Secure Workstation

- Section 11.2.1, “Installing Secure Workstation,” on page 152
- Section 11.2.2, “Installing iManager Plug-In to Secure Workstation,” on page 154

11.2.1 Installing Secure Workstation

If you are installing Novell SecureLogin in the *Complete* option and the *Novel l NMAS Client* option is selected, the Secure Workstation program files are installed during the installation itself.

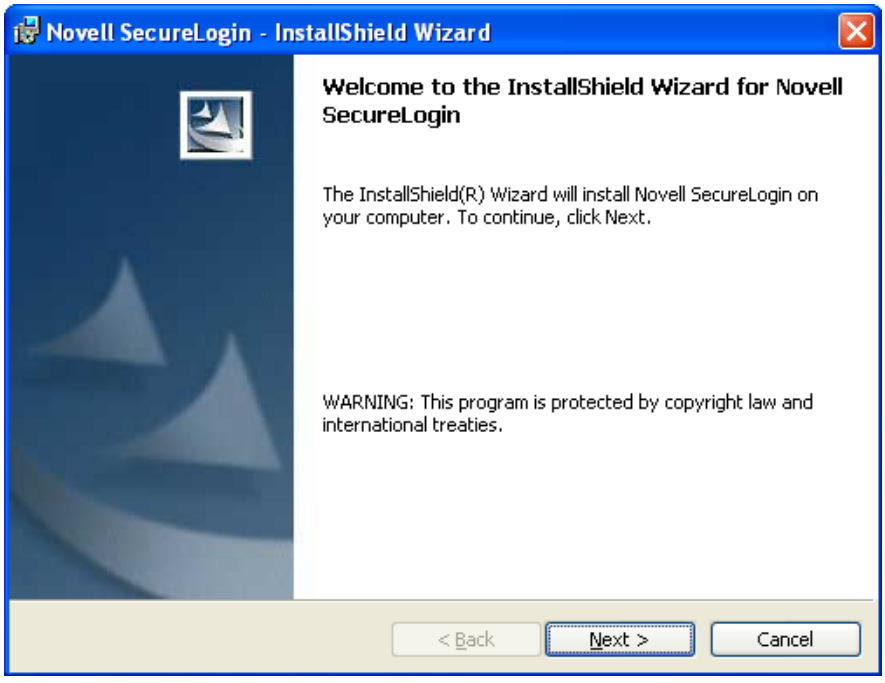
If you have not installed it earlier, you can do it at a later stage.

Secure Workstation is also an option in the *Custom* install. In case you had not selected Secure Workstation earlier, you can later add it through the *Custom* install option.

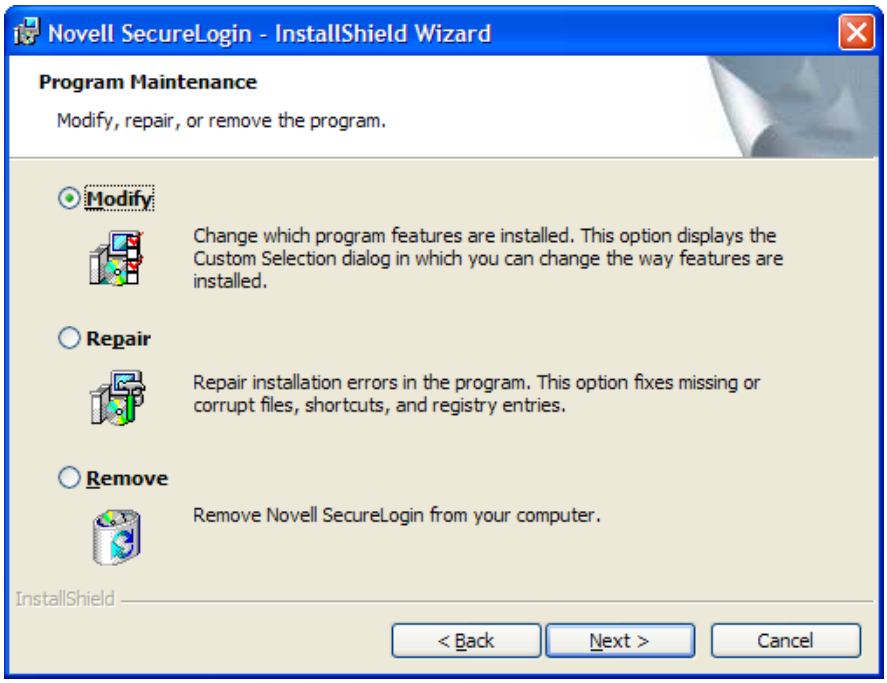
To add Secure Workstation components:

1 Run the `Novell SecureLogin.msi`, found in the `SecureLogin\Client` directory of the Novell SecureLogin installer package.

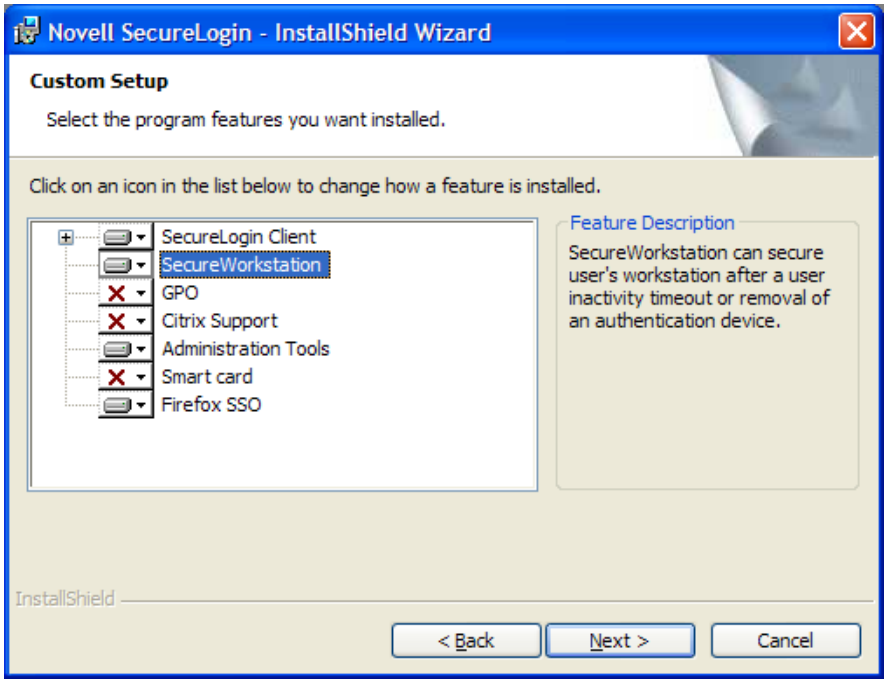
The InstallShield Wizard is launched.



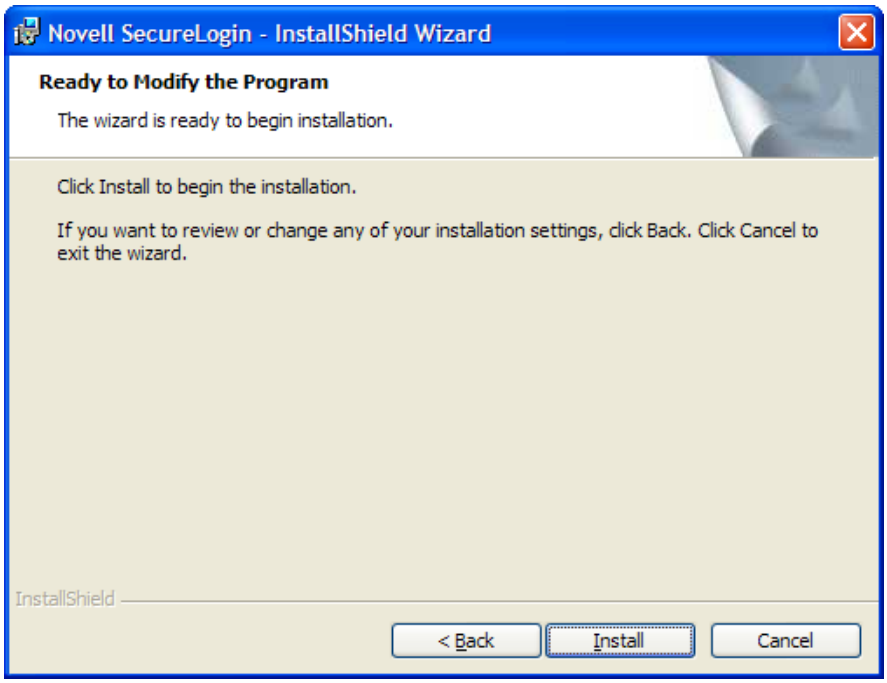
If SecureLogin is already installed, InstallShield launches the Program Maintenance dialog box.



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



3 Select the *Secure Workstation*, then click *Next*.



4 Click *Install*.

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

11.2.2 Installing iManager Plug-In to Secure Workstation

You can administer Secure Workstation by using iManger and by configuring Secure Workstation settings on the workstation.

For more information on installing the iManager plug-in to Secure Workstation, see Chapter 10, "Accessing iManager and Installing the iManager Plug-In," on page 145.

For more information on administering the Secure Workstation, see "Administering Secure Workstation" in the *Novell SecureLogin 6.1 SP1 Administration Guide.*

Upgrading

12

You can migrate all of your servers and workstations to SecureLogin 6.1SP1 at one time, or you can do a phased migration, where you migrate in stages. If you plan to do a phased migration, start with Section 12.1, “Phased Upgrading,” on page 155.

12.1 Phased Upgrading

12.1.1 Developing a Migration Plan

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

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

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

12.1.2 Example of a Migration Plan

The Organization

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

Sales OU users have laptops for mobile access to the network. The Central Administration OUs contain a combination of static workstations and laptop users. Manufacturing and Purchasing OU users are mobile; workstations are accessed in Kiosk mode. Users in the remaining OUs are each allocated a workstation for their sole use.

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

Upgrade Order

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

Week 1

Day 1: Upgrade the server directory; extend the schema, and assign rights to the organizational units. Ensure that all containers and organizational units have the following:

- Directory database version *3.5*.
- Stop tree walking.

Create a test user in the Sales OU and change the setting for the user object to directory database version value *6.1*.

Test single sign-on enabling of required application.

Day 2: On successful deployment of the upgrade for the test user, manually set the directory database version to *6.0* on the Sales OU to enable full upgrade functionality.

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

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

Day 3: Monitor any upgrade issues for the upgraded Sales OU users. If all issues have been resolved successfully, install the Novell SecureLogin upgrade on all laptops and workstations associated with the Central Administration and Human Resources OUs.

Set the directory database version to *6.0* on the Central Administration and Human Resources OUs to enable full upgrade functionality.

Day 4: Install the Novell SecureLogin upgrade on workstations associated with the following OUs:

- Accounting
- Marketing

Day 5: Review and resolve any issues.

Day 6: Install the Novell SecureLogin upgrade on workstations associated with the following OUs:

- Manufacturing
- Purchasing

Review any upgrade issues encountered by Central Administration OU users. If there are no problems, change the directory database version to *6.0* setting for the following OUs:

- Accounting
- Marketing

Week 2

Day 7: All users now have upgraded the Novell SecureLogin application installed.

Review and resolve any issues.

Upgrade the administration workstation.

Day 8: If all issues are resolved successfully, change the directory database version to *6.0* for all remaining OUs.

Ensure that the following OUs are also enabled simultaneously to provide service for mobile and Kiosk users:

- Manufacturing
- Purchasing

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

Day 9: Migration is completed. Review of the migration plan commences.

12.1.3 Running Novell SecureLogin in a Mixed Environment

When SecureLogin 6.1 runs in the same environment as SecureLogin 3.0.*x*, SecureLogin 6.0 does the following:

- Versions the SecureLogin data store.
- Saves SecureLogin 6.1 data in the SecureLogin 6.0 data format.

This mixed mode enables you to gradually deploy SecureLogin 6.1 in a SecureLogin 6.0 environment while still allowing you to perform most administration tasks during the transition.

Deploying SecureLogin 6.1 in a mixed environment has the following limitations:

- Limited administrative functionality

  When you run SecureLogin 6.1 in mixed mode, new features such as shadow variables will not work. Also, some SecureLogin 6.1 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.

12.2 Prerequisites

Before you upgrade:

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

12.2.1 Hot Desk and Mobile Users

Hot desking is the temporary physical occupation of a workstation or work surface by a particular employee. The work surface can either be an actual desk or a terminal link. Hot desking is regularly used in large enterprises where employees are spread across offices or geographical locations at different times, or at out of office for a long time.

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

When these users log in to SecureLogin, their details are downloaded from the directory to the local workstation cache. All workstations accessed by Kiosk mode users must run the same version of SecureLogin. If users log in to an upgraded workstation, they cannot access their SecureLogin data on workstations running a previous version of the software.

12.2.2 Stopping Tree walking

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

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

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

To set the *Stop walking here* option at the Users container:

1. Access iManager, then select *Manage SecureLogin SSO* from the left pane.
2. Select *Preferences* from the drop-down list.
3. Select the *Stop walking here* option and change the value to *Yes*.
4. Click *Apply*.

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

12.3 Upgrading Novell SecureLogin

Scenario 1: Upgrading to Novell SecureLogin 6.1 from Novell SecureLogin 6.0 or 3.5

Even if SecureLogin 6.0 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 6.0 and automatically works with it.

Scenario 2: Novell SecureLogin during an Operating System Upgrade

If you are running Novell SecureLogin 6.1 on Microsoft Windows XP, 2000, or 2003 and, want to Microsoft Windows Vista, you will have to first uninstall Novell SecureLogin on the older operating system, upgrade the operating system, and then reinstall Novell SecureLogin 6.1 on Microsoft Windows Vista.

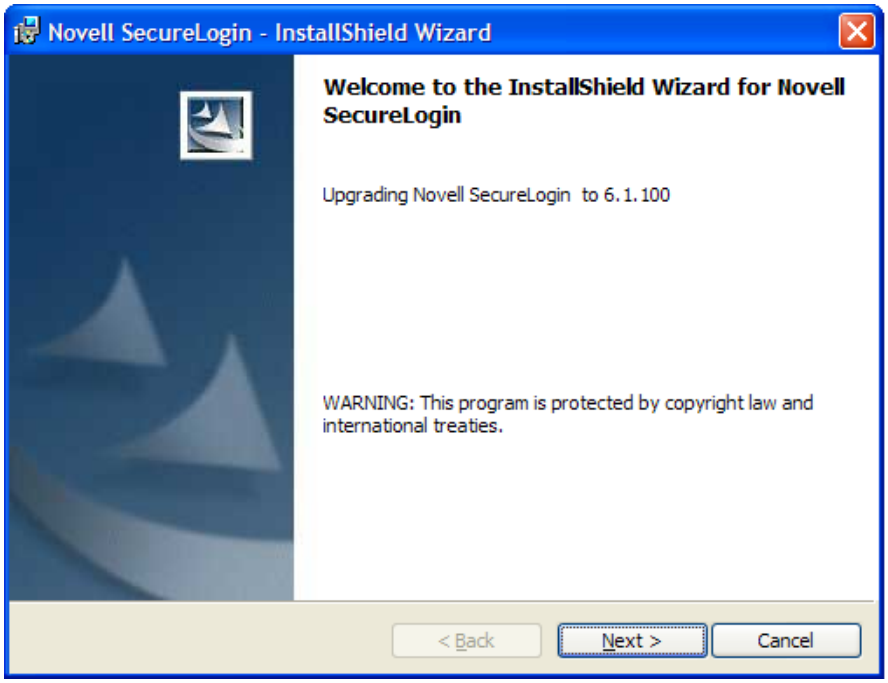
For example, if you are running Novell SecureLogin 6.1 on Microsoft Windows XP, do the following:

1. Uninstall Novell SecureLogin 6.1.
2. Upgrade the Microsoft Windows XP operating system to Microsoft Windows Vista.
3. Install Novell SecureLogin 6.1.

12.3.1 Upgrading Novell SecureLogin On the Operating System

Upgrading from Novell SecureLogin 6.1

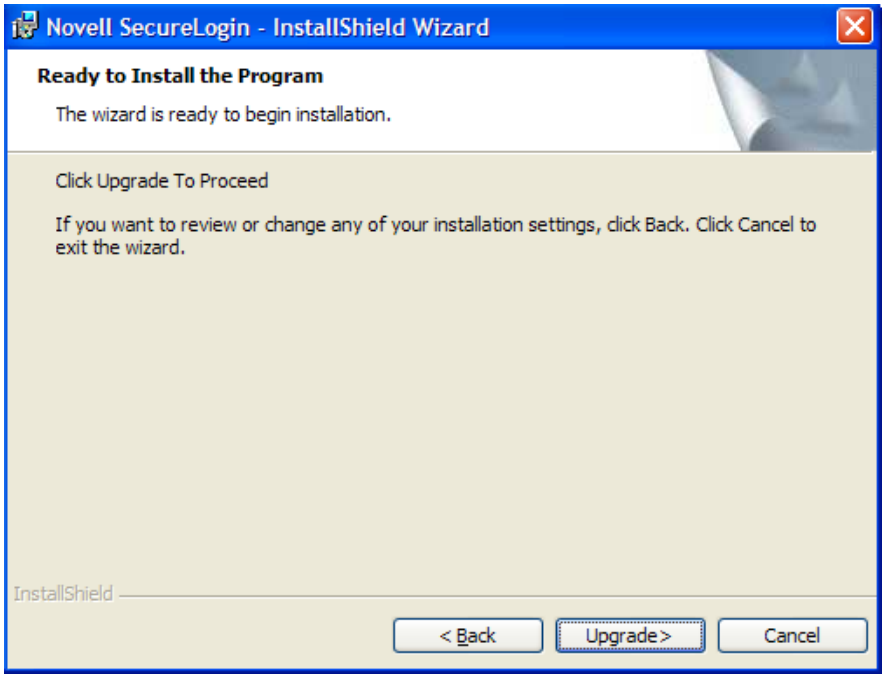
1 Run `Novell SecureLogin.msi` found in the `\securelogin\client` directory in the Novell SecureLogin 6.1.1 installer package.



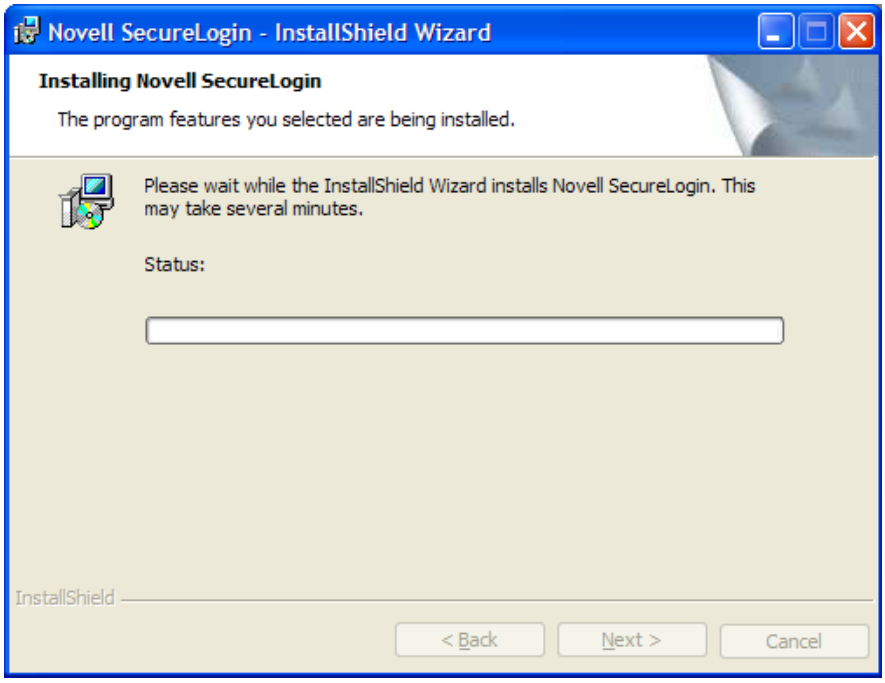
2 The InstallShield Wizard is launched. Click *Next*.

3 The license agreement page appears. Accept the license agreement.

4 Click *Next*. The Ready to Install the Program page appears.



5 Click *Upgrade*.



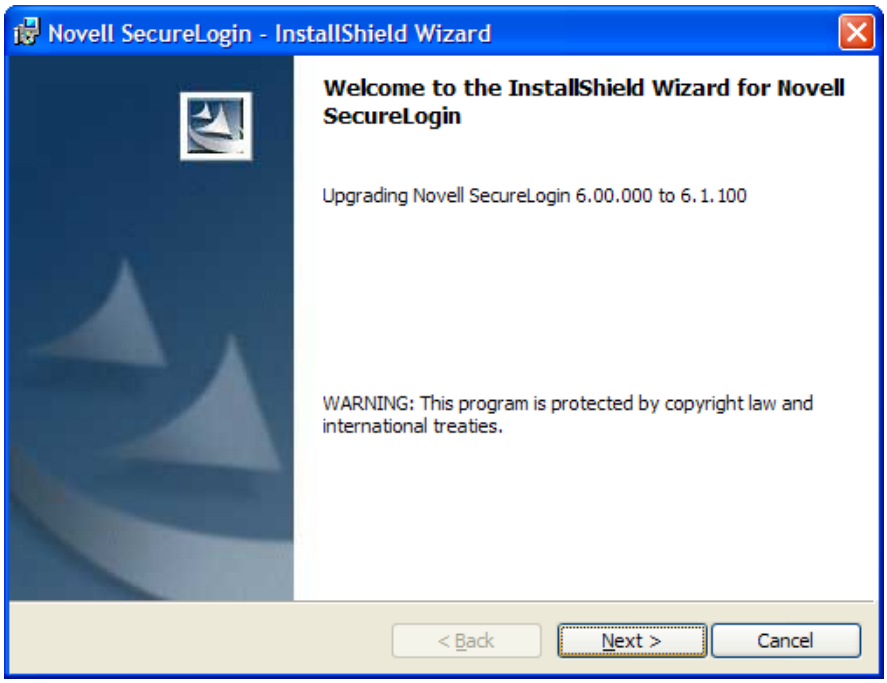
The upgrade takes a few minutes.

Upgrading from Novell SecureLogin 6.1 Hotfixes

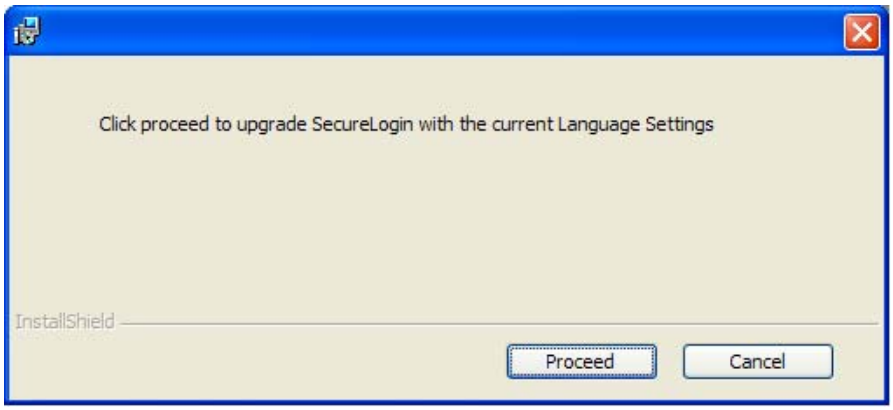
The procedure to upgrade to 6.1.1 from Novell SecureLogin 6.1 with the hotfixes is the same as "Upgrading from Novell SecureLogin 6.1" on page 160.

Upgrading from Novell SecureLogin 6.0

1 Run `Novell SecureLogin.msi` found in the `\securelogin\client` directory in the Novell SecureLogin 6.1.1 installer package.



2 You are prompted to proceed with the upgrade with the current language settings. Click *Proceed*.

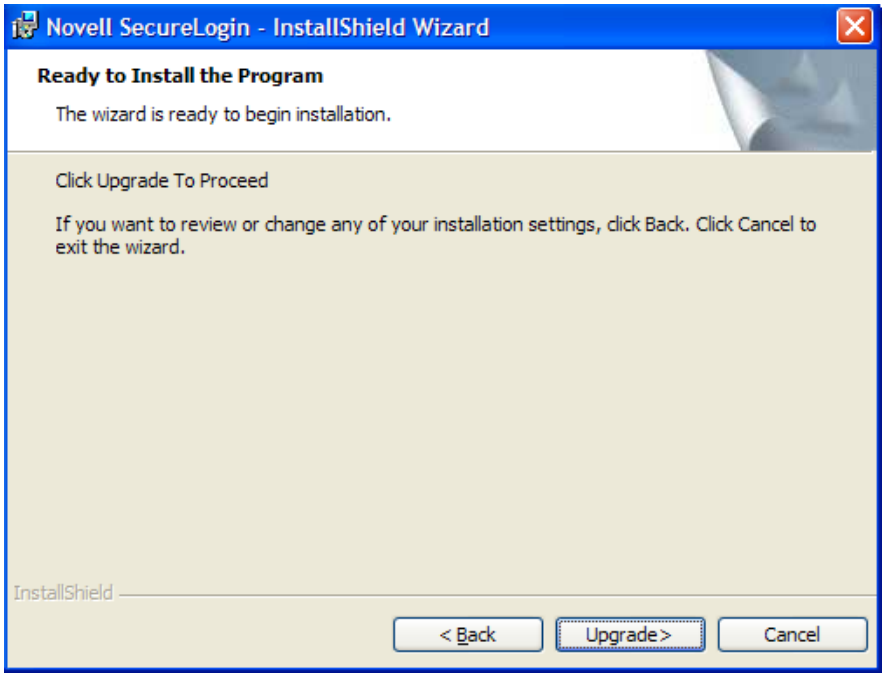


3 The InstallShield Wizard is launched. Click *Next*.

4 The license agreement page appears. Accept the license agreement.

5 Click *Next*. The Ready to Install the Program page appears.

6 Click *Upgrade*.



The upgrade takes a few minutes.

Upgrading from Novell SecureLogin 3.5.*x*

To upgrade from SecureLogin 3.5.*x* versions:

1 Uninstall SecureLogin 3.5.*x* from your workstation.

2 Run `Novell SecureLogin.msi` found in the `\securelogin\client` directory on the Novell SecureLogin 6.1 installer package.

Upgrading from Novell SecureLogin 3.0.*x*

The procedures explained here use the Microsoft Windows 2000 Professional operating system to uninstall Novell SecureLogin 3.0.*x*.

1 On the Windows *Start* menu, click *Control Panel* > *Add/Remove Programs*.

2 Click Novell SecureLogin on 3.0(.*x*), then click *Remove*.

3 If are prompted to restart your workstation, click *Yes* to restart the workstation, or *No* to restart later.

Novell SecureLogin is now uninstalled.

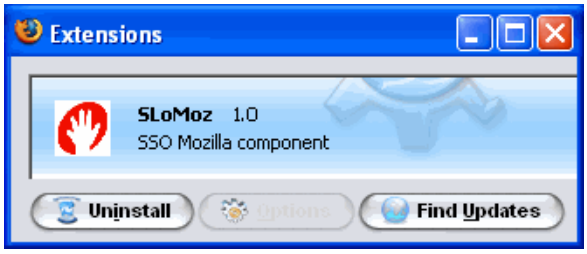
Before installing the new version of Novell SecureLogin, log off and log in again.

12.3.2 Upgrading to Novell SecureLogin with Firefox

Because Mozilla Firefox changes from release to release, there might be some problem when upgrading Novell SecureLogin 6.1 with Mozilla Firefox 1.0.*x* or earlier.

We recommend that you install or upgrade Novell SecureLogin 6.1 with Mozilla Firefox 1.5.*x* or later installed for the `SLoMoz.xpi` extension to be automatically installed and configured.

Figure 12-1 *The SLoMoz File*



NOTE: If you wish to continue using Mozilla Firefox 1.0.x or earlier, then the `SLoMoz.xpi` installed with Novell SecureLogin must be uninstalled and the `slomoz.xpi` of the Novell SecureLogin installer package must be reinstalled.

12.4 Changing the Directory Database Version

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

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

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

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

1. Access iManager, then select *Manage SecureLogin SSO* from the left pane.
2. Select *Advanced Settings* from the drop-down list.
3. From the *Select Version* drop-down list, select the required version.

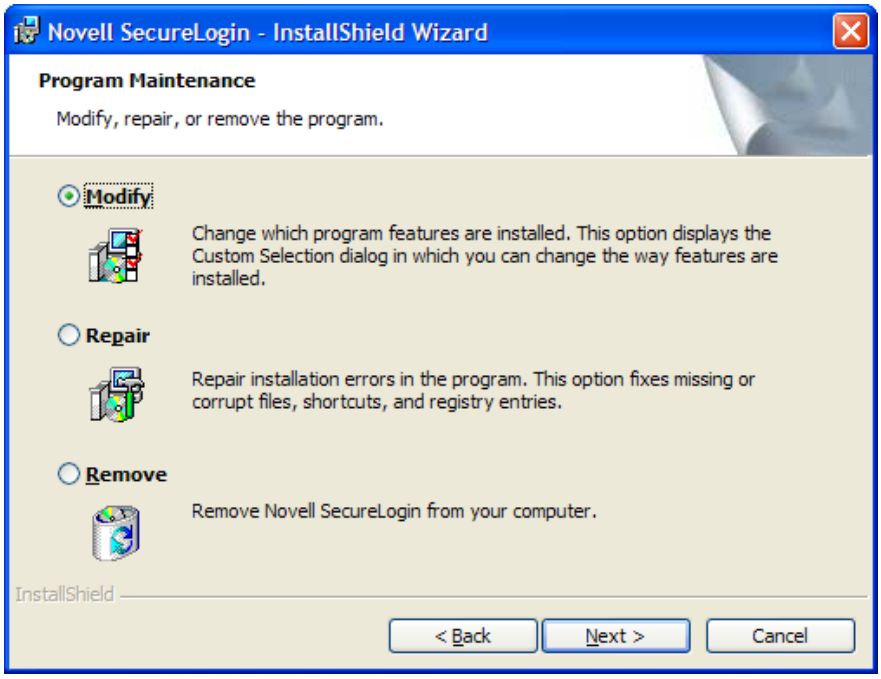
   NOTE: You cannot select a version lesser than your current version.

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

Modifying, Repairing, or Removing an Installation

13

If you have Novell SecureLogin already installed, the InstallShield detects the installation and offers you several options for changing the existing configuration.



Use the *Modify* operation to uninstall features installed during installation.

However, you cannot change the options that are not listed. For example, you cannot use *Modify* to change the platform.

Use the *Repair* operation if you want to install any missing components. The installation program detects the previously installed components and re-installs them.

Use the *Remove* operation if you want to uninstall Novell SecureLogin and do a fresh install. For example, you previously installed an evaluation version of Novell SecureLogin in the standalone mode. After a successful evaluation, you now want to install Novell SecureLogin throughout your organization, which is using eDirectory. However, you cannot directly migrate from standalone mode to eDirectory. You need to select *Remove*, uninstall Novell SecureLogin 6.1, restart your workstation (if you are prompted to restart), then reinstall Novell SecureLogin 6.1.