AUTHORIZED DOCUMENTATION

Installation Guide

Novell® SecureLogin

7.0

February, 2010

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 manual provides information on installing, deploying, and upgrading Novell SecureLogin 7.0.

This document contains the following sections:

Audience

This guide is intended for:

- Network Administrators
- System 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 www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Novell SecureLogin 7.0 Installation Guide*, visit the Novell Documentation Web site. (http://www.novell.com/documentation/securelogin70).

Additional Documentation

For other manuals available for this product, see the Novell Documentation Web site. (http://www.novell.com/documentation/securelogin70)

The other documentation available with this manual are:

- Readme: “Novell SecureLogin 7.0 Readme”

- Overview: *Novell SecureLogin Overview Guide*
- Administration: *Novell SecureLogin Administration Guide*
- Application Definition Administration: *Novell SecureLogin Application Definition Wizard Administration Guide*
- pcProx Administration: *pcProx Guide*
- Application Definition: *Novell SecureLogin Application Definition Guide*
- Citrix and Terminal Services: *Novell SecureLogin Citrix and Terminal Services Guide*
- End User: *Novell SecureLogin User Guide*

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.

Getting Started

This section provides you an overview of Novell® SecureLogin, an enterprise single sign-on solution. The section also explains the limitations in design and behavior that you are useful to you before you begin installing Novell SecureLogin. Wherever we have a workaround for a limitation, we have provided information about it.

Introduction

1

Novell SecureLogin is a credential management tool developed to increase network security. It is an enterprise single sign-on product. It provides authentication solutions to Web, Windows, host, and legacy application-based single sign-on. Novell SecureLogin functions as an identity overseer for all the systems that users access.

It is a credential management tool developed to increase an organization’s network security while lowering support costs.

Novell SecureLogin securely manages and encrypts the authentication information in the directory. It stores usernames and passwords and automatically retrieves them for users, when required.

Before Installing

2

Before you begin installing Novell SecureLogin, note the following behavior and limitations.

The Installation Is Interrupted

User Account Control (UAC) is a new setting on Microsoft* Windows* Vista*. If the UAC is enabled during the installation of Novell SecureLogin, you are prompted about whether you want to continue with the installation process. If you do not respond to the prompts for a long time, a screen saver might come up (depending on the desktop setting) and interrupt the installation process, requiring you to restart the installation.

If the UAC prompts must be avoided, the administrator must disable the UAC setting within the Microsoft Windows Vista.

NICI Client Is Not Uninstalled

Novell International Cryptography Infrastructure (NICI) is installed automatically when SecureLogin is installed in any of the following modes:

- LDAP
- eDirectory with LDAP
- eDirectory with Client32 as the protocol and Novell SecretStore is selected for installation

However, if you uninstall SecureLogin, the NICI client remains because other Novell services (for example, NMAS™, Novell Clien™t, and SecretStore®) might also need the NICI client.

If you plan to uninstall the NICI client, ensure that it is no longer needed before you remove it. To uninstall the NICI client, use *Add/Remove Programs*.

Validating an Old Password

In Microsoft Windows 2003 configurations, users might be able to login to their workstation by using the old password. Because the user has logged in successfully, Novell SecureLogin loads. A Windows 2003 server attribute (the password lifetime period) allows the re-use of an old password.

To disable an old password as soon as a password change occurs, update the domain controller registry setting with the following value:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`

Create new `DWORD` value OldPasswordAllowedPeriod

Set this value to 0.

For more information, see the Microsoft Web site. (http://support.microsoft.com/kb/906305)

Installing a New Version of Java on Windows Vista

If a new version of Java* is installed after installing Novell SecureLogin, the next time you run Novell SecureLogin, it checks for new versions of Java to enable single sign-on.

If a new version of Java is detected, the required information must be updated in `C:\Program Files\Java`, and some files must also be modified in the process. However, Windows Vista does not permit you to write to the `C:\Program Files\Java` files unless you elevate privileges.

To resolve this:

1. Stop the Novell SecureLogin application.
2. Locate `slproto.exe` > right-click it, then select *Run As Administrator*.
3. Specify the administrator password.

   You are now working with administrator privileges and can successfully write to the Java folder.

NSL Login in LDAP GINA Mode with eDirectory

NSL in the LDAP GINA mode with eDirectory™ does not work while setting a passphrase for a new user if the eDirectory user's fully distinguished name (FDN) has 128 characters or more.

SecureLogin Using LDAP Fails to Detect Network Connection Status on VMWare

On VMWare*, SecureLogin in LDAP mode fails to detect the network connection status. Therefore, SecureLogin never switches to the Offline Login dialog box directly and always displays the LDAP Login dialog box.

?syspassword Reflects Universal Password or Simple Password

When SecureLogin is installed in LDAP mode and NMAS authentication is used, ?syspassword reflects the universal password for the logged-in user.

In this mode of operation, it is mandatory to configure and set universal password for the NMAS user.

Display of LDAP GINA On Client With Conflicting IP Addresses

If Novell SecureLogin 7.0 is installed on a workstation with conflicting IP addresses and restarted, it is observed that the LDAP GINA dialog is not displayed. Instead the Novell security message, `You have Encountered unexpected Login Failure: status:0X6f634` is displayed. Users cannot login to workstation or the network.

The resolve the issue:

1. Boot the workstation in *Safe Mode with Networking option*.
2. Change the IP address of the workstation.
3. Restart the workstation.

Using the Workstation Only Option

The login function provided by the *Workstation Only* option was enhanced in hotfix 4 of Novell SecureLogin 6.1 release.

With the release of Novell SecureLogin 6.1, if a user logged in to the workstation through the Workstation only option, he or she was prompted to provide the username and password or passphrase. Because the user was not connected to the network, Novell SecureLogin could not retrieve the user's eDirectory credentials and needed to prompt for them again after Windows launched.

This issue is fixed in Novell SecureLogin hotfix 4.

During the Workstation only login, if the workstation or local credentials are the same as eDirectory credentials, the user is not prompted for the credentials. Novell SecureLogin seamlessly logs in the user.

However, to allow this, the user must manually change the DWORD value of the `TryRegCredInOffline` registry.

IMPORTANT: The user must have logged in to eDirectory at least once to make the change, and must have Novell SecureLogin 6.1 with hotfix 4 and the Novell Client 4.91 SP4 with the latest patch

---

To change the DWORD value:

1. Use a registry editor to access the Windows registry.
2. Change the DWORD value of `TryRegCredInOffline` in `HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin\` as follows:
   - DWORD value of 0 == disabled (default behavior if key is not defined)
   - DWORD value of 1 == enabled (try to login WS only with GINA creds)

   A seamless login to offline mode by using the Windows user credentials happens if the DWORD value is set to 1. Also, the following conditions must be met:
   - LDAP is installed in Credential Manager, GINA mode, or Credential Provider mode.
   - The network or the server is not reachable for the client workstation.
   - The LDAP and Windows user credentials are same.
   - The LDAP user is associated to the Windows user.

     NOTE: This is applicable for LDAP Credential Manager mode.

   - During the log in for GINA or Credential Provider mode, the *Workstation only* option is selected.

Novell SecureLogin Fails When a User With the Same Name and Context in Two Different eDirectory Trees Tries To Log In To The Same Windows Machine

When a user with the same name and context in two different eDirectory trees tries to log in to the same Windows machine, an error message "`Your Cache files have lost synchronization with your directory data. Would you like to delete your local cache files have them re-created?`" appears.

When you click *OK* and proceed, credentials of the previous user with same name are deleted and the cache file has only your credentials.

SecureLogin Using LDAP Fails to Detect Network Connection Status on VMWare

On VMWare*, SecureLogin in LDAP mode fails to detect the network connection status. Therefore, SecureLogin never switches to the Offline Login dialog box directly and always displays the LDAP Login dialog box.

`?syspassword` Reflects Universal Password or Simple Password

When SecureLogin is installed in LDAP mode and NMAS authentication is used, `?syspassword` reflects the universal password for the logged-in user.

In this mode of operation, it is mandatory to configure and set universal password for the NMAS user.

Login Fails for NMAS Post Login Methods for eDirectory 8.8 SP1 or NMAS3.1.0 Server Version

If users have a login with the post-login method (Secure Workstation), users are unable to log in if the Directory is eDirectory 8.8 SP1, because the default NMAS server version installed is NMAS 3.1.0.

If users have a login with the post-login method (Secure Workstation), users are unable to log in after upgrading eDirectory to 8.8 SP1 or to NMAS 3.1.0.

To resolve this, users must upgrade to NMAS 3.1.1 or later by using the Security Service 2.0.2 available at the Novell Download Web site (http://download.novell.com/Download?buildid=9hi7-ELIZ64).

Firefox During Installation

We recommend that you start Mozilla* Firefox* at least once before installing Novell SecureLogin. Otherwise, a message prompting you to import Internet Explorer settings, is displayed during the Novell SecureLogin installation.

If this happens, click *Import* to import the Internet Explorer* setting or click *Cancel* to cancel the import. Novell SecureLogin installation proceeds.

Notification Area Icon Cannot Be Unlocked Using pcProx Authentication

You cannot unlock the SecureLogin notification area (system tray) icon using the NMAS pcProx authentication. Unlock the icon by using the passphrase if you have enabled one, or by using your directory password. Alternatively, you can set and use an universal password.

Logging In after Uninstalling the ZENworks for Desktops Management Agent

Under the following conditions, you might not be able to log in to your workstation:

- ZENworks® for Desktops 4.0.1 Management Agent is installed.
- SecureLogin is installed
- You uninstall the ZENworks for Desktop Management Agent and then restart the workstation.

To solve the problem:

1. Start the workstation in Safe mode.
2. Copy the `nwgina.dll` file to the `windows\system32` directory.

SecretStore on the Server

If you plan to use Novell SecretStore® on the client (SecretStore mode), install or upgrade to SecretStore 3.3.5 or later on the server before selecting the SecretStore option during the client install.

Setting Up a Passphrase

3

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.

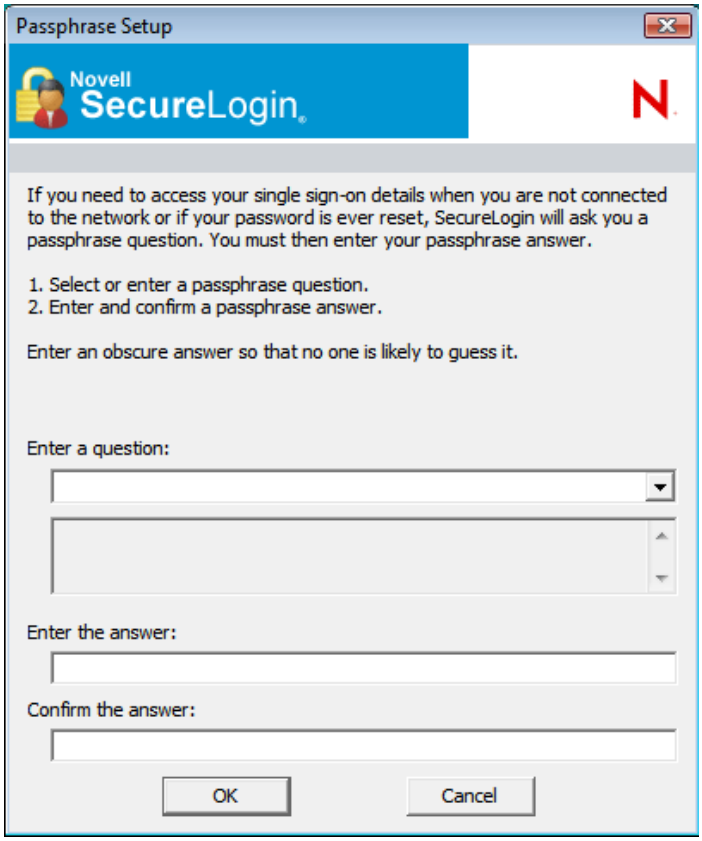
During installation, the passphrase security is enabled to enforce passphrase setup during the initial login. You can disable the passphrase policy by deselecting *Use Passphrase Policy* option in the *Advanced Settings* pane of the Administrative Management utility. If a passphrase has previously been 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. You cannot access the answer if you forget it.

To set up a passphrase:

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



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

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

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

Installing, Configuring, and Deploying in a Novell eDirectory Environment

II

This section provides information on configuring, installing, and deploying Novell® SecureLogin in a Novell eDirectory™ environment.

Before You Begin

4

Before you proceed with installing Novell® SecureLogin in eDirectory™ environment, ensure that you have sufficient disk space and that you have the required versions of additional components listed in the following sections:

4.1 Disk Space

A minimum of 128 MB space is required in the Windows* directory. An additional 55 MB is required for temporary files, which is deleted after installation is complete.

4.2 NICI

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

- Any LDAP platform
- The Novell SecretStore® client feature
- The NMAS™ client feature

NOTE: If you are using NMAS, you must install NICI manually before installing the NMAS client.

Novell SecureLogin requires NICI 2.7.2. Both 32-bit NICI and 64-bit NICI must be installed on a Windows Vista* 64-bit and Microsoft Windows 2008 64-bit..

4.3 NMAS

IMPORTANT: Make sure that Novell Client™ 4.91 or later is installed on your machine before installing NMAS. In addition, make sure that NICI is already installed before you install the NMAS client.

Novell SecureLogin requires the NMAS Client 3.4.3

When installing Novell SecureLogin in eDirectory environment, install the NMAS Client manually before installing Novell SecureLogin.

- For installing on Microsoft* Windows Vista 32-bit, NMAS is available in `\Nmas\NmasClient\x86\Vista nmasclient_v32.exe` in your Novell SecureLogin Windows installer package.

- For installing on Microsoft Windows Vista 64-bit, NMAS is available in `\Nmas\NmasClient\x64\ nmasclient_v64.exe`
- For installing on Windows XP and 2003, NMAS is available in `\Nmas\NmasClient\x86\win32\ nmasclient_setup.exe` in your Novell SecureLogin Windows installer package.

Installing

5

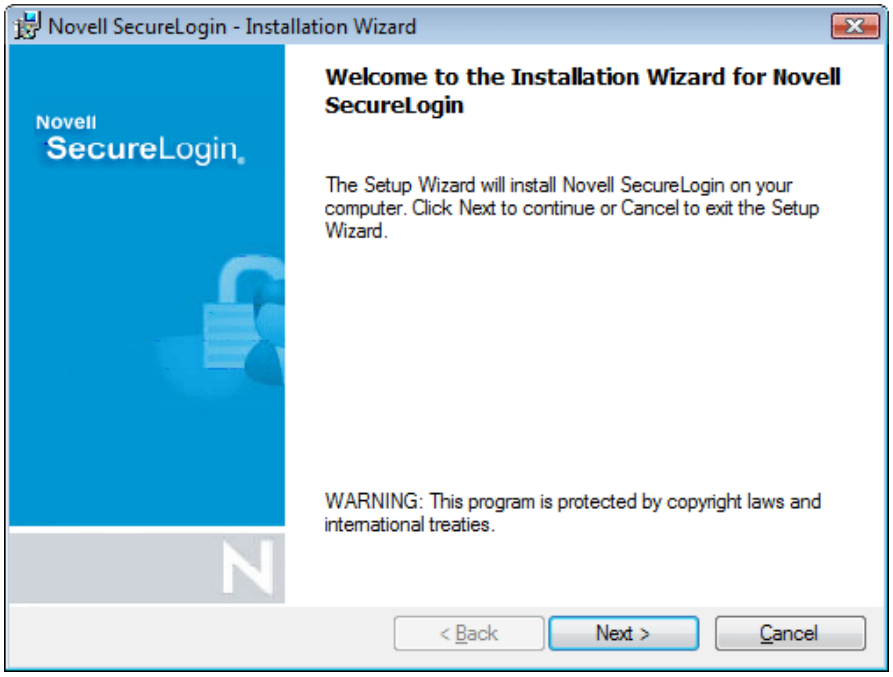
Choosing to install Novell® SecureLogin in a Novell eDirectory™ environment installs Novell SecureLogin on networks that are running eDirectory. This option provides you a secure, centralized storage of user login data by performing encryption on the workstation before the data is saved to eDirectory.

NOTE: The procedures for installing on administrator workstations and user workstations are the same.

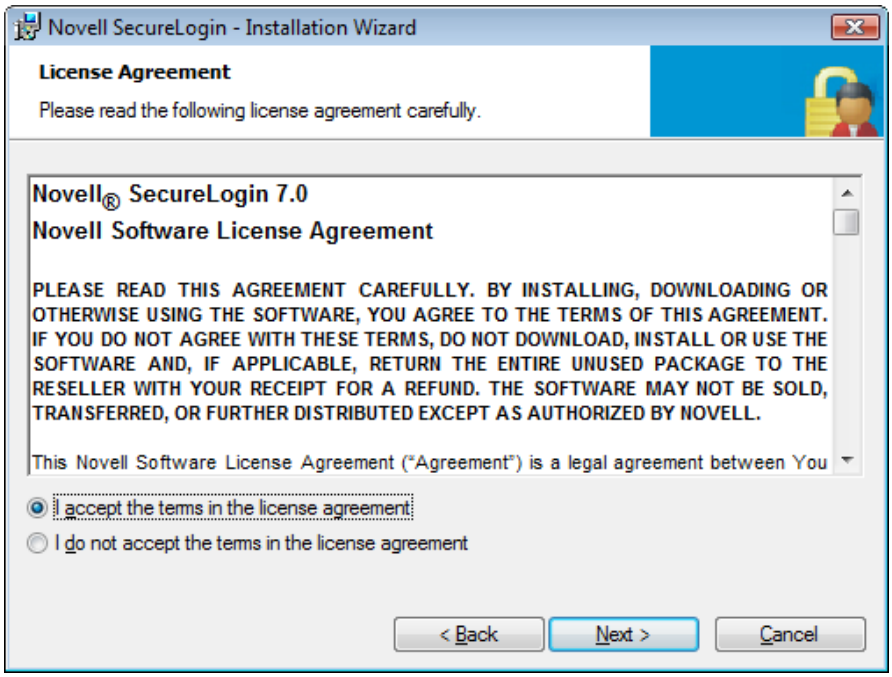
The following procedure uses the Microsoft Windows Vista 64-bit installer.

---

1. Log in to the workstation as an administrator.
2. Double-click `Novell SecureLogin.msi` located in the `SecureLogin\Client\x64` directory of the Novell SecureLogin installer package. The Welcome to the Installation Wizard for Novell SecureLogin is displayed.



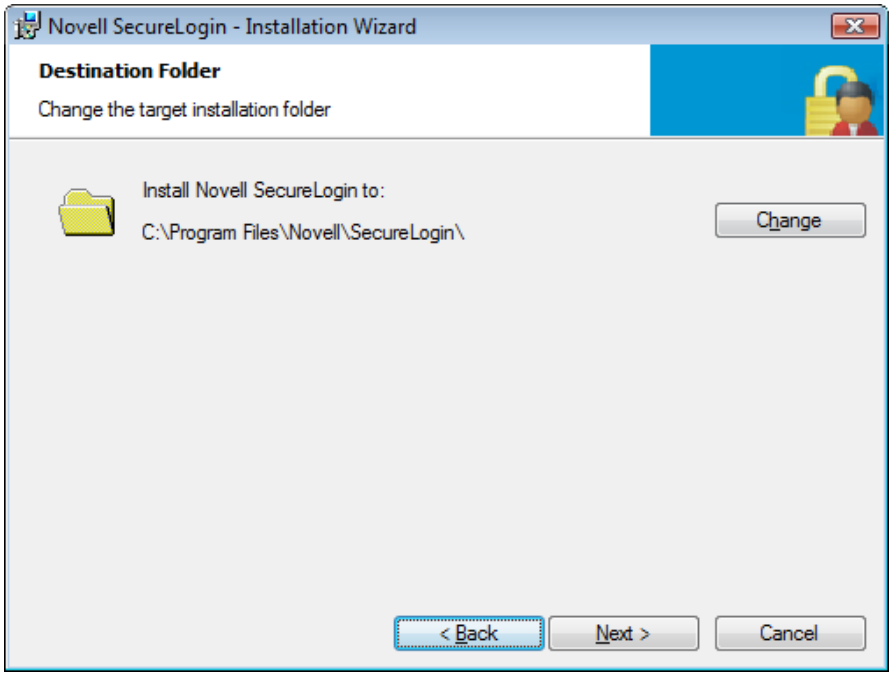
3. Click *Next*. The License Agreement page is displayed.



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

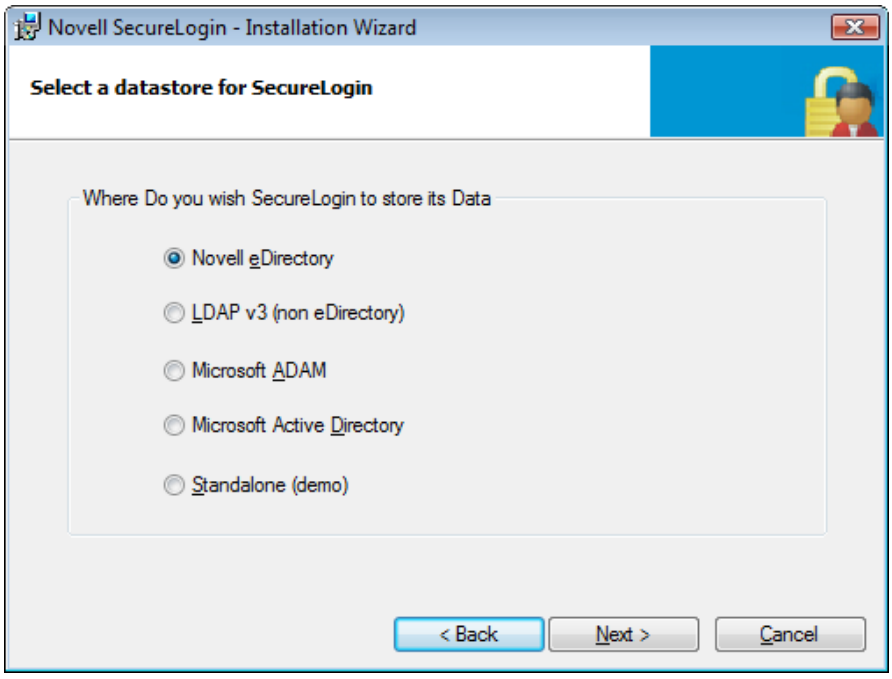
The Destination Folder page is displayed. By default, the program is saved in `C:\Program Files\Novell\SecureLogin\`.You can accept the default folder or choose to change.

To change, click *Change* and navigate to your desired folder.



5 Click *Next*. Select a Datastore for SecureLogin (that is, the installation environment) page is displayed.

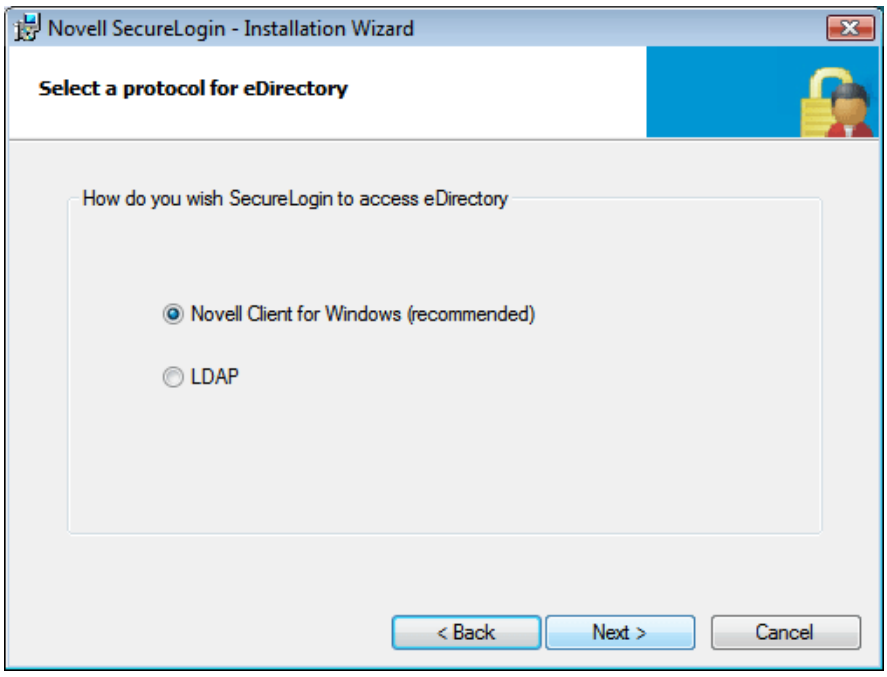
6 Select *Novell eDirectory* as the platform where Novell SecureLogin stores its data, then click *Next*.



7 Select the protocol to access eDirectory.

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

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

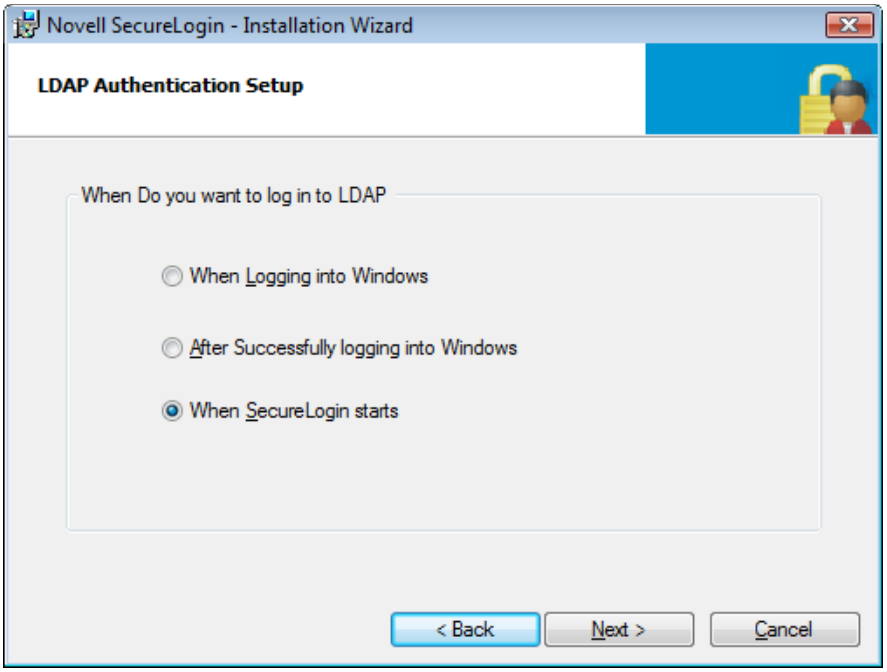


8 (Conditional) If you selected *Novell Client for Windows* in Step 7:

8a Click Next. Continue with Step 9d.

9 (Conditional) If you selected *LDAP*in Step 7;

9a Click *Next*. The LDAP authentication setup dialog box is displayed.



9b Click *Next*. The LDAP server information dialog box is displayed. Select one of the following options:

- **When Logging into Windows:** This is the LDAP (GINA) mode. If you select this option, the default Windows login dialog box is replaced by the Novell SecureLogin authentication dialog box . If the directory authentication is successful, Novell SecureLogin launches seamlessly.

  Continue with Step 9c.

- **After Successfully logging into Windows:** This is the LDAP Credential Manager mode. If you select this option, Novell SecureLogin login dialog box appears after logging in to Windows and before the desktop screen appears. Novell SecureLogin starts seamlessly after the desktop opens.

  1. Select the login user to be associated with your LDAP distinguished user.
  2. Click *Next*. Select how you want to associate your Windows username with the LDAP distinguished name.
  3. Click *Next* and continue with Step 9c.

  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 the Novell Client installed, the default account association is a Windows association.

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

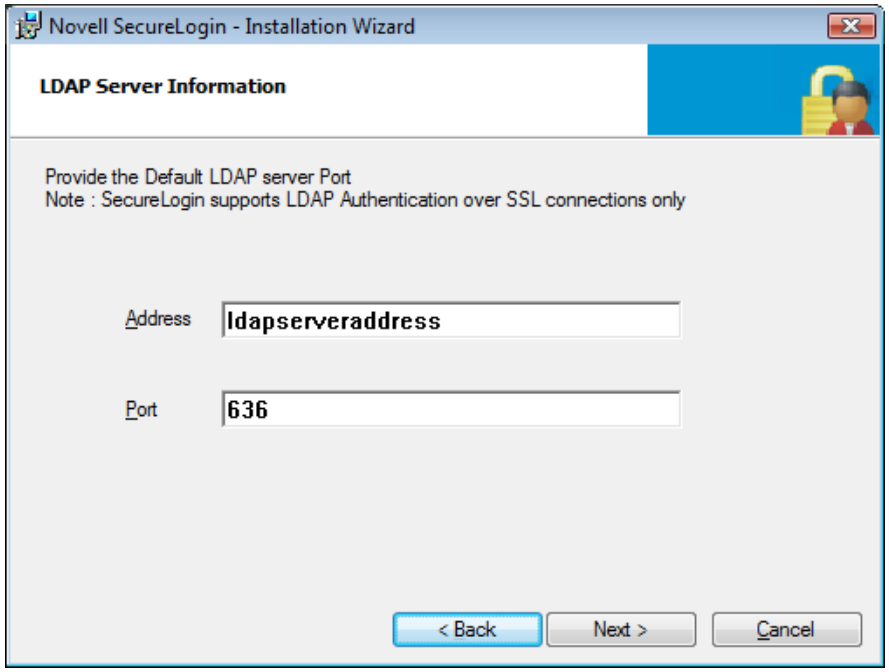
`DoNTAssoc DWORD` *1*

`DoClient32Assoc DWORD` *0*

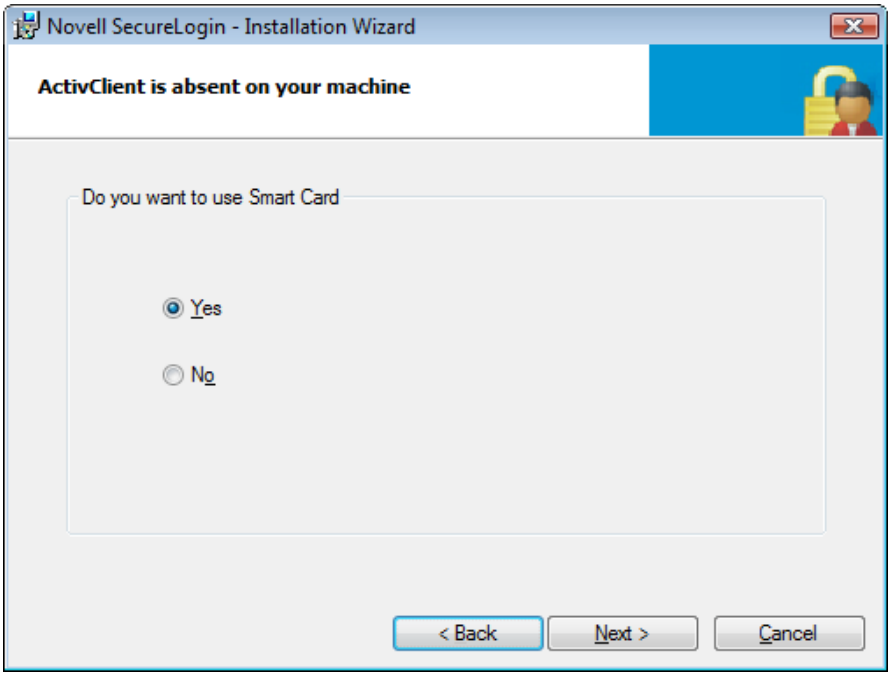
- **When SecureLogin Starts:** This is the LDAP authentication mode. Novell SecureLogin launches after the desktop comes up. Otherwise, the desktop loads and you must manually launch Novell SecureLogin.

  Continue with Step 9c.

9c Click *Next*. Specify the LDAP server information.



9d Click *Next*. The smart card dialog box is displayed.



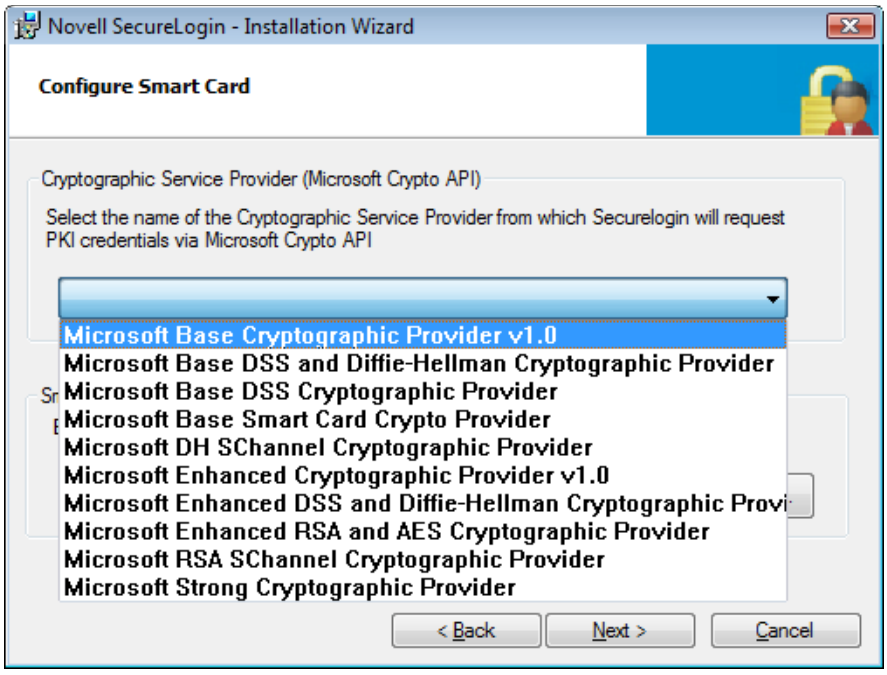
10 (Conditional) If you want to use a smart card, select *Yes* >, click *Next,* then continue with Step 12.

IMPORTANT: If your enterprise policy allows users log in to the workstation by using a smart card, you must select the smart card option.

---

11 (Conditional) If you do not want to use a smart card, select *No* >, click *Next*, then continue with Step 14.

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



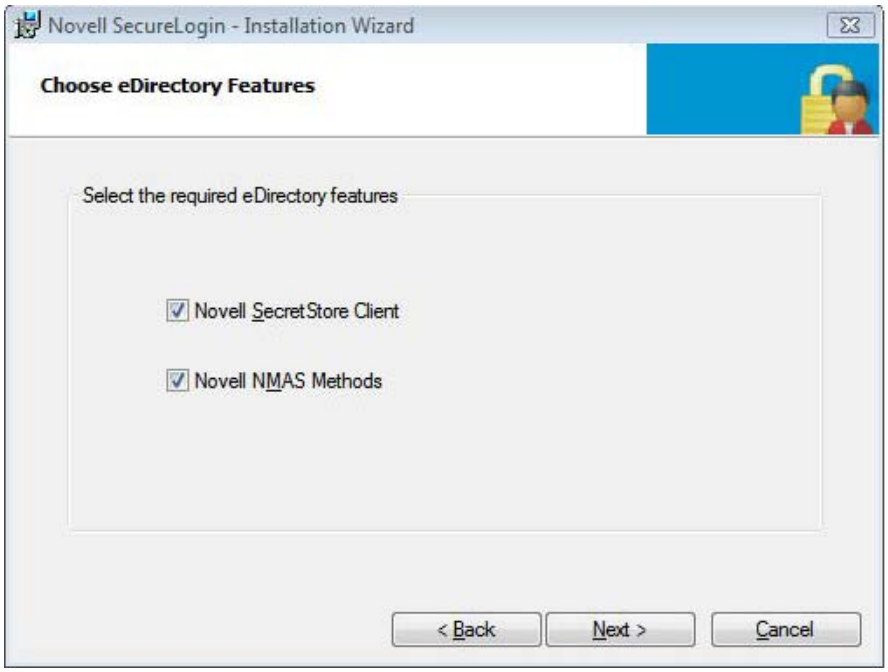
13 Select a PKCS#11 compatible library required for accessing the smart card, then click *Next*.

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 Novell 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.

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

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



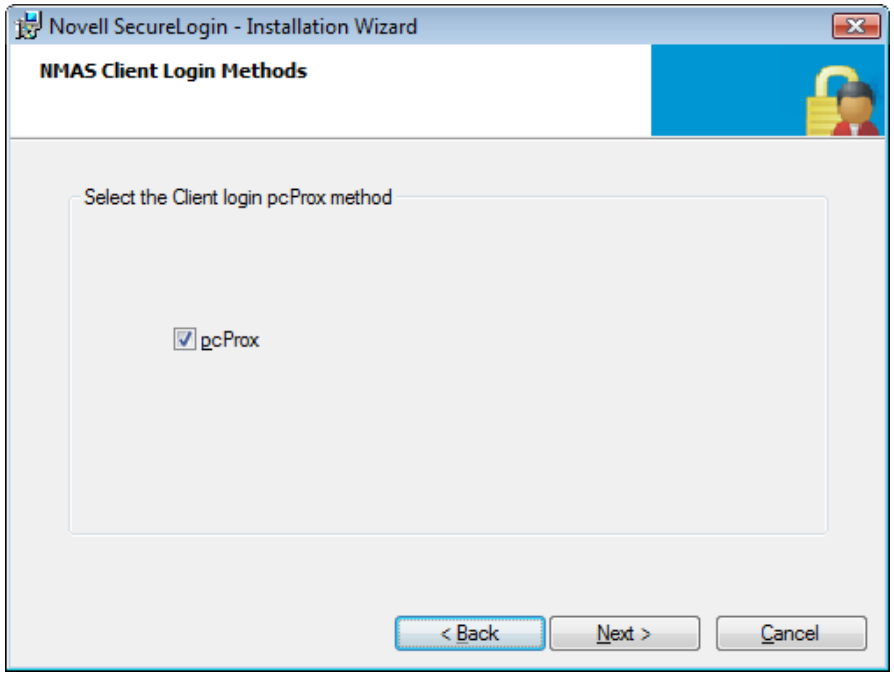
15 Select the NMAS Methods, such as pcProx and Secure Workstation, then proceed with the installation.

16 (Conditional) If you selected *Novell SecretStore Client* in Step 14. ensure that SecretStore is installed on a server, then continue with Step 18.

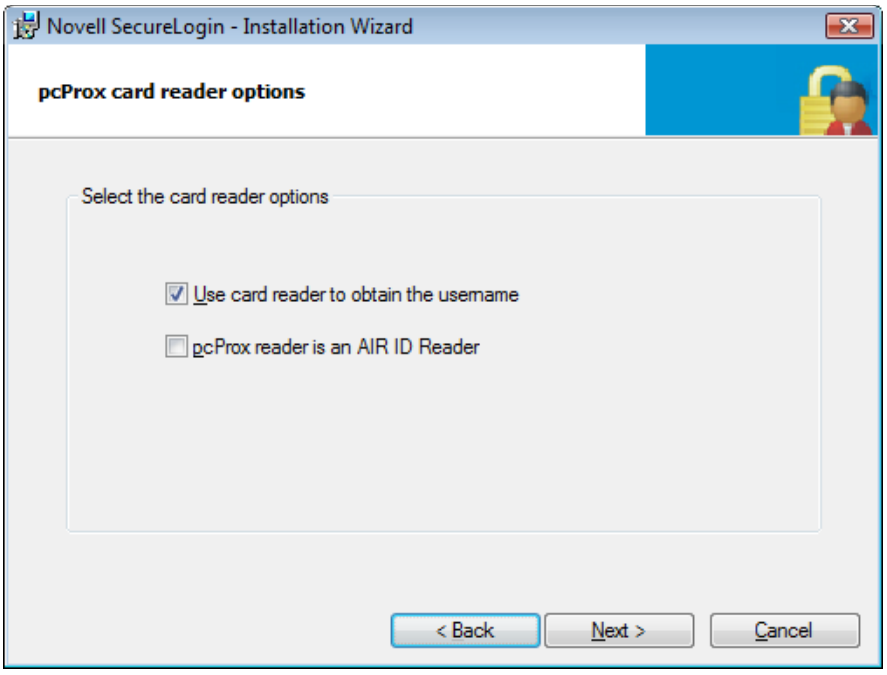
For more information on SecretStore, see "Installing SecretStore" (http://www.novell.com/documentation/secretstore34/nssadm/index.html?page=/documentation/secretstore34/nssadm/data/bsqde0s.html) in the *SecretStore 3.4 Administration Guide*. (http://www.novell.com/documentation/secretstore34/index.html)

17 (Conditional) If you selected *Novell NMAS methods* in Step 14, the NMAS Client Login Methods dialog box is displayed.

17a Select *pcProx*, then click *Next*. The pcProx card reader options dialog box is displayed.

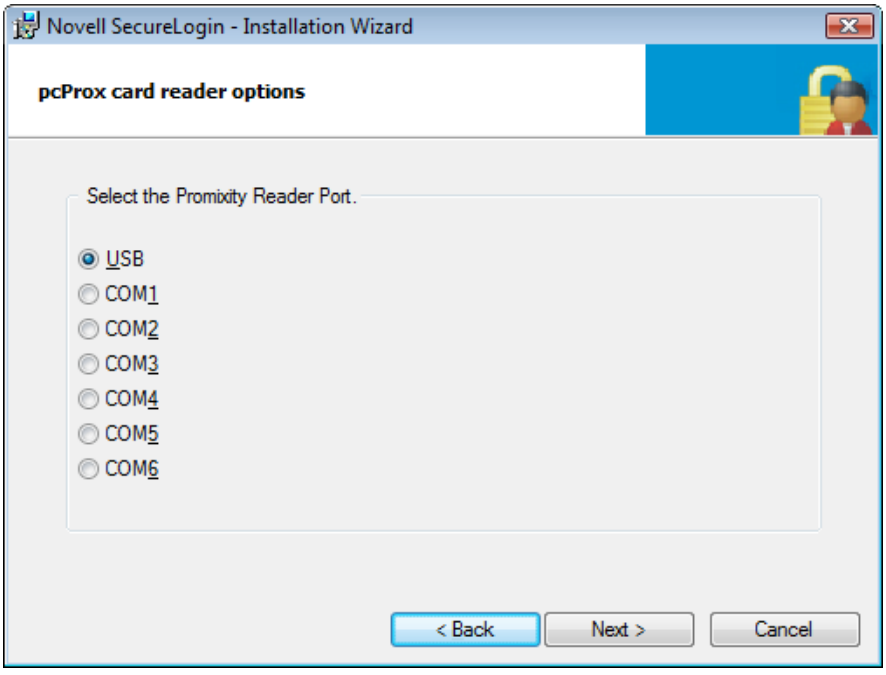


17b Select either *Use card reader to obtain the username* or *pcProx reader is an AIR ID Reader*.

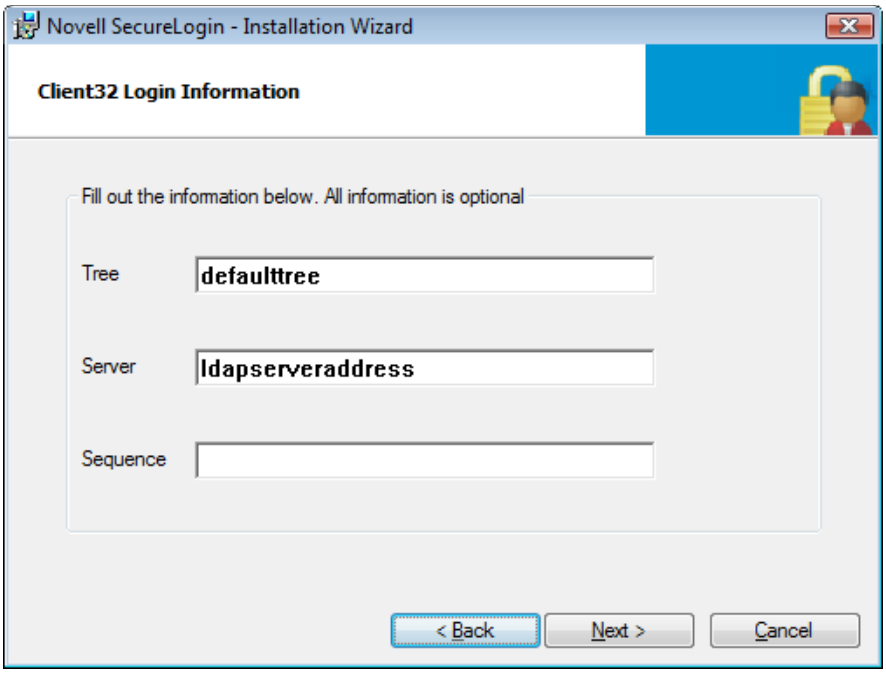


17c Click *Next*. The pcProx card reader options dialog box is displayed.

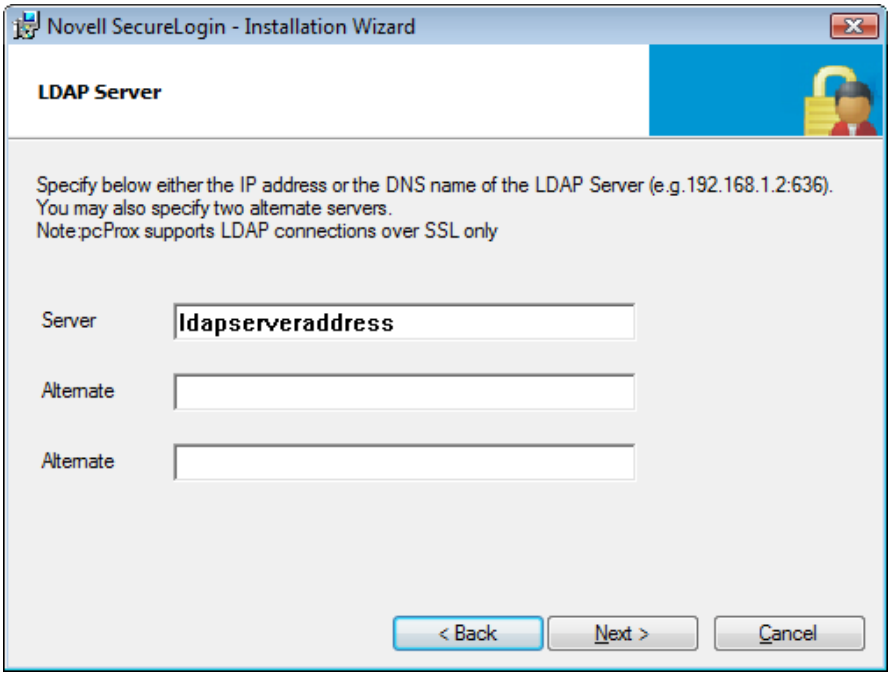
17c1 Select a port for the proximity reader.



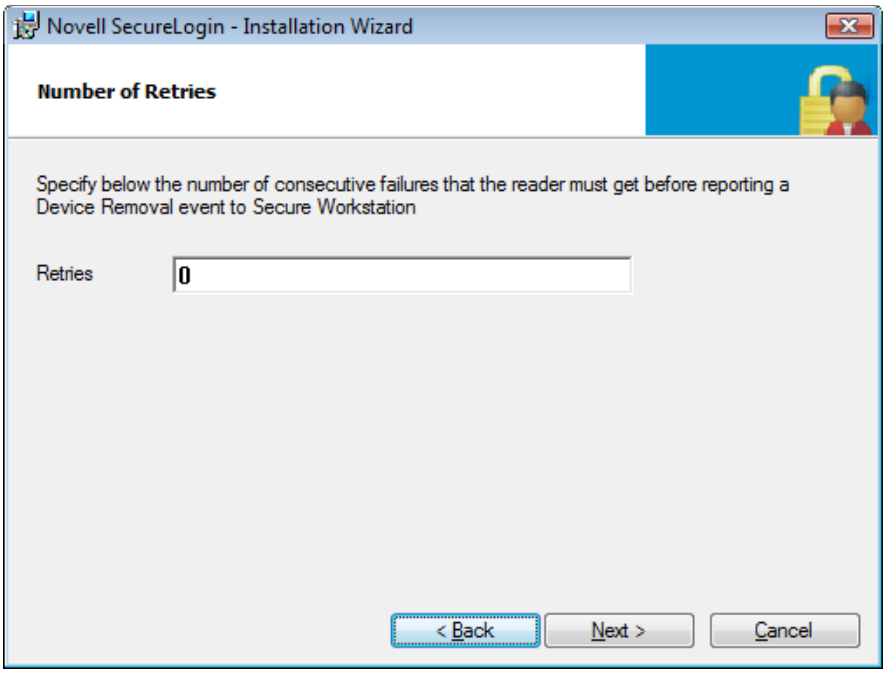
17c2 Click *Next*. The Client32 Login Information dialog box is displayed. Specify the Tree, Server, and Sequence information.



17c3 Click *Next*. The LDAP server dialog box is displayed. Specify the server and alternate server information.



17c4 Click *Next*. Specify the number of failures that are allowed before reporting a device removal event to Secure Workstation.

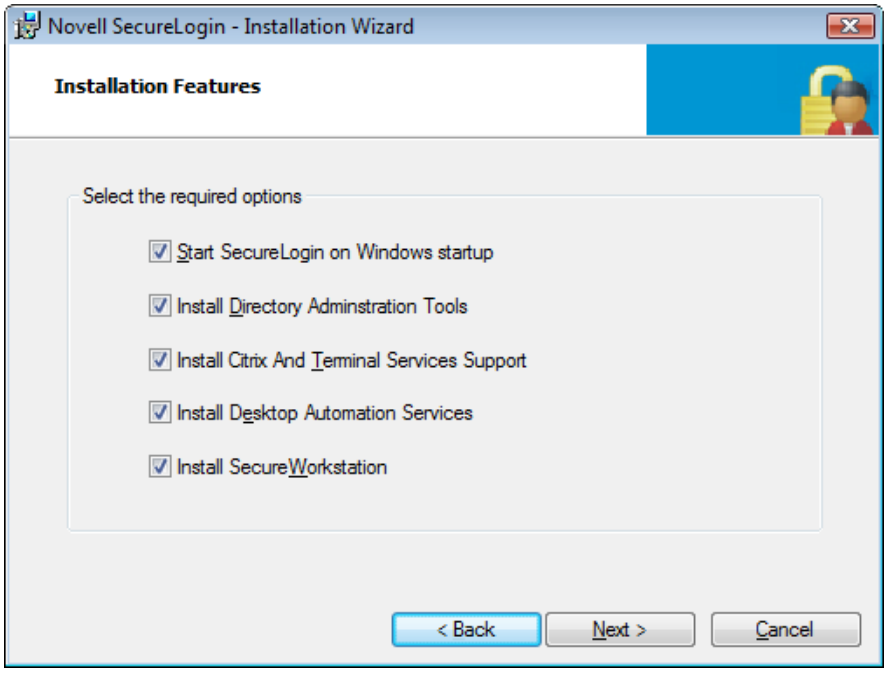


17c5 Click *Next*. The cache option dialog box is displayed.

pcProx supports LDAP connections over Secret Socket Layer (SSL) only.

18 Select the location where you want Novell SecureLogin to store the local cache.

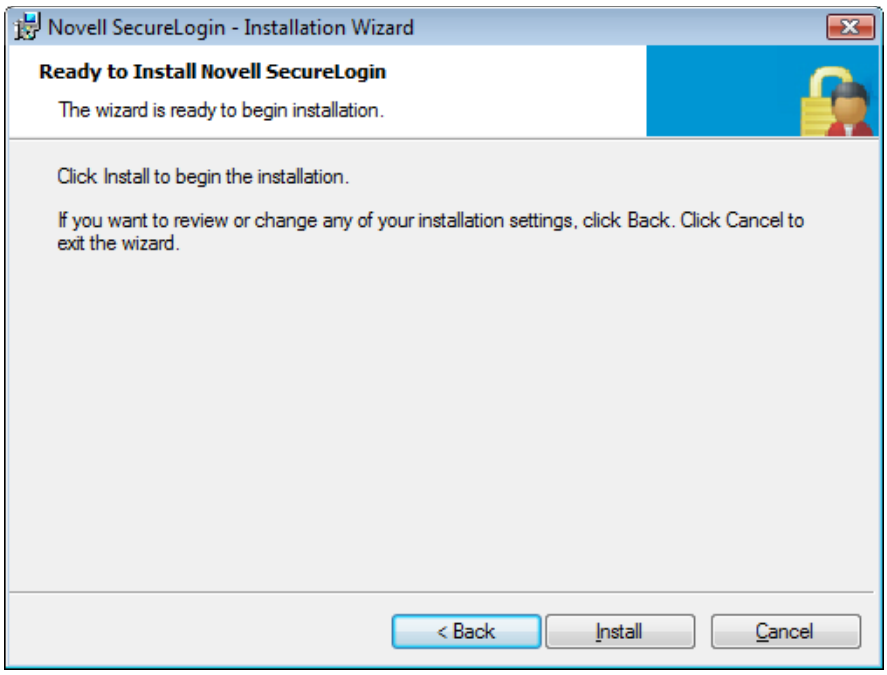
19 Click *Next*. The installation features dialog box is displayed.



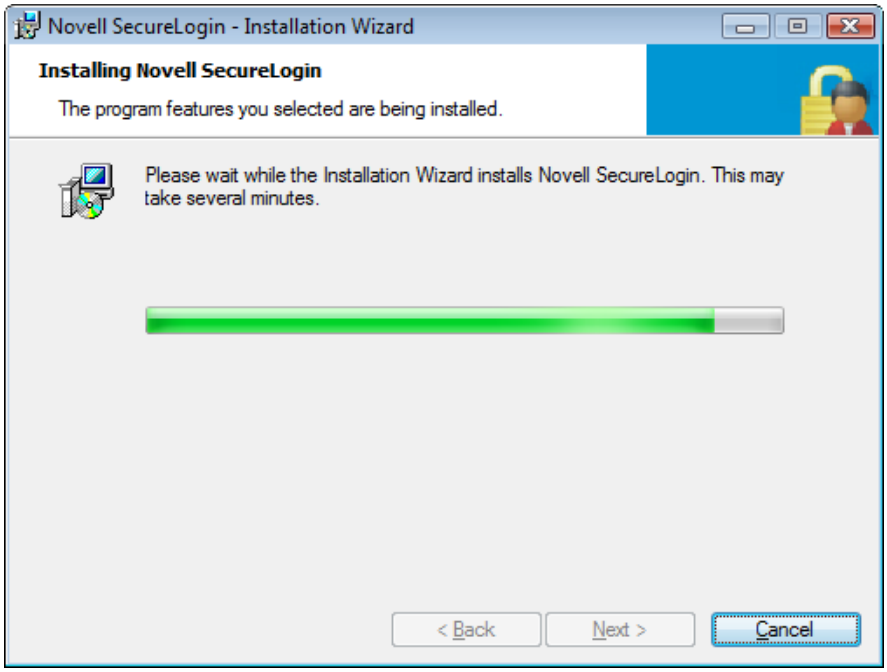
20 Select a location for the configuration file.

If you select *Directory* as the location, you must specify the tree or the IP address of the server and specify a value of the config object on the server tree.

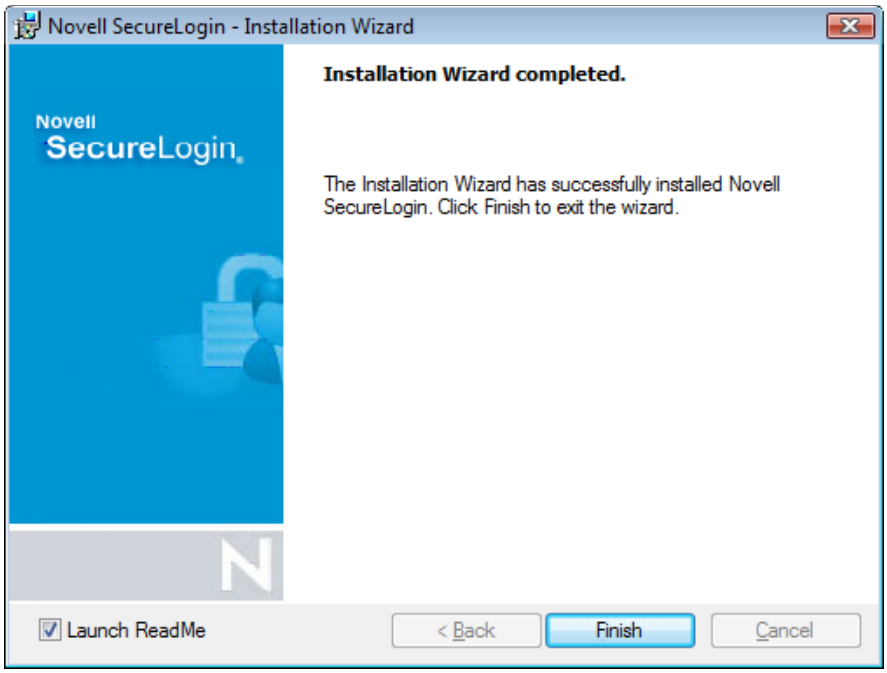
21 Click *Next*. The Ready to Install the Program page is displayed.



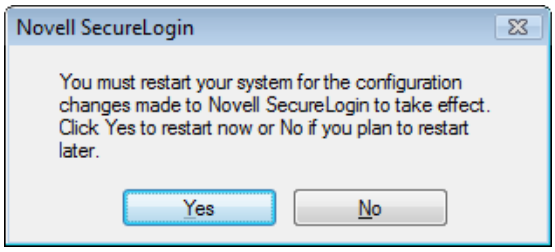
22 Click *Install*.



23 Click *Finish*.



24 You are prompted to restart your system. Select *Yes*. .



5.1 LDAP Credential Provider for Microsoft Windows Vista

With Windows Vista, Microsoft changed the login architecture and replaced the GINA with the Credential Provider for intercepting login details.

When the Credential Provider replaces the GINA module, it minimizes the conflict when multiple authentication methods are used on a shared workstation. A Credential Provider supports multiple concurrent providers, and makes it much easier to implement new user authentication scenarios supported by the operating system. It can be either user-driven or event-driven.

With the Credential Provider module, Novell no longer needs to re-author the user interface for the users. Users are presented with one login dialog box.

Currently, the Credential Provider model for Novell SecureLogin is compatible only with installation on eDirectory and any LDAP v3 compliant mode.

Configuring and Deploying

6

To make Novell® SecureLogin functionality available to users, you must first extend the eDirectory™ schema. You can also provide additional security through Novell SecretStore® and by requiring users on shared workstations to log out securely.

6.1 Extending the eDirectory Schema

You must extend the Novell eDirectory schema to enable Novell SecureLogin to save users’ single sign-on information. `ndsschema.exe` found in `Securelogin\Tools\Schema\`NDS directory 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 4.91or later installed on your machine.

NOTE: If you use iManager to administer Novell SecureLogin, you must also extend the LDAP schema. For information on extending the LDAP schema Section 9.3, “Extending the LDAP Directory Schema and Assigning Rights on the Server,” on page 59.

---

1. Run `ndsschema.exe`.

   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 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

2. Specify the 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 (Optional) Grant rights to local cache directories.

Users on 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).

6.2 Using the SecretStore Client for Enhanced Security

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

You can choose to install SecretStore while installing Novell SecureLogin. For information on installing SecretStore Client when installing Novell SecureLogin, refer Step 14 on page 35.

- If you are using eDirectory 8.7.3, upgrade SecretStore on your server to version 3.3.5
- If you are using eDirectory 8.8, upgrade SecretStore on your server to version 3.4

For more information on SecretStore, see "Installing SecretStore" (http://www.novell.com/documentation/secretstore34/nssadm/index.html?page=/documentation/secretstore34/nssadm/data/bsqde0s.html) in the *SecretStore 3.4 Administration Guide*. (http://www.novell.com/documentation/secretstore34/index.html)

6.3 Deploying Novell SecureLogin on Shared Workstations

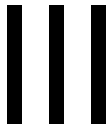
If Novell SecureLogin in deployed on a shared workstation where more than one user shares the local credentials, you should require users to use either Secure Workstation or DAS to close all programs and log out of the network.

This is because Novell SecureLogin fails to log off directory users on a shared workstation. Directory users who have logged in with workstation credentials are not disconnected and can access the directory data store.

This occurs when users use either of the following to lock the workstation and later try to unlock the workstation using the workstation credentials.

- Novell SecureLogin in Novell Client mode on Microsoft Windows Vista or Microsoft Windows XP.
- Novell SecureLogin in LDAP mode on Microsoft Windows Vista.

Installing, Configuring, and Deploying in an LDAP Environment



This section explains installing, configuring, and deploying Novell SecureLogin in an Lightweight Directory Access Protocol (LDAP) environment. LDAP is an open-directory structure that provides fast access to the directory.

The LDAP authentication client uses LDAP to connect to a server and securely administer applications enabled for single sign-on.

Novell SecureLogin supports LDAP authentication over Secret Socket Layer (SSL) connections only.

The instructions and examples in this section applies to the majority of LDAP compliant directories. Specific examples are given for Sun* Java* System Directory Server and a directory server managed through an administration workstation. If you have implemented another LDAP directory environment, refer the particular documentation or contact Novell Support for help.

This section consists of the following sections:

Prerequisites

7

Before proceeding with installing Novell SecureLogin 7.0 in an LDAP environment, ensure that the following prerequisites are in place:

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

- Certificate servers are installed and available on your LDAP server.
- Export a copy of the server certificate in `.der` format to a temporary location for user deployment. Ensure that the extension of the filename is `.der` only. If not, rename the file.
- Have administrator access to the server, directory, and administration workstation.
- Uninstall all versions of Novell SecureLogin prior to version 3.5.*x* and later.
- If you intend to enable single sign-on for Java applications, install one of the following:
  - Sun Java Runtime Engine (JRE) 1.3 or later. You can download this from the Sun Java Web site. (http://www.java.com)
  - Oracle* JInitiator* 1.3.1 or later. You can download this from the Oracle Web site. (http://www.oracle.com)

  on workstations prior to installing Novell SecureLogin.
- Back up the existing directory.

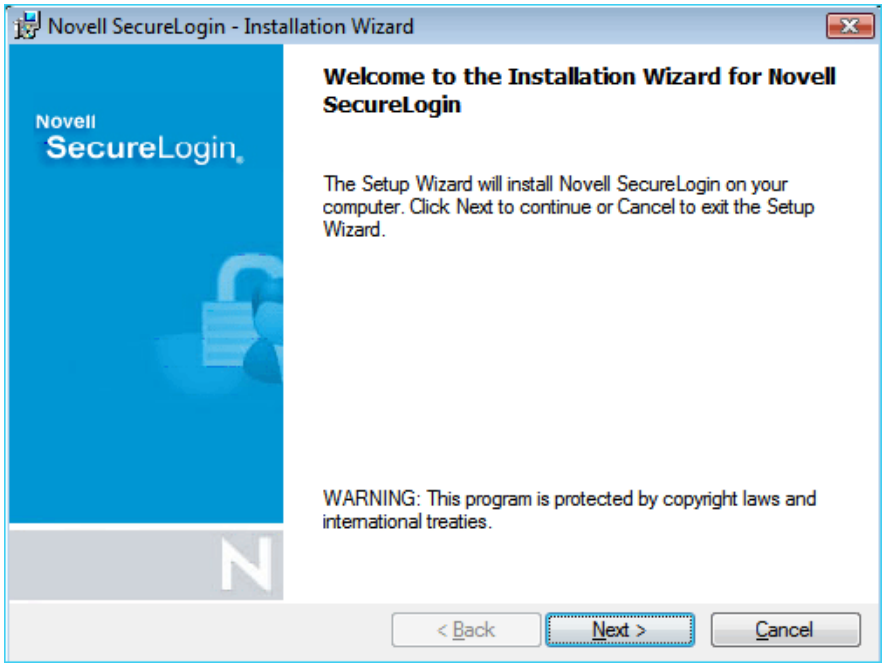
Installing

8

IMPORTANT: The procedure explained in the following section uses the 64-bit installer.

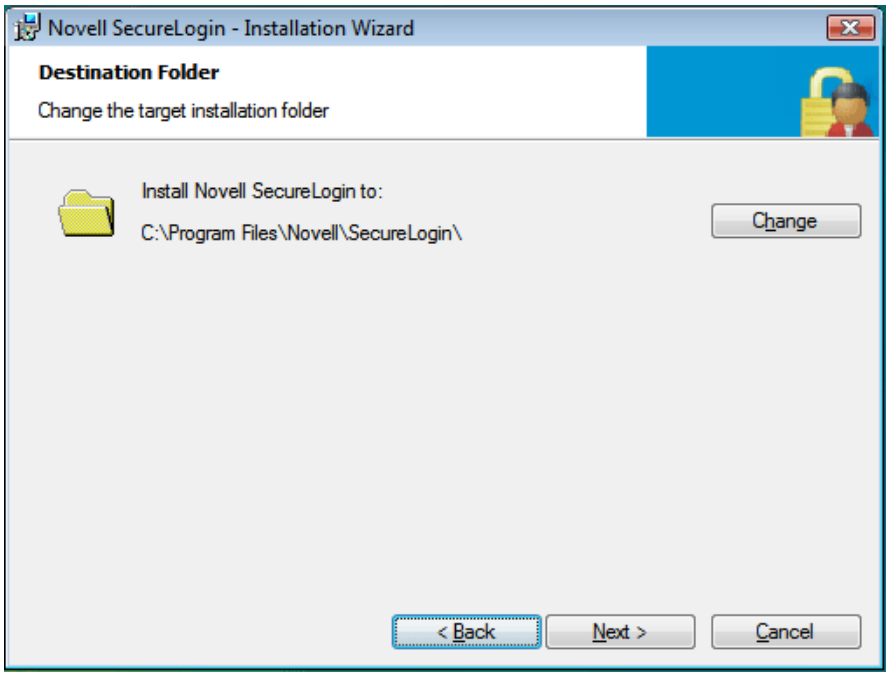
8.1 Installing Novell SecureLogin in Non-eDirectory LDAP Environment

1. Log in to the workstation as an administrator.
2. Double-click the Novell SecureLogin.msi located in the `SecureLogin\Client` directory of the Novell SecureLogin 7.0 installer package to begin the install process. The Installation Wizard launches.



3. Click *Next*. The License Agreement page is displayed.
4. Accept the license agreement, then click *Next*.

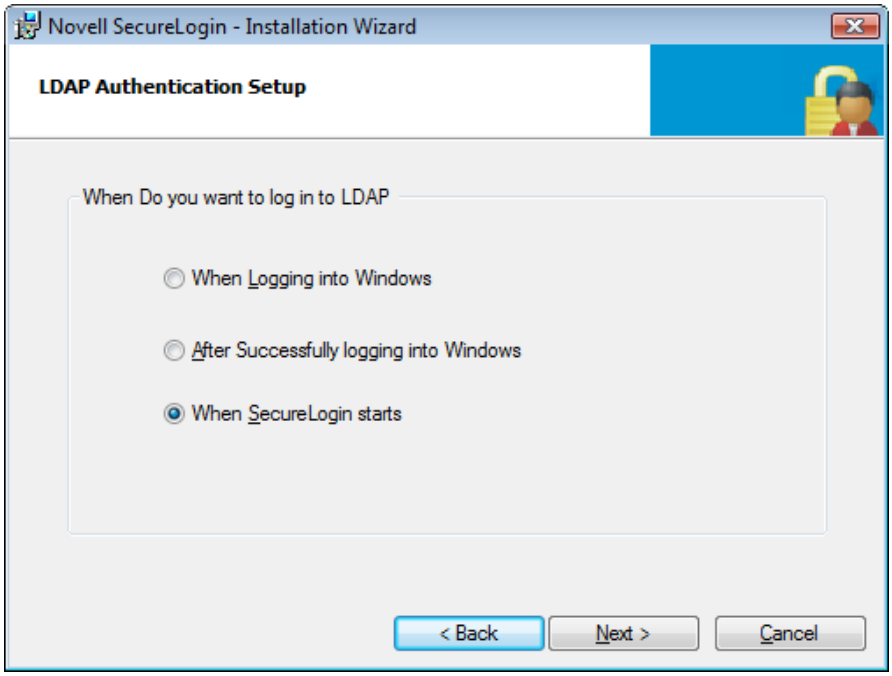
   The Destination Folder page is displayed. By default, the program is saved in `C:\Program Files\Novell\SecureLogin\`.You can accept the default folder or choose to change. To change, click *Change* and navigate to your desired folder.



5 Click *Next*. The Select a datastore for SecureLogin (that is the installation environment) page is displayed.

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

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



Select one of the following options:

- **When Logging into Windows:** This is the LDAP (GINA) mode. If you select this option, the default Windows login dialog box is replaced by the Novell SecureLogin authentication dialog box . If the directory authentication is successful, Novell SecureLogin launches seamlessly.

  Continue with Step 9c.

- **After Successfully logging into Windows:** This is the LDAP Credential Manager mode. If you select this option, Novell SecureLogin login dialog box appears after logging in to Windows and before the desktop screen appears. Novell SecureLogin starts seamlessly after the desktop opens.

  1. Select the login user to be associated with your LDAP distinguished user.
  2. Click *Next*. Select how you want to associate your Windows username with the LDAP distinguished name.
  3. Click *Next* and continue with Step 9c.

  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 the Novell Client installed, the default account association is a Windows association.

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

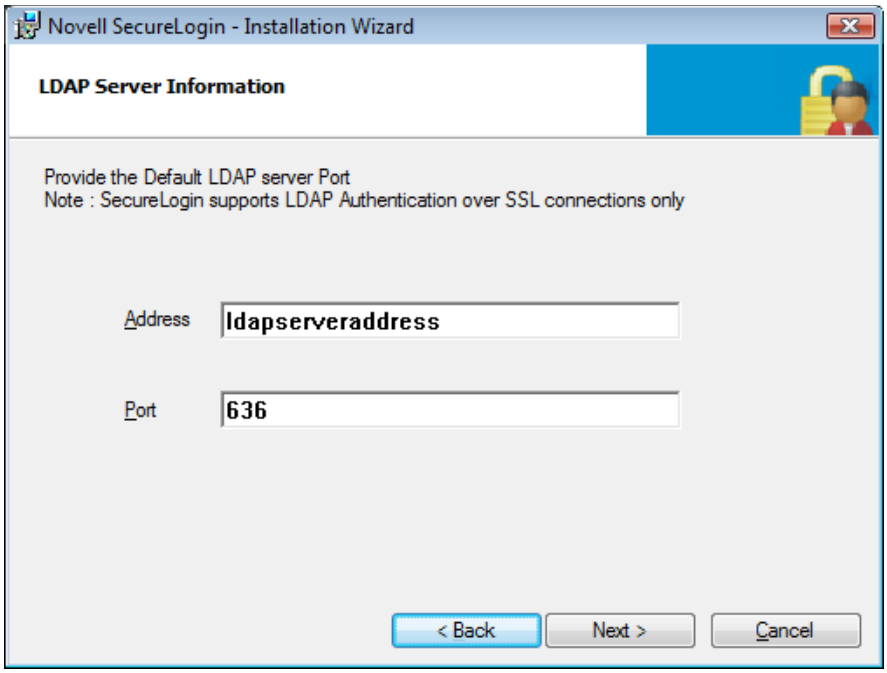
  `DoNTAssoc REG_SZ` *1*

  `DoClient32Assoc REG_SZ` *0*

- **When SecureLogin Starts** This is the LDAP authentication mode. Novell SecureLogin launches after the desktop comes up. Otherwise, the desktop loads and you must manually launch Novell SecureLogin.

  Continue with Step 9c.

8 Click *Next*. Specify the LDAP server information.



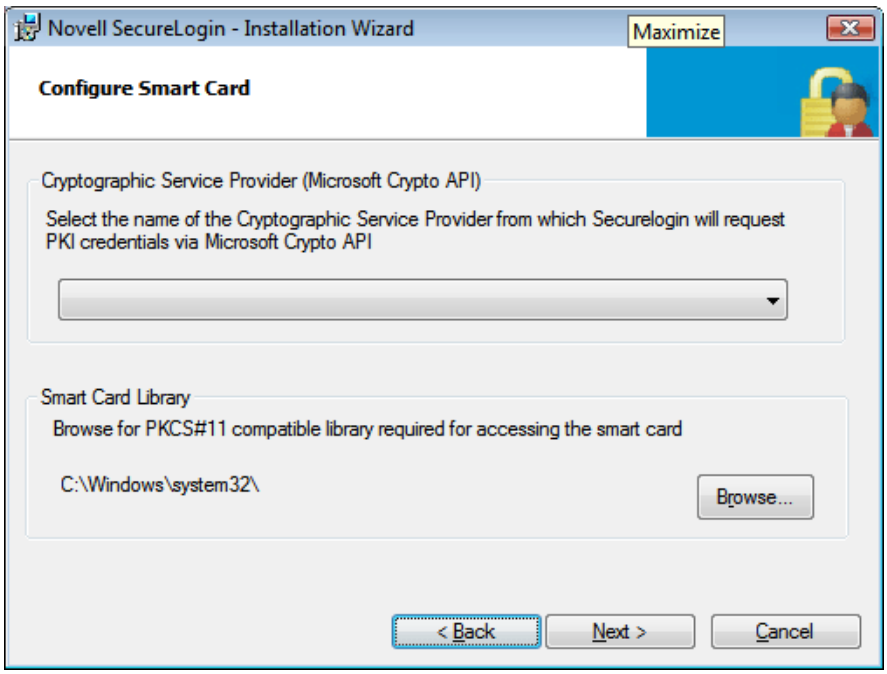
9 Click *Next*. The Smart Card dialog box is displayed.

10 (Conditional) If you want to use smart card, select *Yes* > click *Next*, then continue with Step 12

11 (Conditional) If you do not want to use smart card, select *No* > click *Next*, then continue with Step 14.

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

13 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.

14 Click *Next*. Select the location where you want Novell SecureLogin to store the local cache.

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

16 Select the installation features you want to install.

17 In the Ready to Install SecureLogin dialog box, click *Install*.

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

19 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.

NOTE: The `?syscontext` variable indicates the computer name instead of displaying the context in which the user's directory object resides.

8.2 Installing Novell SecureLogin in LDAP Environment With eDirectory

The LDAP option installs Novell SecureLogin into LDAP v3 directory environments (for example, Novell eDirectory 8.8 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.

1 Log in to the workstation as an administrator.

2 Double-click the `Novell SecureLogin.msi` located in the `SecureLogin\Client` directory of the Novell SecureLogin 7.0 installer package to begin the install process. The Installation Wizard launches.

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

4 Accept the license agreement, then click `Next`.

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 Click *Next*. The Select a datastore for SecureLogin (that is the installation environment) page is displayed.

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

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

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

The three LDAP log in options are:

- **When Logging into Windows:** If you select this option, the default Windows login dialog box is replaced by the Novell SecureLogin authentication dialog. If the directory authentication is successful, Novell SecureLogin launches seamlessly.
- **After Successfully logging into Windows:** If you select this option, Novell SecureLogin login dialog box appears after logging in to Windows and before the desktop screen appears. In this scenario too, Novell SecureLogin launches seamlessly.
- **When SecureLogin Starts:** If you have earlier selected the Launch SecureLogin on Startup option, Novell SecureLogin launches after the desktop comes up. Otherwise, the desktop loads and you must manually launch Novell SecureLogin.

Click *Next*.

8 Specify the LDAP server information. The smart card option page is displayed.

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 11.

10 If you do not want to use smart card, select *No* > click *Next*, then continue with Step 13.

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

12 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.

---

13 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 more information on SecretStore, see "Installing SecretStore" in the SecretStore 3.4 Administration Guide. (http://www.novell.com/documentation/secretstore34/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.

14 (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.

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

16 Select the installation features. Click *Next*.

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

18 Click *Install*.

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

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

NOTE: The `?syscontext` variable indicates the computer name instead of displaying the context in which the user's directory object resides.

8.3 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 to manage LDAP. You can launch this utility through *Start* > *Programs* > *Novell SecureLogin* > *SecureLogin Manager*.

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.

Configuring

9

9.1 LDAP and Active Directory

To install or upgrade Novell SecureLogin 7.0 in an LDAP directory environment, you must extend the LDAP schema with Novell SecureLogin attributes. However, no change is required to Microsoft Active Directory (AD) schema.

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

If the LDAP directory and Microsoft AD are synchronized, Novell SecureLogin can seamlessly pass a users’ AD’s credentials to LDAP so that users enter their login credentials only once.

9.2 Extending the eDirectory Schema

If you are installing on a workstation that uses Novell eDirectory, use the `ndsschema.exe` found in the `\SecureLogin\Tools` of the Novell SecureLogin 7.0 Windows installer package.

9.3 Extending the LDAP Directory Schema and Assigning Rights on the Server

Installing Novell SecureLogin on the server requires extending the LDAP schema and assigning user rights to record data against these attributes.

9.3.1 SecureLogin Attributes

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

Table 9-1 *Attributes*

Attribute To Be Mapped	LDAP Mapping
Prot:SSO Auth	
Prot:SSO Entry	protocom-SSO-Entries
Prot:SSO Entry Checksum	protocom-SSO-Entries-Checksum

Attribute To Be Mapped	LDAP Mapping
Prot:SSO Profile	protocom-SSO-Profile
Prot:SSO Security Prefs	protocom-SSO-Security-Prefs
Prot:SSO Security Prefs Checksum	protocom-SSO-Security-Prefs-Checksum

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

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.

If you intend to use Microsoft Group Policy (GPO) support, Novell recommends that you re-extend the SecureLogin directory schema extensions to include the new schema extensions for GPO support.

If the LDAP-compliant directory extension is deployed using the `ldapschema.exe` file copied from rather run from the Novell SecureLogin installer package, then you need to copy the entire LDAP folder containing the LDAP schema files to your preferred location.

9.3.2 Extending the Schema on the LDAP Server

1. Log in to the server as administrator.
2. Run `ldapschema.exe` found in the `\Securelogin\Tools\Schema\LDAP` directory of the Novell SecureLogin 7.0 Windows installer package. The Novell SecureLogin - Active Directory Schema dialog box is displayed.

   or

   Click *Schema Extension Tools* and click *LDAP Compliant*.
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 is displayed, click *Close*.

   NOTE: LDAP schema extension is replicated to all servers in the LDAP Group, and not to all servers in the tree. Schema extensions are LDAP group specific and must be repeated for each LDAP group. By default, each NetWare® server is in its own LDAP group, which means that by default `LDAPSchema.exe` must be run on every LDAP server.

9.3.3 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.

9.4 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.

9.5 Using LDAP in Non-eDirectory Environments

9.5.1 Configuring the Server

Retrieving the Certificate

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

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

For details on certificate service, refer to the 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 9-2 *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 62.

  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.

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

9.5.2 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

Deploying

10

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.

Use 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`.

10.1 Distribution Options

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

Table 10-1 *Distribution Options*

Options	Descriptions
Copy settings	Copies Novell SecureLogin configuration from one object in a directory to another object in the same directory.
Export and import	Uses an XML file to distribute the configuration.
Directory object inheritance	Inherits the configuration from a higher-level directory object, for example, a Group Policy.
Corporate configuration re-direction	Redirect configurations of a specified directory of a different group to the directory.

10.2 Configuring Anonymous Bind Setup for Active Directory 2003 and 2008

By default, anonymous LDAP operations are not permitted on Active Directory. This means that an attempt to perform anonymous search in Active Directory results in the server requesting authenticated connection to LDAP and refusing the query. Therefore, some additional configuration is required to make Active Directory allow anonymous queries.

This section consists of the following information:

Configuring anonymous bind setup consists of the following tasks:

1. Enabling Anonymous Login for 2003 Server.
2. Allowing Access to Anonymous Users.

10.2.1 Prerequisite

- Install `suptools.msi` found in the support folder of the Microsoft Windows 2003 Server installation CD. This installs the `adsiedit.msc` MMC snapin

10.2.2 Enabling Anonymous Login for 2003 Server

This section helps you understand how to enable anonymous login. You can configure this setup using any LDAP browser.

1. Launch the ADSI Edit tool.

   Click *Start* > *Run*, then type `adsiedit.msc`. The ADSI Edit tool is launched.
2. In the left panel, navigate to *CN=Configuration* > *CN=Services* > *CN=Windows NT*, right-click *CN=Directory Service*s container, then select *Properties*.

   The Directory Services Properties dialog box opens.
3. In the *Attribute Editor* tab, select *dsHeuristics*.
4. Click *Edit*. The String Attribute Editor opens.
5. If the value is blank, specify the value as 0000002.

   WARNING: If the attribute already contains a value, change only the seventh character from the left. This is the only character that must be changed to enable anonymous binds.

   For example, if the value is 0000001, change the number 1.

   ---
6. Click *OK* to save the changes and exit the String Attribute Editor and return to the Directory Services Properties dialog box.
7. Click *OK* to exit the Directory Services Properties and return to the ADSI Edit tool.

You have now successfully enabled anonymous login. The next task is Allowing Access to Anonymous Users.

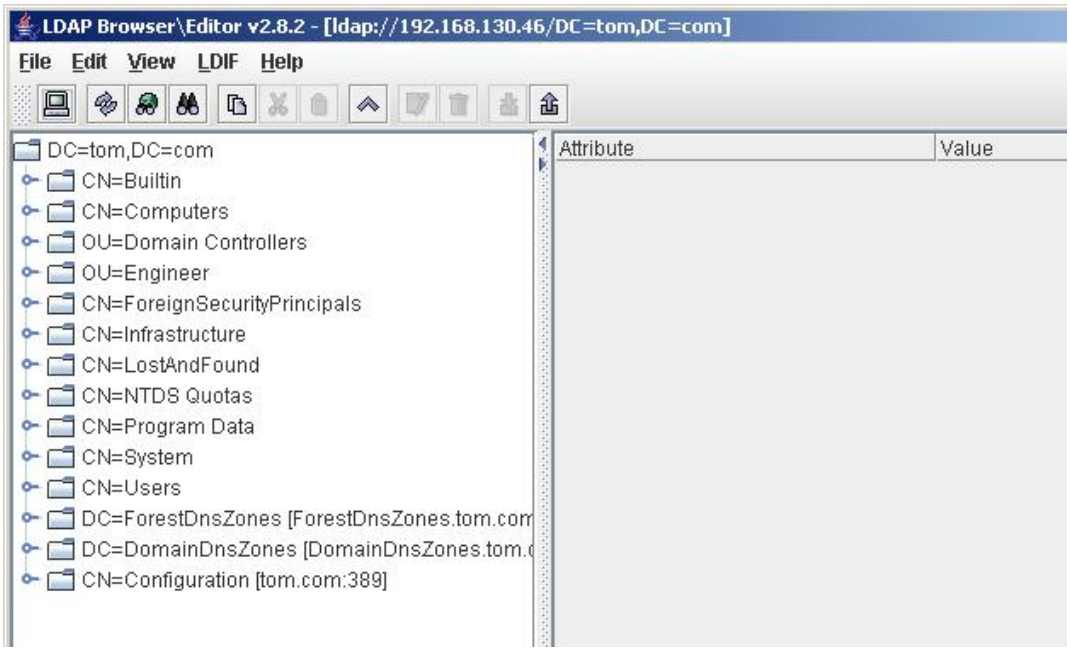
10.2.3 Allowing Access to Anonymous Users

1. Launch the ADSI Edit tool.
2. Expand the domain entry, then right-click on your domain and select *Properties*.
3. Select the *Security* tab, then click *Advanced*. The Advanced Security Setting dialog box opens.
4. Click *Add*. The Select User, Computer, or Group dialog box opens.
5. Click *Advanced* > *Find Now*, double-click *Anonymous Logon*, then click *OK*. The Permission Entry dialog box opens.
6. Click the *Objects* tab.
7. Set the *Apply onto* drop down list to *This object and all child objects*.
8. Select the *Allow* checkbox for the permission *List Contents*.
9. Click the *Permissions* tab .
10. Set the *Apply onto* drop down list to *This object and all child objects*.
11. Select *Allow* checkbox for both occurrences of the Read Name permission.
12. Set the permission as *Allow* for `Read ObjectClass`.
13. Click *OK*.

Testing if Anonymous Binding Is Allowed

1. Launch LDAP browser.
2. Connect to the LDAP server with the LDAP browser using anonymous settings.

   If you see a window similar to the following image, the anonymous binding is successful.



Testing in a Non-eDirectory LDAP Environment

1. Add a key in the registry HIVE.
2. Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP`.
3. Create a registry key of the STRING value.
4. Name the registry key as `CertFilePath`.
5. Specify the path to your certificate.

10.2.4 Troubleshooting

Adding Anonymous Logon to Admin account

Follow these instructions if you have trouble starting SecureLogin in LDAP Mode as an admin user.

1. Launch the ADSI Edit tool.
2. Right-click Administrator, then select *Properties*.
3. Click the Security tab, then click Advanced.
4. Select the *Allow inheritable permissions from the parent to propegate to this object and all child objects. Include these with entries explicity defined here* option.

Adding Rights to Enable Anonymous Login

If you need to add rights to enable anonymous login, do the following:

1. Launch the ADSI Edit tool.
2. Navigate to your domain.
3. Right-click the domain, then select *Properties*. The properties of the domain opens.
4. Click the Security tab.
5. Select the ANONYMOUS LOGON group.

   If the group does not exist, add the group. See Section 10.2.3, "Allowing Access to Anonymous Users," on page 67.
6. From *Permissions for ANONYMOUS LOGON*, allow Read access.
7. Click *Advanced*. The Advanced Security Settings dialog box opens.
8. Select ANONYMOUS LOGON.
9. Click Edit. The Permission Entry dialog box opens.
10. In the *Object* tab, set the value of *Apply to*, to *This object and all child objects*.
11. Click *OK* to return to the Advanced Security Settings dialog box.
12. Click *OK* to return to the domain properties dialog box
13. Click *OK* to return to the ADSI Edit tool.

10.3 Using the LDAPCE Utility to Encrypt LDAP Credentials

The `ldapce.exe` is a command-line utility used to encrypt the credentials of an authorised user who has rights to browse the LDAP directory tree. The utility encrypts the authorized LDAP user's distinguished name and password into a string which is then stored in the `LDAPContextlessSearchBindCreds` registry key file. An additional registry key, `LDAPAnonymousLoginsDisallowed`, must also be configured if using this method.

NOTE: The `ldapce.exe` utility is unsupported and is only available on request.It is not distributed with Novell SecureLogin package.

The syntax is:

```
ldapce.exe <user DN> <password> [output file]
```

Where,

- `<user DN>` is the the full distinguished name of the LDAP user.
- `<password>` is the password of the LDAP user.
- `[output file]` is the name of the output file to which the encrypted string is written. If this option is omitted, the string is displayed on the screen.

10.4 Logging in to LDAP Directory

1. Log in to the LDAP directory 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 7.0 for LDAP for the first time, then the *Context* and *Primary host* areas are blank.
- If you are upgrading to Novell SecureLogin 7.0 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. See Section 10.4.1, "Updating the System Registry," on page 69.

10.4.1 Updating the System Registry

Use ADM files to configure the operation of SecureLogin by setting registry key values on users' machines. The keys are located in the local machine hive of the registry. So, the CLASS MACHINE must be specified in your ADM files. The values that populate the *Advanced* tab of the SecureLogin dialog box are located at:

```
HKLM\Software\Protocom\SecureLogin\LDAP Settings
```

Use the following table to guide you in setting values displayed in the *Advance* tab of the SecureLogin dialog box.

Table 10-2 *Setting Values in the Advance Tab*

Value	Type	Default Value
AttributesToSearch	STRING	◆ name ◆ sn ◆ givenname ◆ cn ◆ uid ◆ samAccountname
Context1	STRING	CN=Users,DC=example, DC=com
Context2	STRING	
Context3	STRING	
Context4	STRING	
Context5	STRING	
PrimaryHost	DWORD	
PrimaryPort	DWORD	636
SecondaryHost	STRING	
SecondaryPort	DWORD	636
SSL Cert File	STRING	`C:\Program Files \Novell\SecureLogin \rootcert.der`
NonSecureLDAPPort	DWORD	389

The values that control SecureLogin's use of seamless pass-through are located at:

`HKLM\Software\Protocom\SecureLogin`

To set the values, refer the following table.

Table 10-3 *Setting Values for Seamless Pass-Through*

Key	Type	Default
LDAPIsSynched	DWORD	1
SyncDelay	DWORD	5
LDAPAnonymousLoginsDisallowed	DWORD	0
LDAPContextlessSearchBindCreds	STRING	

For example ADM scripts to set values for seamless pass-through, see

10.4.2 Novell SecureLogin LDAP settings

The following settings populate the Advanced section of the SecureLogin dialog box. To control the operation of SecureLogin in synchronized mode, see Section 10.4.3, “Novell SecureLogin LDAP Pass-Through Settings,” on page 75.

Specifying the LDAP Attributes

Specify the LDAP credential attributes to search.

Example: Attributes to search

```
POLICY !!AttributesToSearch
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
  EXPLAIN !!AttributesToSearchExplain
  PART !!AttributesToSearch EDITTEXT
    VALUENAME "AttributesToSearch"
    DEFAULT "name sn givenname cn uid samAccountname"
END PART
END POLICY

[strings]
AttributesToSearch="Attributes To Search"
AttributesToSearchExplain="List the attributes to use in your LDAP search.
Separate each attribute with a space."
```

Specifying LDAP Search Contexts

Specify the distinguished names of LDAP directory hierarchies to search for users. You can specify up to five contexts.

Example: LDAP contexts to search

```
POLICY !!Context1
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
  EXPLAIN !!ContextExplain
  PART !!Context1 EDITTEXT
    VALUENAME "Context1"
  DEFAULT "CN=Users,DC=example,DC=com"
  END PART
  END POLICY

POLICY !!Context2
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
```

```
  EXPLAIN !!ContextExplain
  PART !!Context2 EDITTEXT
    VALUENAME "Context2"
  END PART
END POLICY

POLICY !!Context3
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
  EXPLAIN !!ContextExplain
  PART !!Context3 EDITTEXT
    VALUENAME "Context3"
  END PART
END POLICY

POLICY !!Context4
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
  EXPLAIN !!ContextExplain
  PART !!Context4 EDITTEXT
    VALUENAME "Context4"
END PART
END POLICY

POLICY !!Context5
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
  EXPLAIN !!ContextExplain
  PART !!Context5 EDITTEXT
    VALUENAME "Context5"
  END PART
END POLICY

[strings]
Context1="Context 1"
Context2="Context 2"
Context3="Context 3"
Context4="Context 4"
Context5="Context 5"
ContextExplain="Enter the LDAP context to search within.
Eg: CN=users,DC=Test,DC=com"
```

Specifying the Primary Host

Specify the IP address, name of your LDAP server, or the name of your primary LDAP server. You can specify both a primary and a secondary LDAP server.

Example: Primary host

```
POLICY !!PrimaryHost
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
  EXPLAIN !!PrimaryHostExplain
  PART !!PrimaryHost EDITTEXT
    VALUENAME "PrimaryHost"
  END PART
END POLICY

[strings]
PrimaryHost="Primary Host"
PrimaryHostExplain="Enter the name or IP address of the primary LDAP server to
connect to."
```

Specifying the Primary Port

Specify the SSL port used by the LDAP server, or the name of your primary LDAP server. You can specify both a primary and a secondary LDAP server.

Example: Primary Port

```
POLICY !!PrimaryPort
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
  EXPLAIN !!PrimaryPortExplain
  PART !!PrimaryPort NUMERIC
    VALUENAME "PrimaryPort"
    MIN 1
    MAX 65535
    DEFAULT 636
  END PART
END POLICY

[strings]
PrimaryPort="Primary Port"
PrimaryPortExplain="Enter the port used to connect to the primary host."
```

Specifying the Secondary Host

Specify the name or IP address of a backup LDAP server to use if an attempt to connect to your primary LDAP server fails.

Example: Secondary Host

```
POLICY !!SecondaryHost
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
  EXPLAIN !!SecondaryHostExplain
  PART !!SecondaryHost EDITTEXT
    VALUENAME "SecondaryHost"
  END PART
END POLICY

[strings]
SecondaryHost="Secondary Host"
SecondaryHostExplain="Enter the name or IP address of the secondary or backup
LDAP server to connect to. This is used if an attempt to connect to the primary
host fails."
```

Specifying the Secondary Port

Specify the SSL port of a backup LDAP server to use if an attempt to connect to your primary LDAP server fails.

Example: Seconday Port

```
POLICY !!SecondaryPort
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
  EXPLAIN !!SecondaryPortExplain
  PART !!SecondaryPort NUMERIC
    VALUENAME "SecondaryPort"
    MIN 1
    MAX 65535
```

```
    DEFAULT 636
  END PART
END POLICY

[strings]
SecondaryPort="Secondary Port"
SecondaryPortExplain="Enter the port used to connect to the secondary host."
```

Specifying the SSL Certificate File

Specify the fully qualified path of the SSL certificate file used by LDAP.

Example: SSL Certificate File

```
POLICY !!SSLCertFile
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
  EXPLAIN !!SSLCertFileExplain
  PART !!SSLCertFile EDITTEXT
    VALUENAME "SSL Cert File"
    DEFAULT "C:\Program Files\Novell\SecureLogin\rootcert.der"
  END PART
END POLICY

[strings]
SSLCertFile="SSL Cert File"
SSLCertFileExplain="Enter the full path to the SSL certificate needed to
authenticate to the LDAP server."
```

Specifying the LDAP Non-Secure Port

Specify the non-secure port used by LDAP. SecureLogin assumes a default value of port 389 if a value is not specified.

Example: Non-secure Port

```
POLICY !!NonSecureLDAPPort
  KEYNAME "Software\Protocom\SecureLogin\LDAP Settings"
  EXPLAIN !!NonSecureLDAPPortExplain
  PART !!NonSecureLDAPPort NUMERIC
    VALUENAME "NonSecureLDAPPort"
    MIN 1
    MAX 65535
    DEFAULT 389
  END PART
END POLICY

[strings]
NonSecureLDAPPort="Non Secure LDAP Port"
NonSecureLDAPPortExplain="Enter the non-secure port number for your LDAP
server. Default is 389, but on some servers it may be different, eg, Sun ONE
Directory Server may use a port other than 389 such as 57433."
```

10.4.3 Novell SecureLogin LDAP Pass-Through Settings

The following settings control Novell SecureLogin use of seamless pass-through of credentials from Microsoft Active Directory (MS AD) to LDAP. To control the interaction of SecureLogin with LDAP, see Section 10.4.2, "Novell SecureLogin LDAP settings," on page 71.

Specifying Directory Synchronization

Specify whether the LDAP directory and MS AD are synchronized, and consequently whether SecureLogin must attempt to seamlessly pass users' MS AD credentials to LDAP.

Example: Directory Synchronization

```
POLICY !!LDAPIsSynched
  KEYNAME "Software\Protocom\SecureLogin"
  EXPLAIN !!LDAPIsSynchedExplain
  PART !!LDAPIsSynched NUMERIC
    VALUENAME "LDAPIsSynched"
    MIN 0
    MAX 1
    DEFAULT 1
  END PART
END POLICY

[strings]
LDAPIsSynched="LDAP Passthrough"
LDAPIsSynchedExplain="When this is set to 1 SecureLogin assumes that your
Active Directory login credentials and your LDAP directory credentials are
synchronized and an attempt is made to connect to your LDAP server silently. A
value of 0 disables this setting."
```

Specifying Directory Synchronization Delay

Specify the delay in seconds before SecureLogin attempts to connect to the LDAP directory again when a connection attempt has failed. The default value is five seconds.

Example: Directory Synchronization Delay

```
POLICY !!SyncDelay
  KEYNAME "Software\Protocom\SecureLogin"
  EXPLAIN !!SyncDelayExplain
  PART !!SyncDelay NUMERIC
    VALUENAME "SyncDelay"
    MIN 0
    MAX 36000
    DEFAULT 5
  END PART
END POLICY

[strings]
```

```
SyncDelay="LDAP Passthrough Login Retry Delay"
SyncDelayExplain="This setting sets the delay in seconds before retrying to
login to the LDAP directory in pass-through mode a second time. If a password
change has occurred in Active Directory, it may take some time to propagate to
the LDAP directory. This delay is provided to allow for this propagation
of the new Active Directory password to the LDAP directory, so the new password
can be used to authenticate to the LDAP directory. The default value is 5
seconds."
```

Disallowing LDAP Anonymous Binding

Specify that anonymous binding to the LDAP server is not allowed. If anonymous binding is not allowed, then the encrypted LDAP credentials used by SecureLogin search LDAP must be specified in `LDAPContextlessSearchBindCreds`.

For details, see "Specifying Contextless Search Binding Credentials" on page 76.

Example: Disallowing LDAP Anonymous Binding

```
POLICY !!LDAPAnonymousLoginsDisallowed
  KEYNAME "Software\Protocom\SecureLogin"
  EXPLAIN !!LDAPAnonymousLoginsDisallowedExplain
  PART !!LDAPAnonymousLoginsDisallowed NUMERIC
    VALUENAME "LDAPAnonymousLoginsDisallowed"
    MIN 0
    MAX 1
    DEFAULT 0
  END PART
END POLICY

[strings]
LDAPAnonymousLoginsDisallowed="LDAP Anonymous Logins Disallowed"
LDAPAnonymousLoginsDisallowedExplain="Some LDAP servers do not allow anonymous
binds. In this case a user name and password must be supplied in order for a
bind to be performed. Set this value to 1 if anonymous binds to the server are
not allowed. A value of 0 or absence of this registry key will cause
SecureLogin to default to using anonymous binding."
```

Specifying Contextless Search Binding Credentials

Specify the encrypted LDAP credentials used by SecureLogin and SecureLogin Manager to search LDAP.

To specify the credentials:

1. Set the `LDAPContextlessSearchBindCreds` value to the encrypted string generated by the `ldapce.exe` utility.

For details, see Section 10.3, "Using the LDAPCE Utility to Encrypt LDAP Credentials," on page 69.

Provide only the minimum permissions required to browse the directory tree to the account specified on user machines. The account specified in this key is also used by SecureLogin Manager, so the account specified on the administrator workstation must have suitable permissions.

Example: Contextless Search Binding Credentials

```
POLICY !!LDAPContextlessSearchBindCreds
  KEYNAME "Software\Protocom\SecureLogin"
  EXPLAIN !!LDAPContextlessSearchBindCredsExplain
  PART !!LDAPContextlessSearchBindCreds EDITTEXT
    VALUENAME "LDAPContextlessSearchBindCreds"
  END PART
END POLICY

[strings]
LDAPContextlessSearchBindCreds="LDAP Contextless Search Bind Credentials"
LDAPContextlessSearchBindCredsExplain="This value stores the encrypted LDAP
credentials which should be used when anonymous binding is not allowed. The
credentials should be encrypted with the command line tool ldapce.exe provided
with SecureLogin."
```

10.5 Contextless Login

If you configure Novell SecureLogin to use LDAP mode, a login 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 might find confusing.

Table 10-4 *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.

10.5.1 Using Contextless Login

For example, Henry Dubois' DN is cn=hdub, ou=rdev,o=vmp. Henry enters hdub in the login dialog box. The LDAP Authentication client finds and displays every user ID that contains hdub anywhere in the context. If multiple hdub IDs exist, the client lists all user IDs that contain hdub. Henri then selects the DN for his user ID and logs in.

If just one user ID qualifies, the LDAP authentication client is expected to authenticate using Henry's entire DN. However, Novell SecureLogin fails to find the user and automatically log in the user. An error indicating `Username entered is not found. Please check the username and try again. If the problem persists, contact your helpdesk or system administrator` is displayed.

To resolve,

1. Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP`
2. Create a registry key named LDAPSearch.
3. To the LDAPSearch key, add a multi-string of SearchAttributes.
4. Change the names of the SearchAttributes to,
   - name
   - sn
   - givenname
   - cn
   - uid
   - samAccountName

10.6 Setting Up Passphrase

After you have successfully installed Novell SecureLogin 7.0 on a user workstation, you can set up a passphrase for the user.

Refer Chapter 3, "Setting Up a Passphrase," on page 23 for detailed information on setting up a passphrase.

Installing and Configuring in Active Directory Environment

IV

This section provides information on installing, configuring, and deploying Novell® SecureLogin 7.0 in an Active Directory environment.

The examples in this section apply to Microsoft Windows 2003 and 2008 Active Directory environments with a directory server managed through an administrative workstation.

Before You Begin

11

The following procedures apply to the standard configuration of a server managed through an administration workstation. It also applies if your configuration does not separate the server from the administration workstation.

In Active Directory's MMC, the current datastore version (displayed in the Advanced Settings page) might not update immediately when the directory database version is changed. To update, click OK, then exit the MMC Properties dialog box.

11.1 Prerequisites

- A minimum of 128 MB is required in the Windows directory. An additional 55 MB is required for temporary files, which is deleted after installation is complete.
- You must have administrator-level access to the server and the administration workstations.
- Ensure that the LDAP certificate file is saved in the default certificate location of the LDAP log, for example, `securelogin\rootcert.der`.
- 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.

11.2 Requirements for Microsoft Windows Server 2003 and 2008

The following information applies to the configuration of a server in a Microsoft Windows Server* 2003 or Windows Server 2008 operating system environment.

11.2.1 Internet Explorer Enhanced Security

By default, Microsoft Windows Server 2003 and 2008 install 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.

If you are using Internet Explorer, some Web sites might not display or perform as expected when Novell SecureLogin is installed. Add-ons and Browser Help Objects (BHOs) such as single sign-on might not be fully functional.

For more information on enhanced security, see the Microsoft Support Web site (http://support.microsoft.com/kb/815141) for knowledge base article 815141 (http://support.microsoft.com/kb/815141/en-us).

11.2.2 Enabling Single Sign-On for Internet Explorer

To enable single sign-on for Internet Explorer, disable the Microsoft's Internet Explorer Enhanced Security Configuration before deploying Novell SecureLogin.

You can do this by:

- "Enabling Web Browser Extensions" on page 82
- "Enabling Browser Help Objects in Internet Explorer" on page 82

Enabling Web Browser Extensions

- **On both Windows Server 2003 and 2008:** Go to *Internet Options* > *Advanced* > *Browsing*, then select the *Enable Third party web browser extension (requires restart)* option.
- **On Windows Server 2003:** Go to *Start* > *Control Panel* > *Add/Remove Windows Component*.
- **On Windows Server 2008:** Go to *Start* > *Service Manager*, *Security Manager* > *Configure IE ESC*.

Enabling Browser Help Objects in Internet Explorer

- **In Internet Explorer 8:** Open Internet Explorer, go to *Tools* > *Internet Options* > *Advanced* > under *Browsing* section, select *Enable third party web browser extensions* option.

  After SecureLogin is installed, open Internet Explorer, go to *Tools* > *Manage Add-ons* > *Tools and Extensions* and check if the `IESSOObj Class` entry is displayed as *Enabled*.
- **In Internet Explorer 7:** Lauch Internet Explorer, go to *Tools* > *Internet Options* > *Advanced* > under *Browsing* section select *Enable third party web browser extensions (requires restart)* option.

  After SecureLogin is installed, open Internet Explorer, go to *Tools* > *Manage Add-ons* > *Enable or Disable Add-ons* and check if the `IESSOObj Class` entry is displayed as *Enabled*.
- **In Internet Explorer 6:** Lauch Internet Explorer, go to *Tools* > *Internet Options* > *Advanced* > under *Browsing* section select *Enable third party web browser extensions (requires restart)* option.

  After SecureLogin is installed, open Internet Explorer, go to *Tools* > *Manage Add-ons* and from the Add-ons currently loaded in Internet Explorer, check if the `IESSOObj Class` entry is displayed as *Enabled*.

11.3 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.

11.4 Installation Overview

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 versions prior to 6.0.
4. If the application type is enabled for single sign-on, 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 7.0 on the administration workstation.

   On Microsoft Windows Vista, write access requires administrator privileges.
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. Install the Novell SecureLogin application on user workstations.

Secure Workstation is not supported in an 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.

11.5 Microsoft Active Directory

11.5.1 Novell SecureLogin on Windows

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.

11.5.2 LDAP Environment

Novell SecureLogin supports Microsoft Active Directory operating in an LDAP environment. 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. For details, see Section 9.3, "Extending the LDAP Directory Schema and Assigning Rights on the Server," on page 59

11.5.3 ADAM

Novell SecureLogin supports deployment in an ADAM instance. For more information, see Part V, “Configuring, Installing, and Deploying In Active Directory Application Environment,” on page 101.

Configuring

12

Novell® SecureLogin uses the directory structure and administration tools to provide centralized management and deployment of users. In the Active Directory environment, Novell SecureLogin installs an additional tab to the Active Directory Users and Computers User Properties dialog box. This dialog box provides administrative functionality in the same utility you currently use to manage your Active Directory users.

Before you install Novell® SecureLogin, you must first extend the eDirectory™ schema. You can also configure the user's environment or create roaming profiles.

12.1 Extending the Active Directory Schema and Assigning Rights

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 access objects, including group policy, organizational units, and containers. Authorizing read or write rights to the Novell SecureLogin directory schema attributes is referred to as *assigning user rights.*

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 such as 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.

12.1.1 Extending the Schema

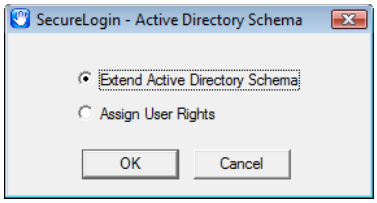
The following instructions apply to the configuration of the Microsoft Active Directory instance stored and administered on a separate server from the Active Directory server domain controller.

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*.

   The following Novell SecureLogin attributes 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

   A confirmation message is displayed.

   IMPORTANT: 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.

   ---

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

   Now that directory schema is extended, you must assign access rights to the relevant containers and organizational units.

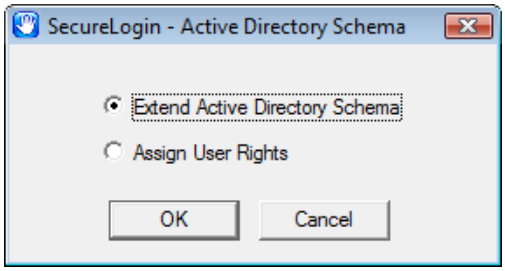
   If you have previosuly extended the schema, a message listing the existing schema appears. Ignore this message.
6. Click *OK* in the Active Directory Schema dialog box.
7. Continue with Section 12.1.2, “Assigning User Rights,” on page 87 to assign user access rights to the relevant containers and organizational units.

12.1.2 Assigning User Rights

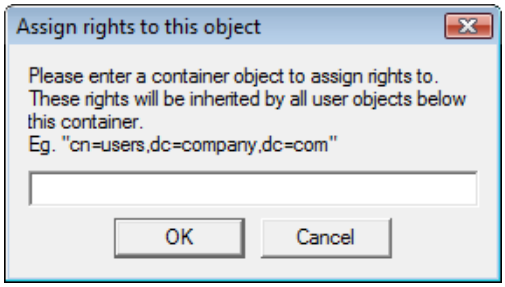
You must assign permission to objects in the directory to store data against the new Novell SecureLogin schema attributes. You assign rights to all objects that access Novell SecureLogin, including user objects, containers, group policies, and organizational units.

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`, which is found in the `Securelogin\Tools\Schema\ADS` directory.



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



For example, if you assign rights to Users container, the User container definition is:

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

To assign rights to an organizational unit, such as 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 Step 2 to Step 4 to assign rights to all required user objects, containers and organizational units.

If you see an error message indicating `Error opening specified object: - 2147016661`, it means that rights have already been assigned to the object.

If you see an error message indicating `Error opening specified object: -214716656`, it means that you have attempted to assign rights to an object that does not exist in the 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.*

NOTE: You can extend rights to objects at any time after the schema is extended. If you add organizational units, 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.

12.1.3 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.

12.2 Configuring a User's Environment

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

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).

Configure Novell SecureLogin on a test user account before installing SecureLogin on user workstations.

The following table shows the options available for deploying and distributing the user configuration. For information on deploying and distributing configuration, see "Distributing Configurations" in the *Novell SecureLogin Administration Guide*.

Table 12-1 *Deployment and Distribution Options*

User Configuration Options	Description
Copy Settings	Copies the 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.

User Configuration Options	Description
Corporate Configuration redirection	Specifies a directory object from which the configuration is inherited.

12.3 Configuring Roaming Profiles

Enterprises often create roaming profiles for specific groups of users, defined by their organizational role or function, such as field engineers connecting from remote locations or accounting staff working at different locations. For these users, you can create a roaming profile and set the path to the target user's profile.

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

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

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

Installing

13

After you have extended the Active Directory schema as described in Section 12.1.1, “Extending the Schema,” on page 86 and assigned permissions to the required directory objects as described in Section 12.1.2, “Assigning User Rights,” on page 87, you can install the Novell SecureLogin application on the administration and user workstations.

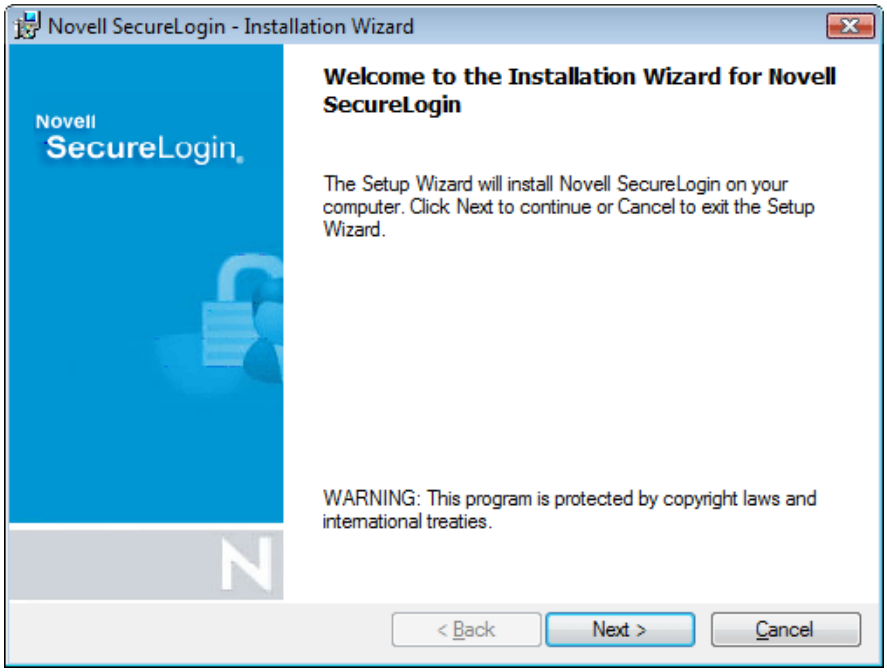
- Section 13.1, “Installing on Administrator Workstations,” on page 91
- Section 13.2, “Installing on a User Workstation,” on page 98
- Section 13.3, “Installing for Mobile Users and Notebook Users,” on page 98

13.1 Installing on Administrator Workstations

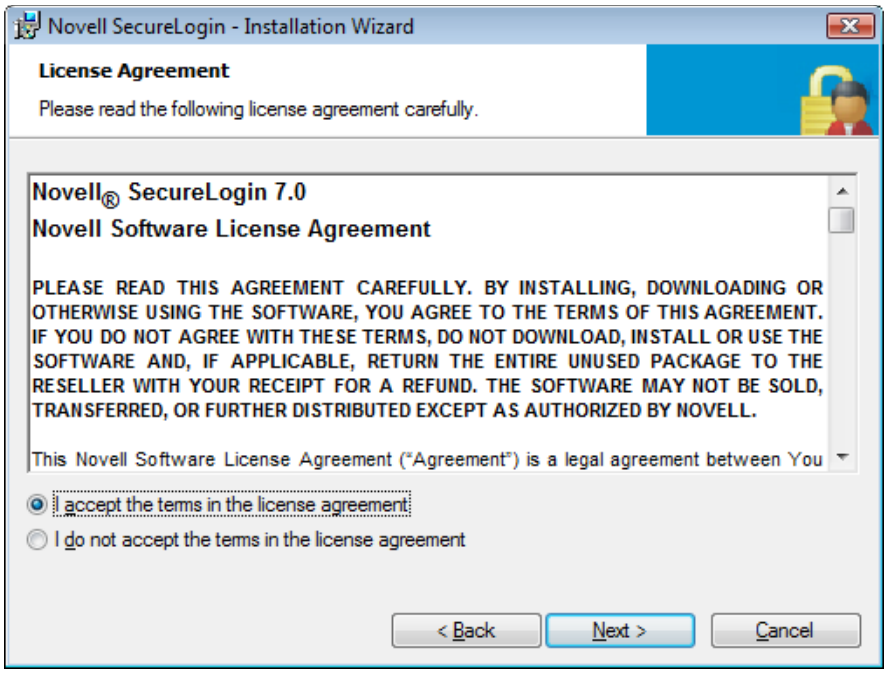
NOTE: The procedures for installing on administrator workstations and user workstations are the same.

The following procedureuses the Microsoft Windows Vista 64-bit installer.

1. Log in to the workstation as an administrator.
2. Double-click the `Novell SecureLogin.msi` that is available in `SecureLogin\Client\x64` directory of the installer package. The Welcome to the Installation Wizard for Novell SecureLogin is displayed.



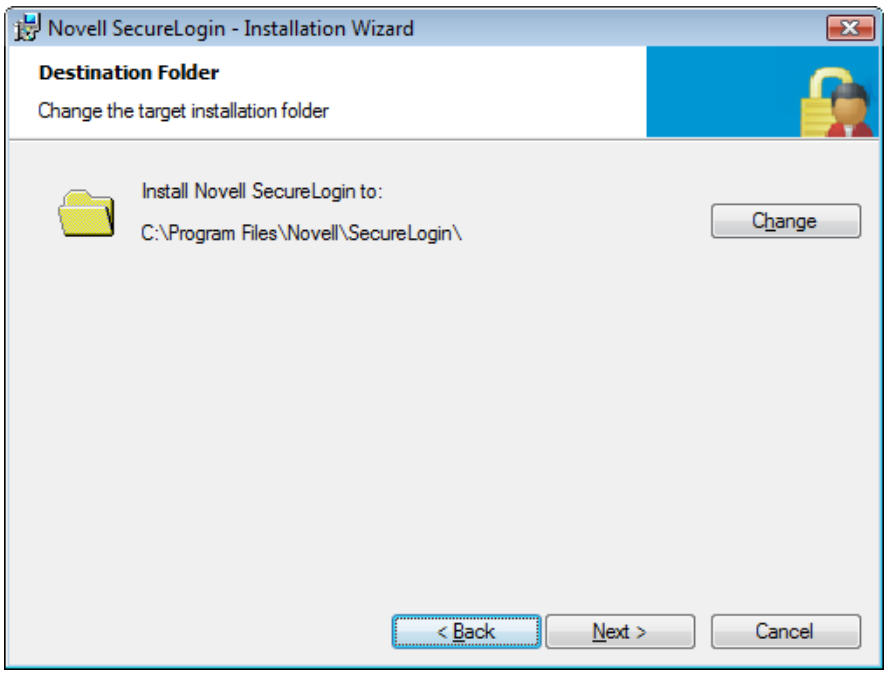
3. Click *Next*. The License agreement page is displayed.



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

5 Click *Next*. The destination folder is displayed.

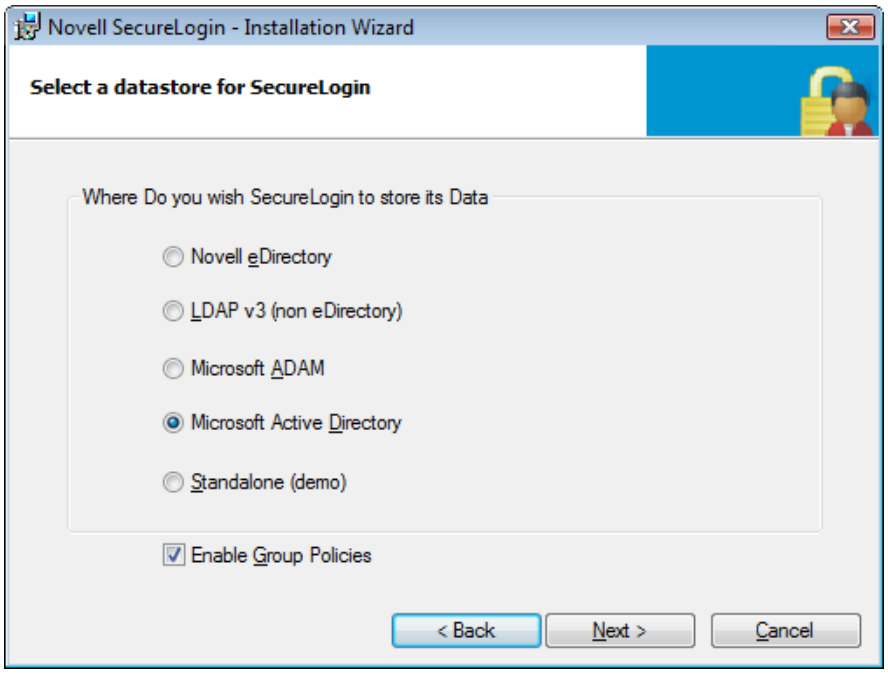
The default location for Novell SecureLogin is, `..\Program Files\SecureLogin\`. If you want to change the location, click *Change* and select an alternative location for Novell SecureLogin on the drive.



6 Click *Next*. The Select a datastore for SecureLogin (that is, the installation environment) page is displayed.

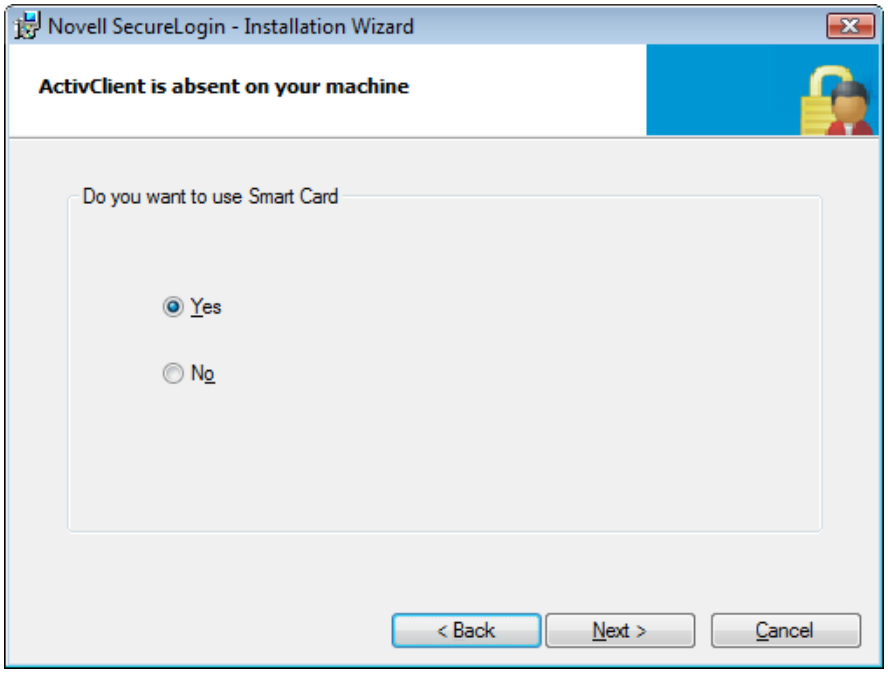
7 Select *Microsoft Active Directory*

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



8 (Optional) Select *Enable Group Policies*.

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



The ActivIdentity* ActivClient card settings are used if they are detected.

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 through Public Key Infrastructure (PKI) tokens.

10 (Conditional) If you want to use a smart card, select *Yes* >, click *Next*, then continue with Step 12.

IMPORTANT: If your enterprise policy allows users log in to the workstation by using a smart card, you must select the smart card option

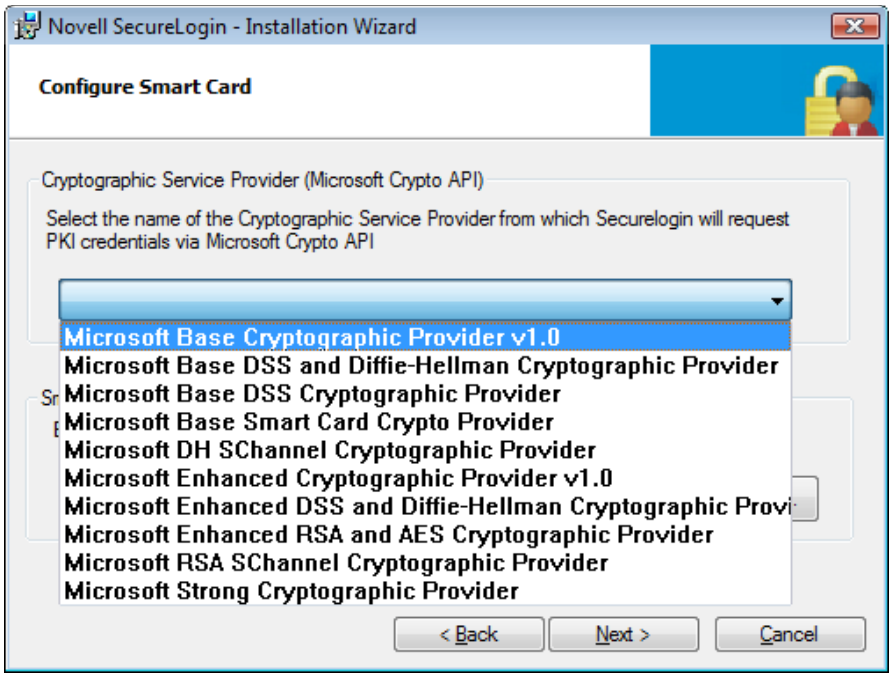
---

11 (Conditional) If you do not want to use a smart card, select *No* > , click *Next*, then continue with Step 15.

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

13 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 Novell 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.

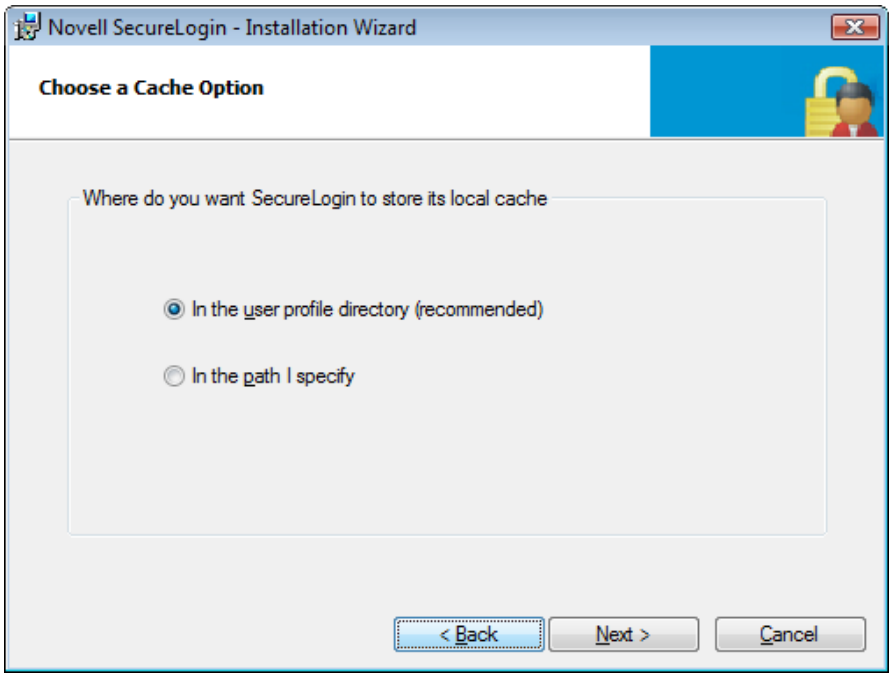
14 Select the features that you want to install, then click *Next*.

Select the options you want to install.

Secure Workstation is not available in Active Directory environment.

15 Select the location where you want Novell SecureLogin to store the local cache.

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



17 (Optional) If you want to change the location of the cache folder, select *In the path I specify* and specify an alternative folder.

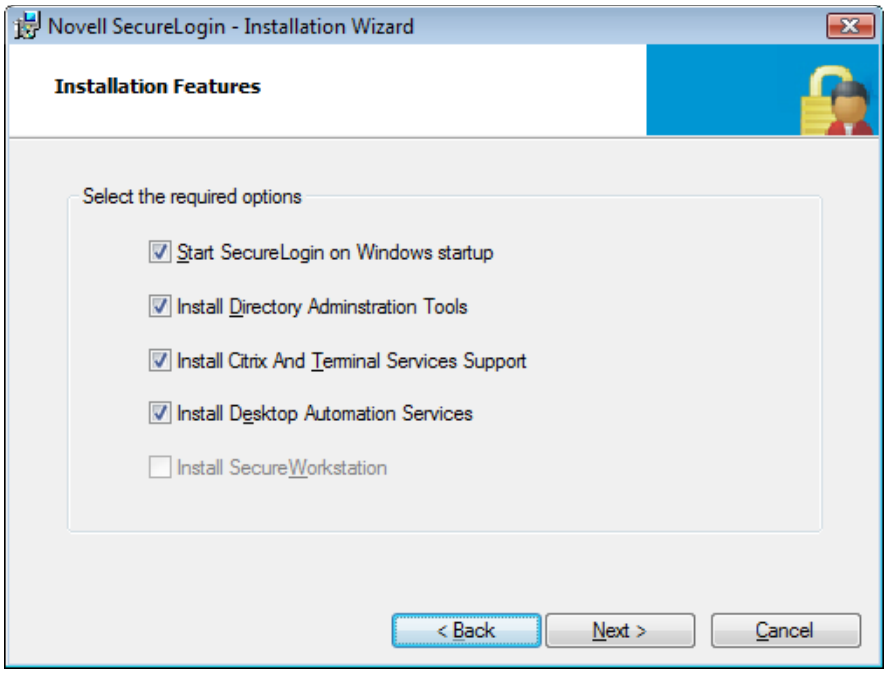
IMPORTANT: If you selected *Enable Group Policies* option in Step 6, you must create or locate a unique custom folder for every user of the workstation. Include a user-specific variable such as `%USERNAME%` in the directory path

---

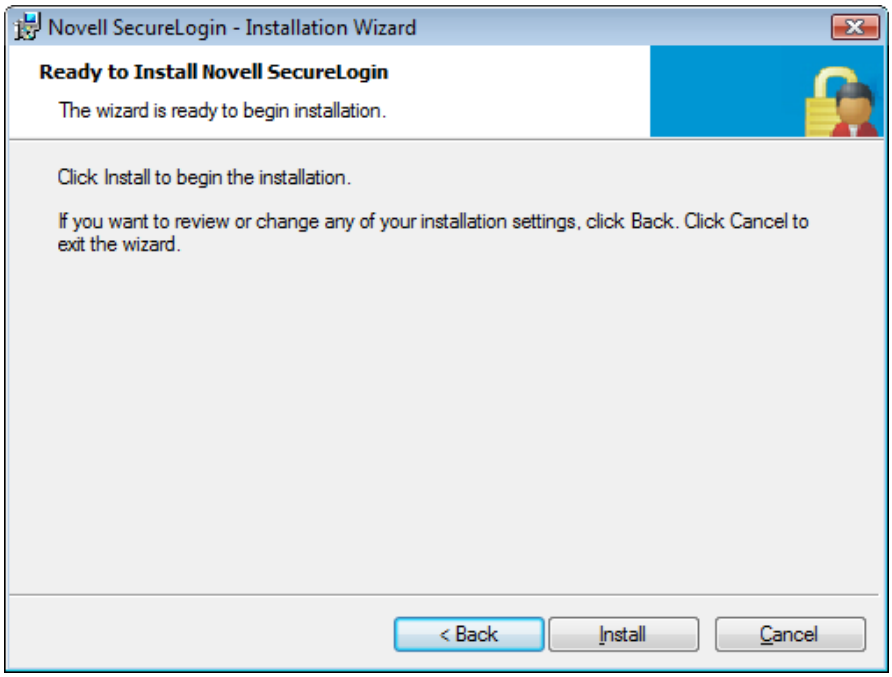
18 Click *Next*. The installation features page is displayed.

Select the options you want to install.

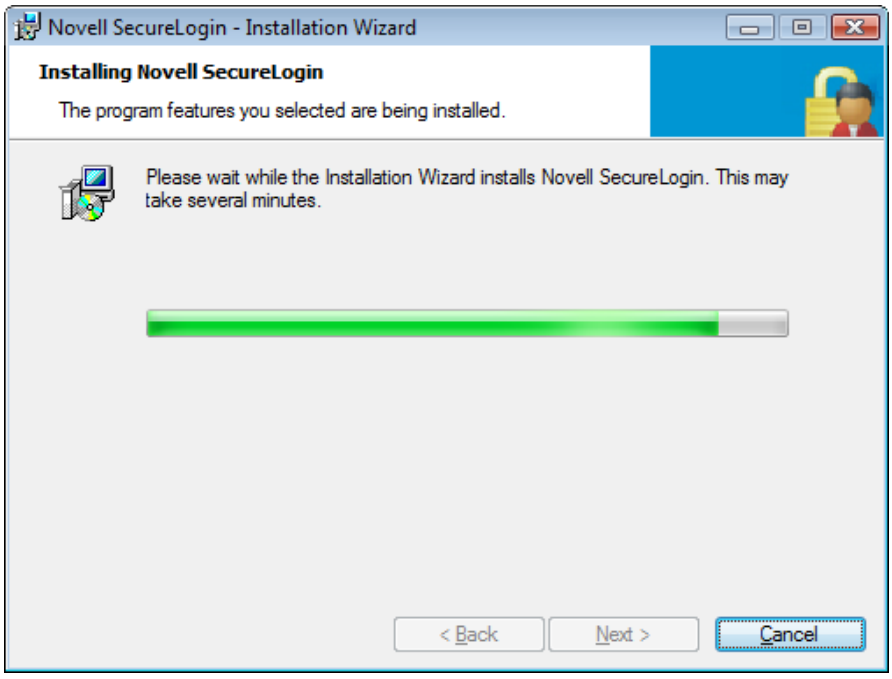
Secure Workstation is not available in Active Directory environment.



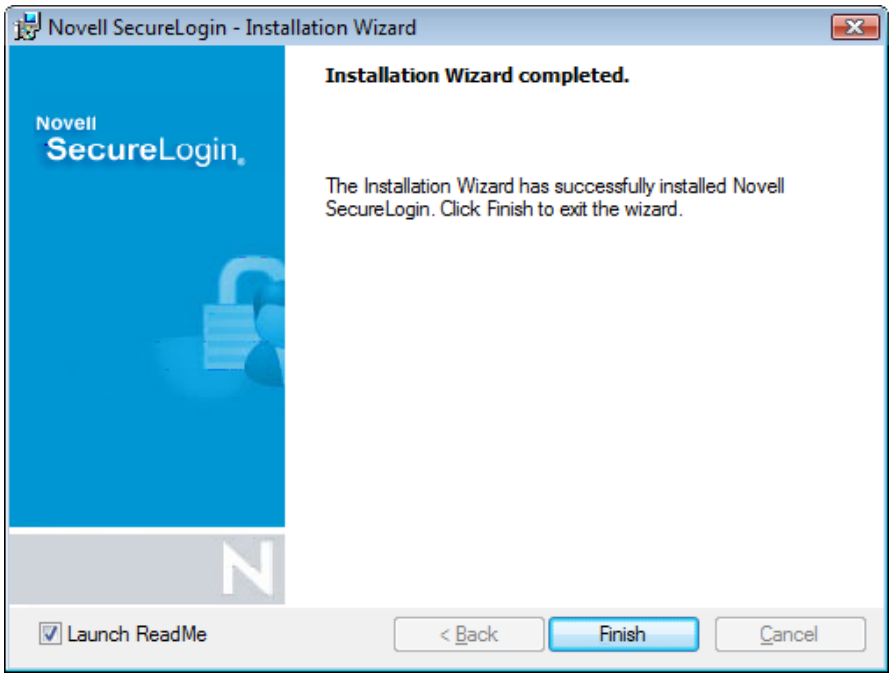
19 Click *Next*. The Ready to Install the Program page is displayed.



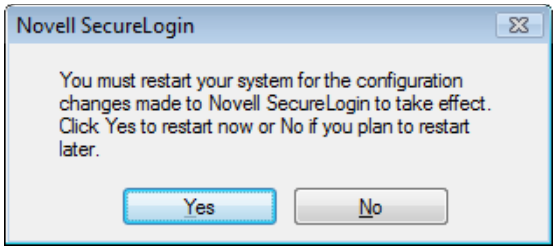
20 Click *Install*. The installation process takes a few minutes.



21 Click *Finish*.



22 You are prompted to restart your system. Select *Yes*.



13.2 Installing on a User Workstation

Installing Novell SecureLogin on user workstations uses the same procedure asChapter 13, “Installing,” on page 91. 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.

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

13.3 Installing for Mobile Users and Notebook Users

Installing Novell SecureLogin for mobile and remote users uses the same procedure as

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

Deploying

14

After you have successfully installed Novell SecureLogin 7.0 on a user workstation, you can set up a passphrase for the user.

Refer to Chapter 3, “Setting Up a Passphrase,” on page 23 for detailed information on setting up a passphrase.

Configuring, Installing, and Deploying In Active Directory Application Environment

V

This section provides information on configuring, installing, and deploying Novell SecureLogin 7.0 in Active Directory Application Environment (ADAM).

The instructions and examples provided in this section apply to Microsoft Windows 2003 Active Directory* environments with a directory server managed through an administration workstation.

Before You Begin

15

This chapter explains issues to consider before installing Novell SecureLogin 7.0 in ADAM environment.

Novell SecureLogin supports deployment in an ADAM instance. Active Directory is responsible for the network authentication while ADAM stores and provides Novell SecureLogin configuration data, settings, policies, and application definition. For example, if a user logs in to the network and authenticates successfully to Active Directory, the user can then access ADAM for the user's single sign-on data.

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

15.1 Prerequisites

- Ensure that the Microsoft redistributable components are installed.

  Novell SecureLogin requires Microsoft* Windows Installer 3.0 or later. Depending on the operating system and the level of patches and service packs applied to it, download the redistributables from the Microsoft Download Web site. (http://www.microsoft.com/downloads/details.aspx?familyid=889482fc-5f56-4a38-b838-de776fd4138c&displaylang=en).

  Microsoft Windows Installer 4.5 is available as a redistributable system component for Microsoft Windows Server 2003 SP2, Microsoft Windows Vista, Microsoft Windows Vista SP1, and Windows Server 2008 (64-bit). You can download these from the Microsoft Download Web site. (http://www.microsoft.com/downloads/details.aspx?FamilyId=5A58B56F-60B6-4412-95B9-54D056D6F9F4&displaylang=en).

- Download and save the ADAM application.

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

- Assign permissions to a network service account.
- Create an ADAM instance.
- Back up the existing Active Directory server.
- 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.

15.2 Language Support

Support for Novell SecureLogin deployed in ADAM mode is provided in English only.

15.3 Supported Platforms

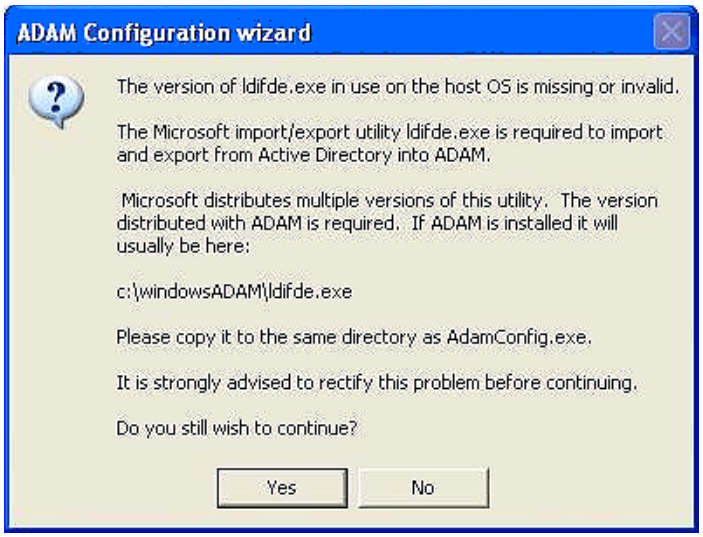
- Microsoft Windows Vista (32-bit and 64-bit) and Vista SP1 (32-bit and 64-bit)
- Microsoft Windows XP SP2 and SP3

15.4 ADAMconfig.exe and LDIFDE.exe

`ADAMconfig.exe` relies on Microsoft's LDAP Data Interchange Format Directory Extension (`ldifde.exe`) to run properly. However Microsoft distributes two versions of this file, one for Active Directory and another for ADAM. Only the version distributed with an ADAM installation is suitable for use with `ADAMconfig.exe`. You must be located in the same folder as `ADAMconfig.exe` unless you have edited the default system path.

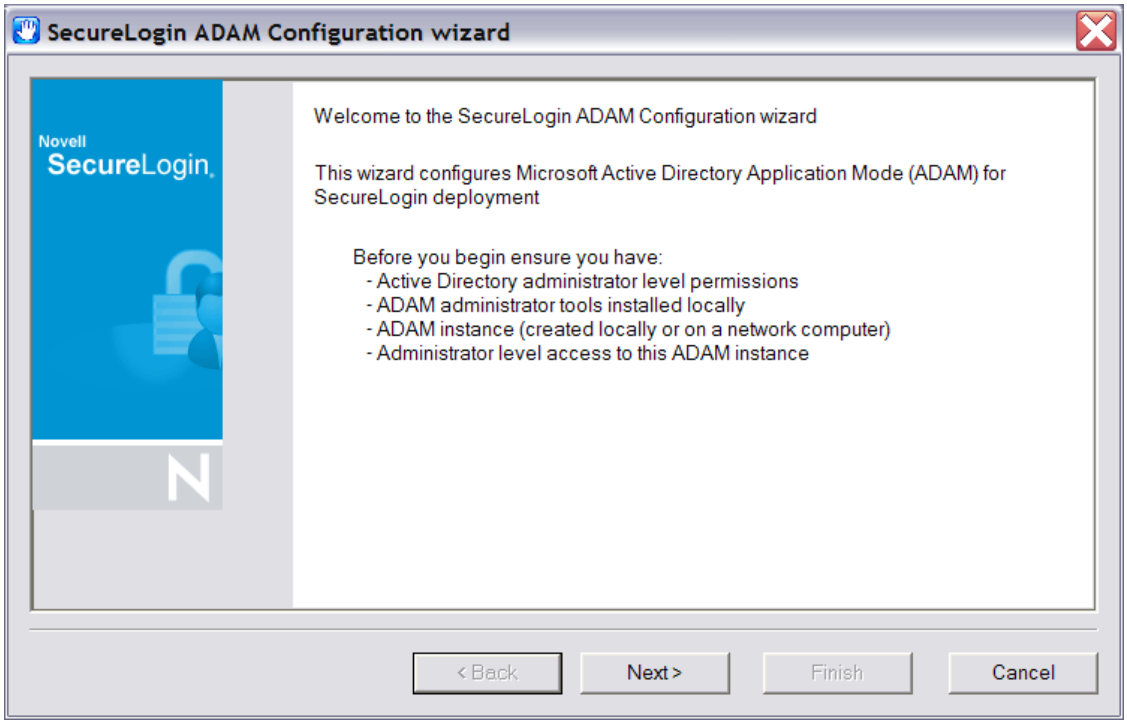
During the install process, Novell SecureLogin checks for `ldifde.exe` file. If the required version is not found, the following warning is displayed.

Figure 15-1 *Warning message*



If the correct version of ldifde.exe is installed in a customized file path, click Yes to continue. Otherwise, click *No*. It launches the ADAM configuration wizard.

Figure 15-2 *ADAM Configuration Wizard*



Configuring

16

The instructions provided in this section apply to the configuration of the ADAM instance stored and administered on a separate server from the Active Directory server domain controller. Follow the same instructions even if your configuration does not separate the Active Directory server and the ADAM instance server.

Active Directory and ADAM

Novell SecureLogin supports deployment in an ADAM instance. Active Directory is responsible for network authentication, while ADAM is responsible for storing and providing the SecureLogin configuration data, setting, policies, and application definitions. For example, if a user logs in to the network and authenticates successfully to Active Directory, the user can then access ADAM for the user's single sign-on data.

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

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

Also read the ADAM release notes from the ADAM Service Pack 1 available at the Microsoft Knowledge Base article KB902838. (http://support.microsoft.com/kb/902838)

Following are the tasks involved in configuring Novell SecureLogin in an ADAM environment:

16.1 Creating a Network Service Account and Assigning Permissions

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

Creating a Network Service Account enables the ADAM instance. To create a Network Service Account:

1. Click *Start* > *All Programs* > *Administrative Tools* > *Active Directory Users and Computers*. 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.

16.2 Configuring 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.

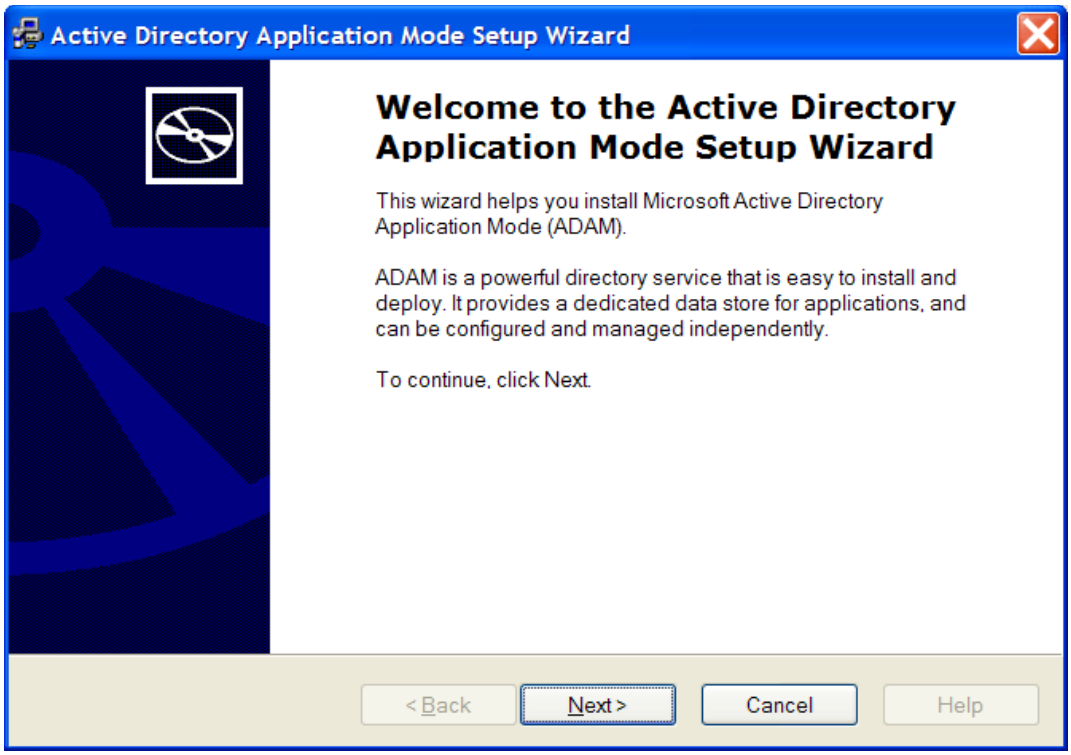
Following are the attributes added to the schema:

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

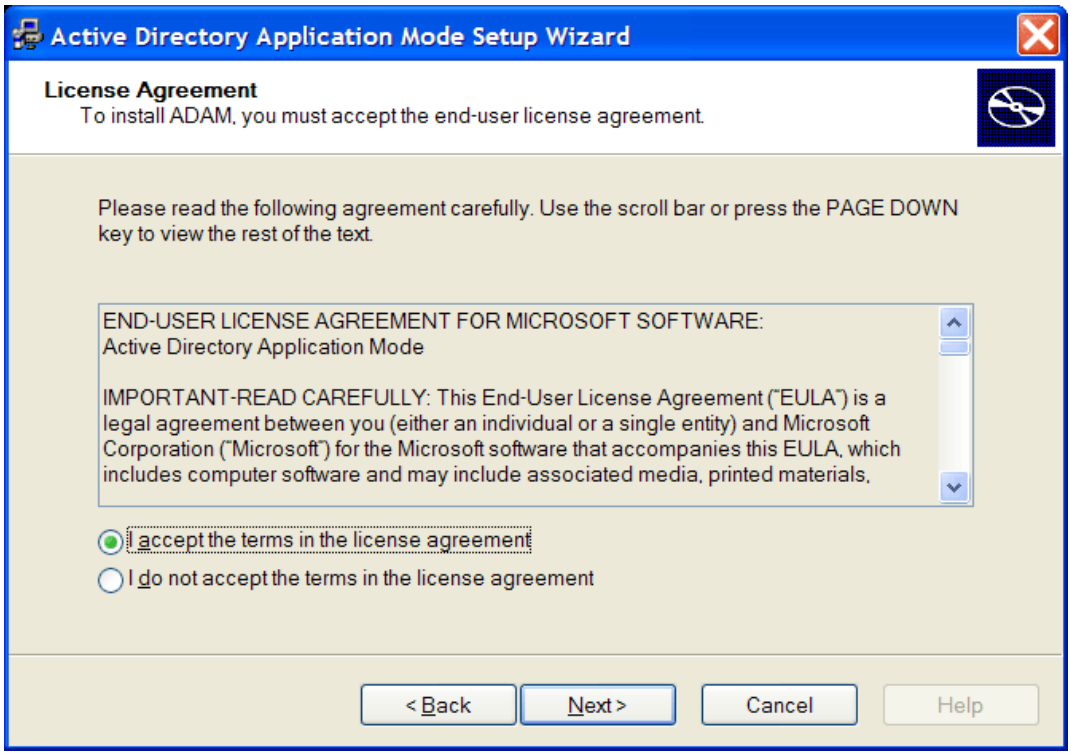
16.3 Creating an ADAM Instance

1 Browse to the ADAM set up file that you downloaded from the Microsoft Web site.

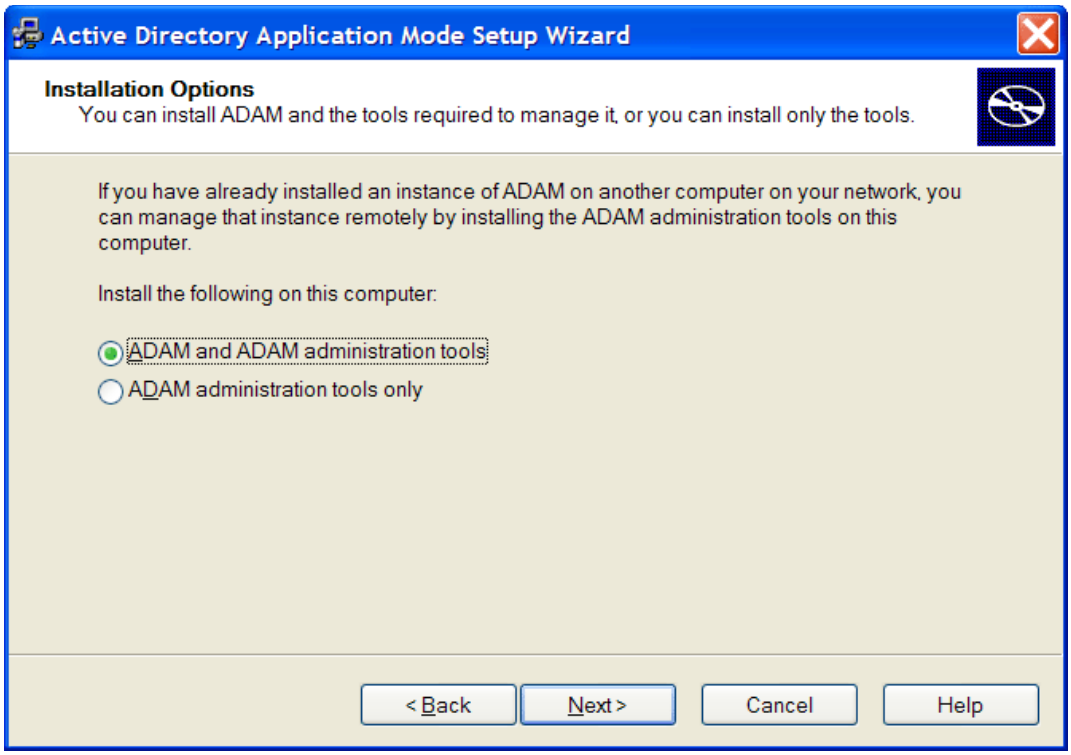
2 Double-click to run the `ADAMredistX86.exe` file. The Active Directory Application Environment Setup Wizard is displayed.



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

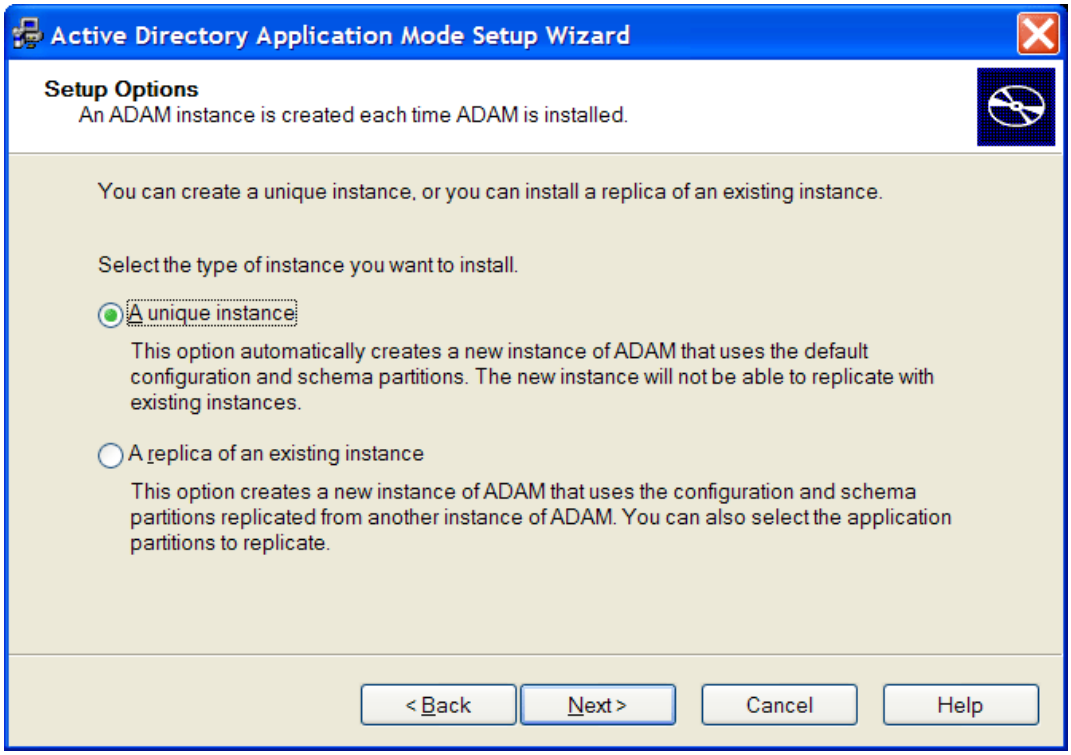


4 Accept the license agreement, then click *Next*. The Installation Options dialog box is displayed.



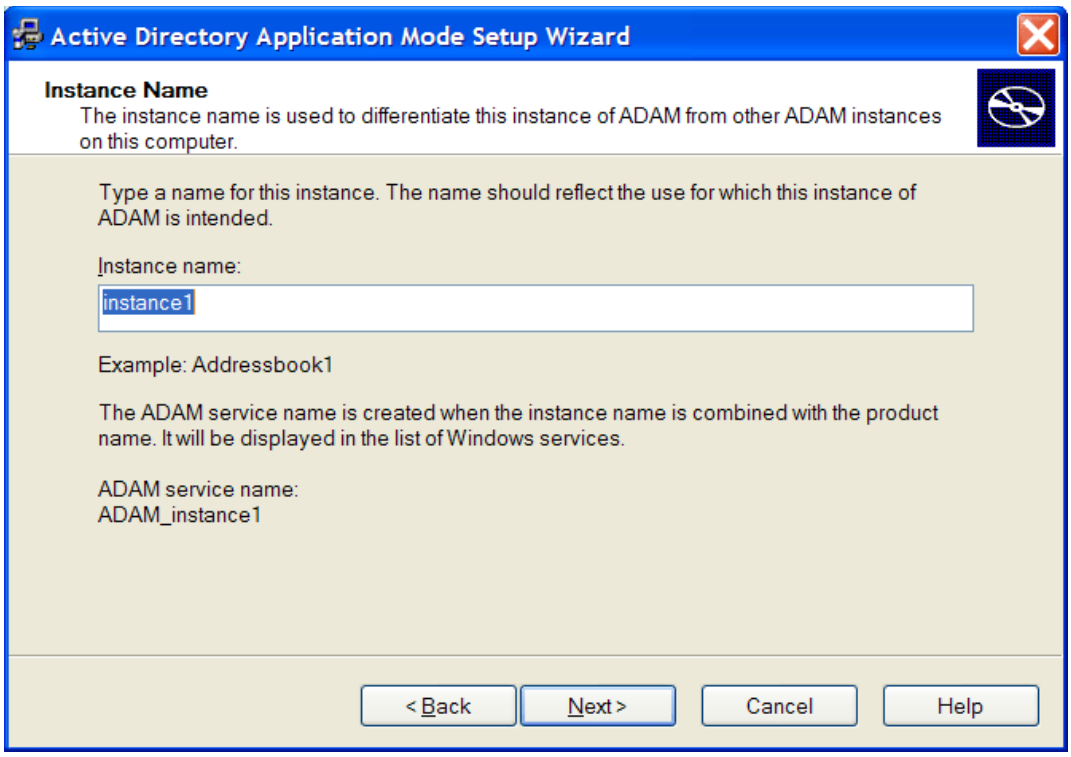
5 Select the *ADAM and ADAM administration tools* option.

6 Click *Next*. The Setup Options dialog is displayed.

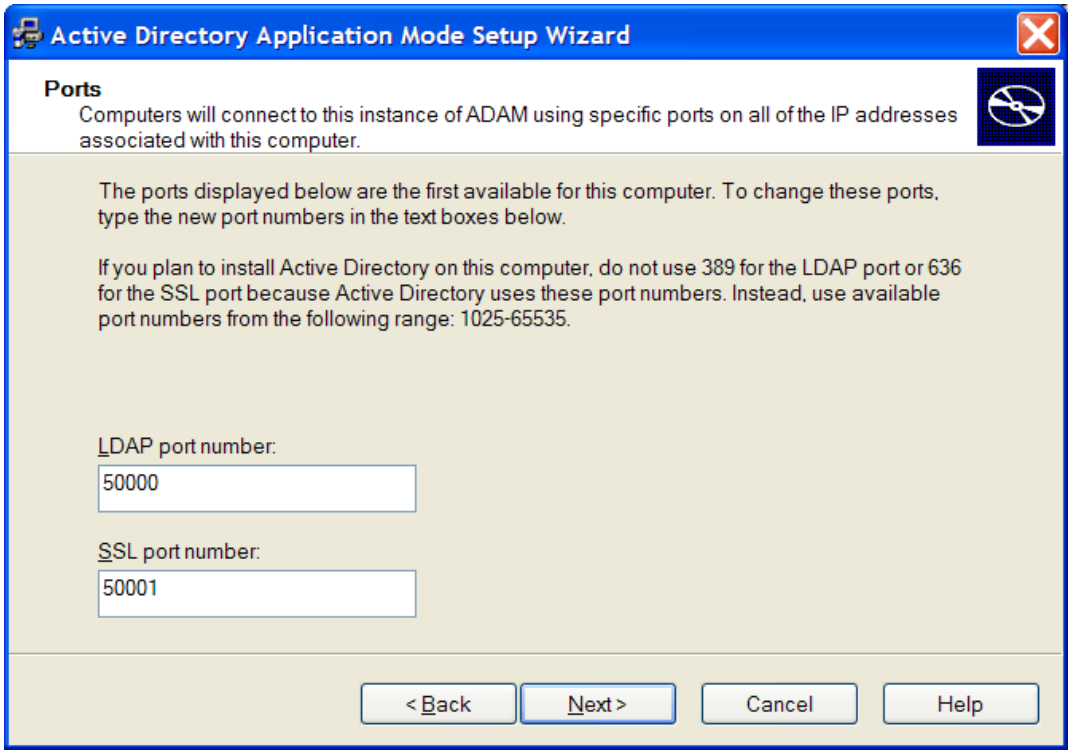


7 Select *A unique instance*. The Instance Name page is displayed.

8 In the *Instance name* field, specify a name for the ADAM instance.



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



10 In the *LDAP port number* field, specify the ADAM instance port number.

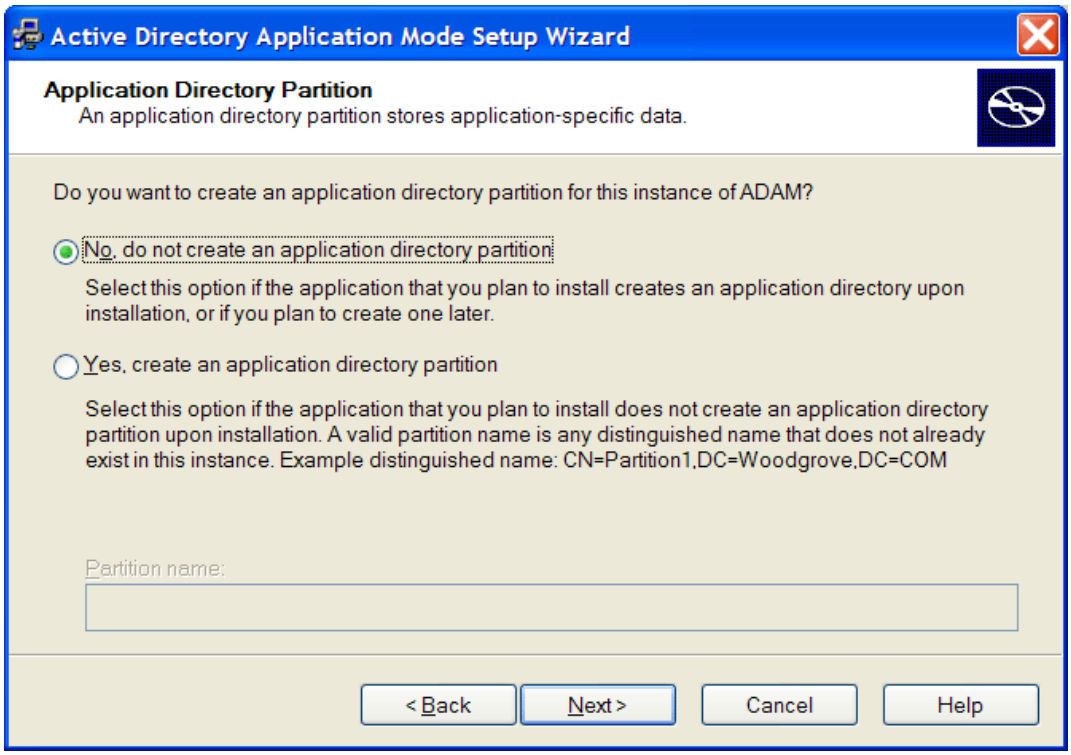
In the SSL port number, specify the ADAM instance SSL port number.

NOTE: The default LDAP port number is 50000 and the SLL port number is 50001. However if Active Directory is not installed on your workstation, the default LDAP port number is 389. The default SSL port number is, 636.

We recommend the default values. However if required, the values can be manually changed.

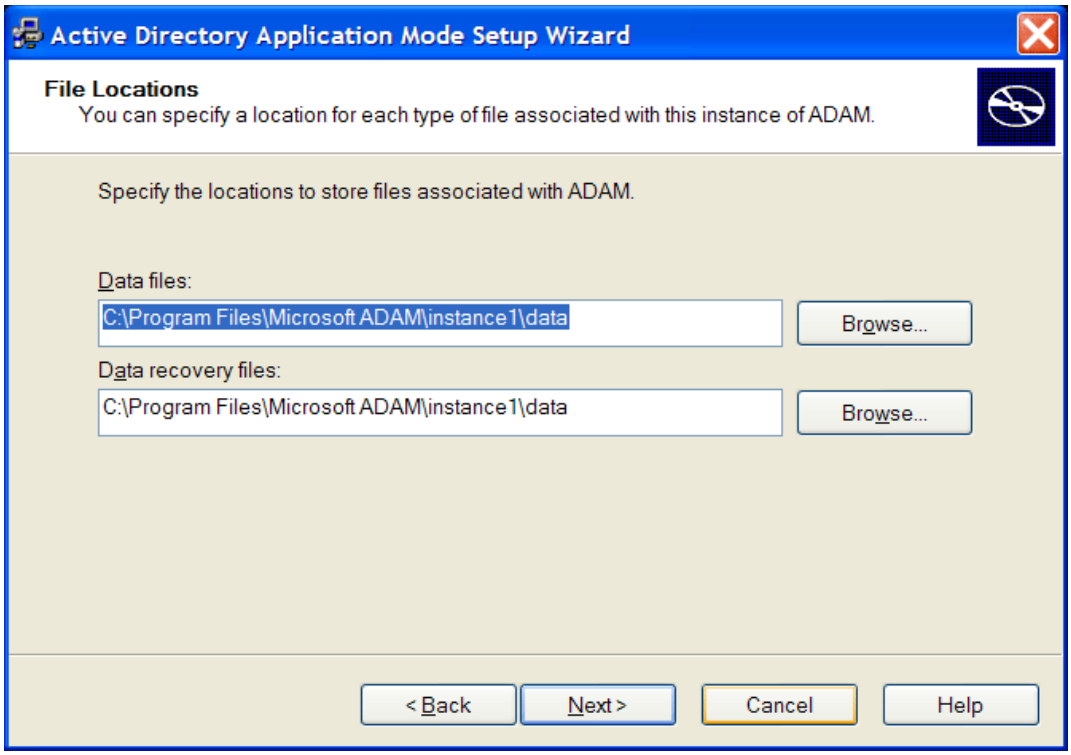
IMPORTANT: Ensure to make a note of the LDAP port number and the SSL port number because this information is required for further configuration.

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



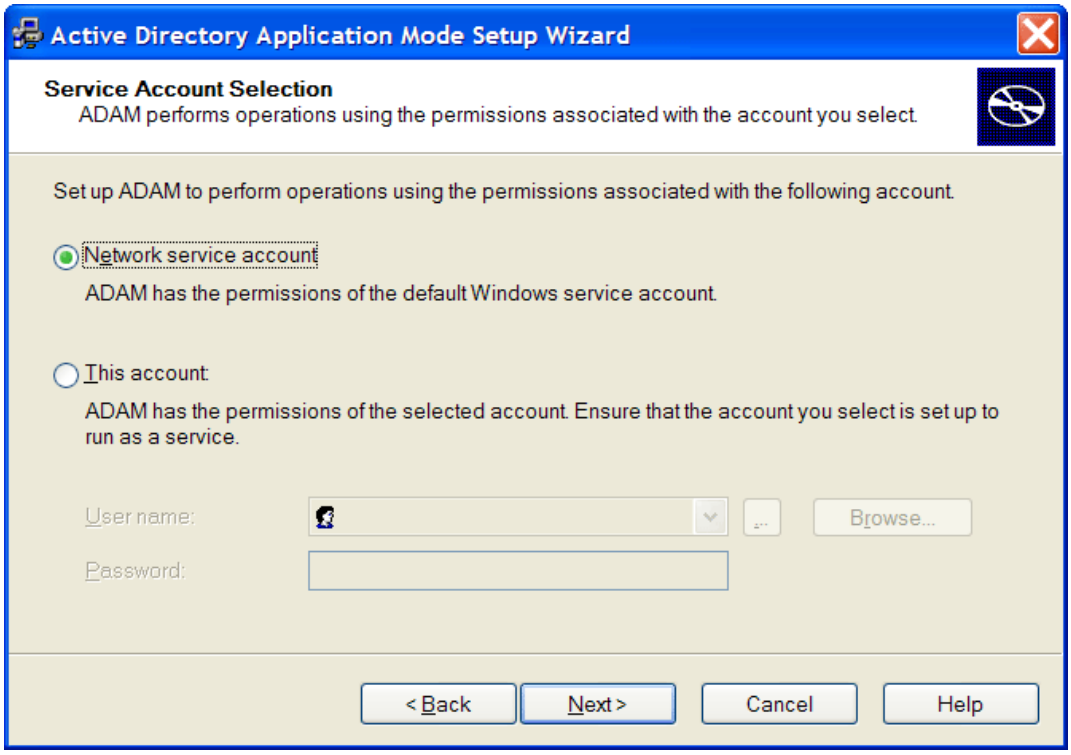
12 Select *No, do not create an application directory partition*.

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



14 Accept the default locations for ADAM files in the *Data files* and *Data recovery files* fields or click *Browse* to select an alternate location.

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



16 Select the *Network service account*.

or

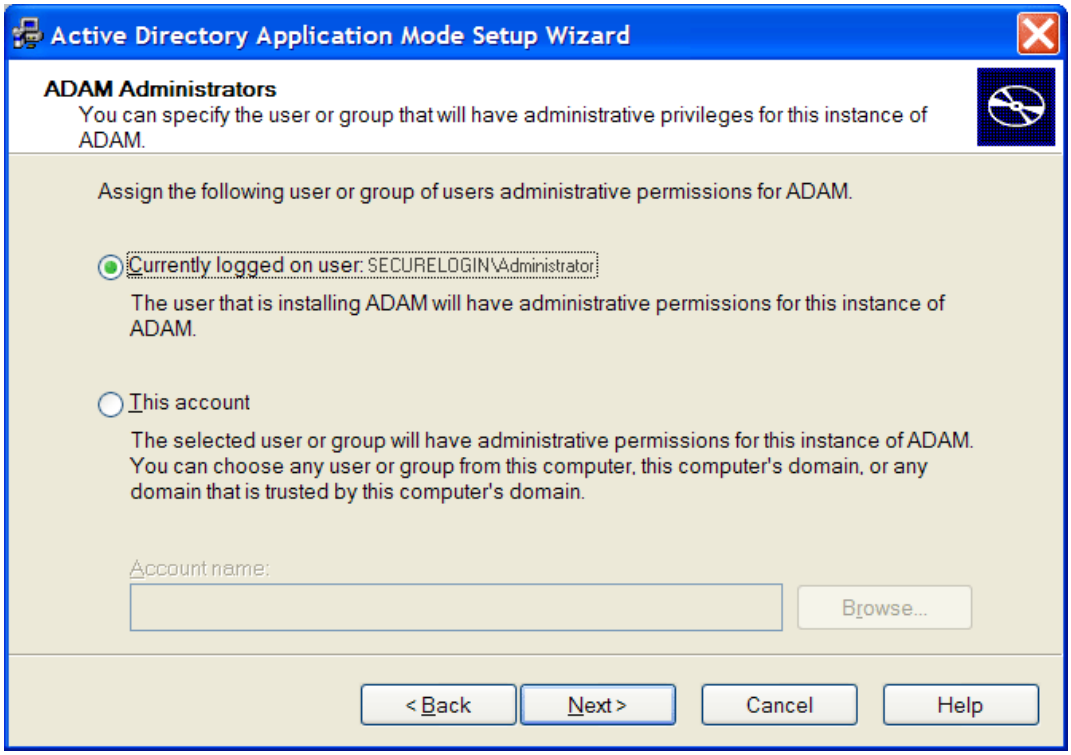
Select *This account* and provide the credentials for the selected service account.

We recommend you to select *Network service account*. Nevertheless, you can specify an account with a static password.

NOTE: The selected service account must have permissions to register a Service Connection Point (SCP) and permission to install Novell SecureLogin.

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

18 Select the *Currently logged on user: SECURELOGIN\Administrator* option.



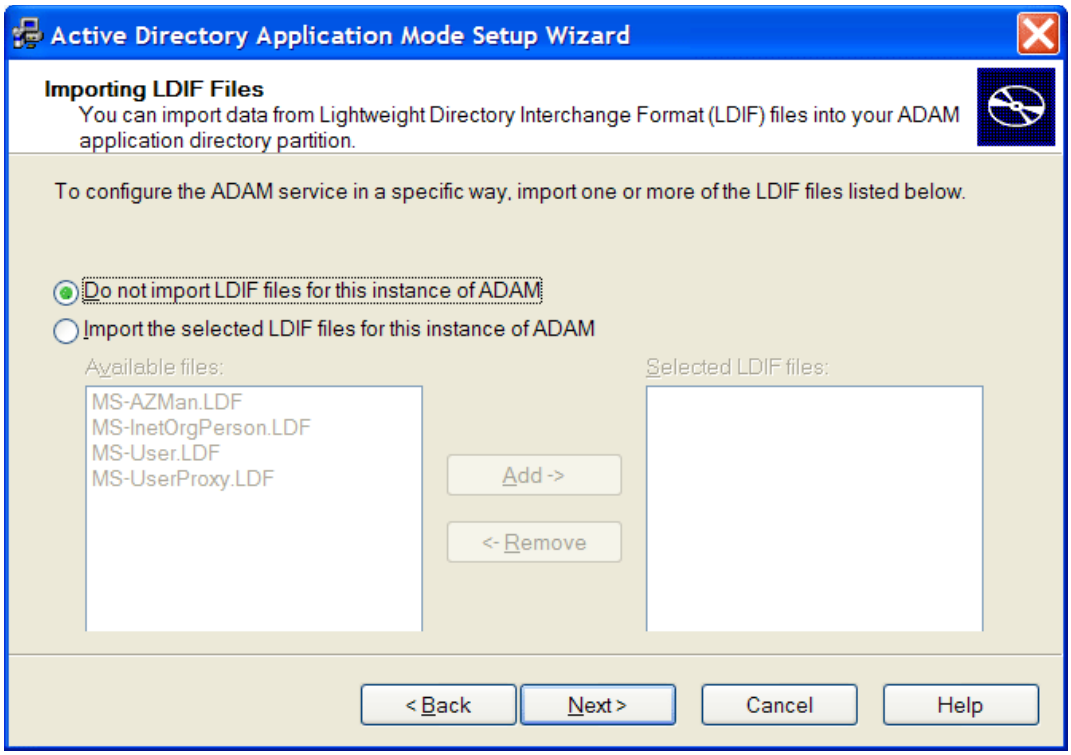
NOTE: The selected account must have administrator level permissions. In this example, the default is selected as the current user. So, the administrator administers this ADAM instance.

or

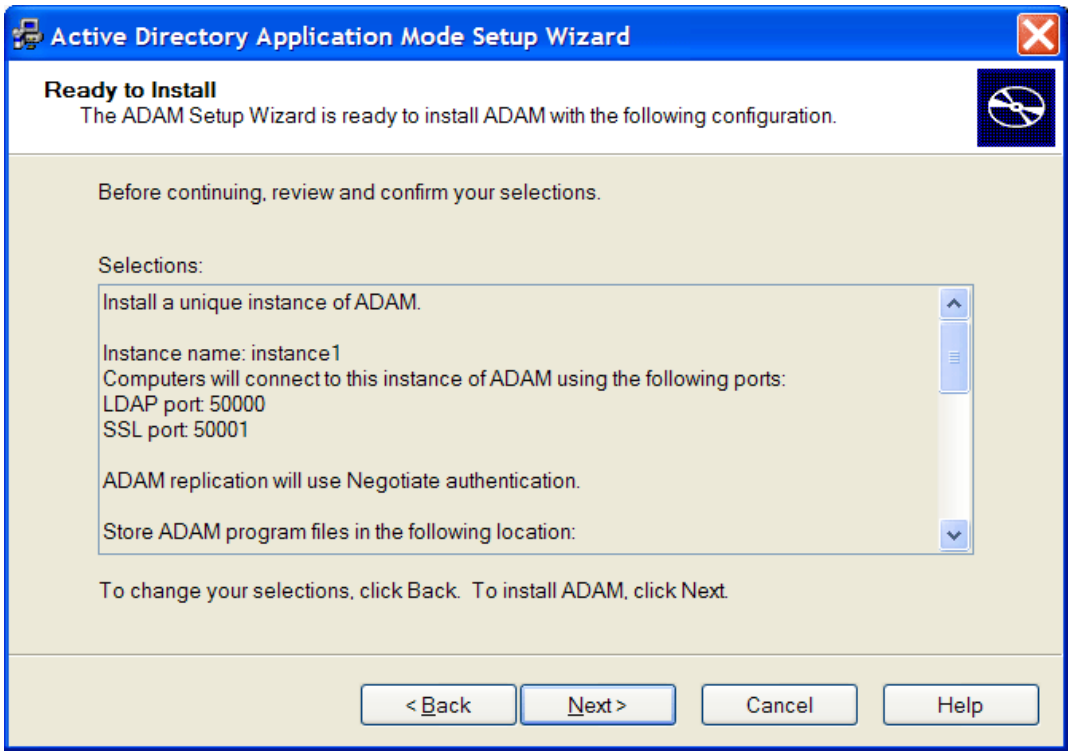
If an alternative account or group is preferred, select *This account* and specify the account or group name and credentials.

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

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



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

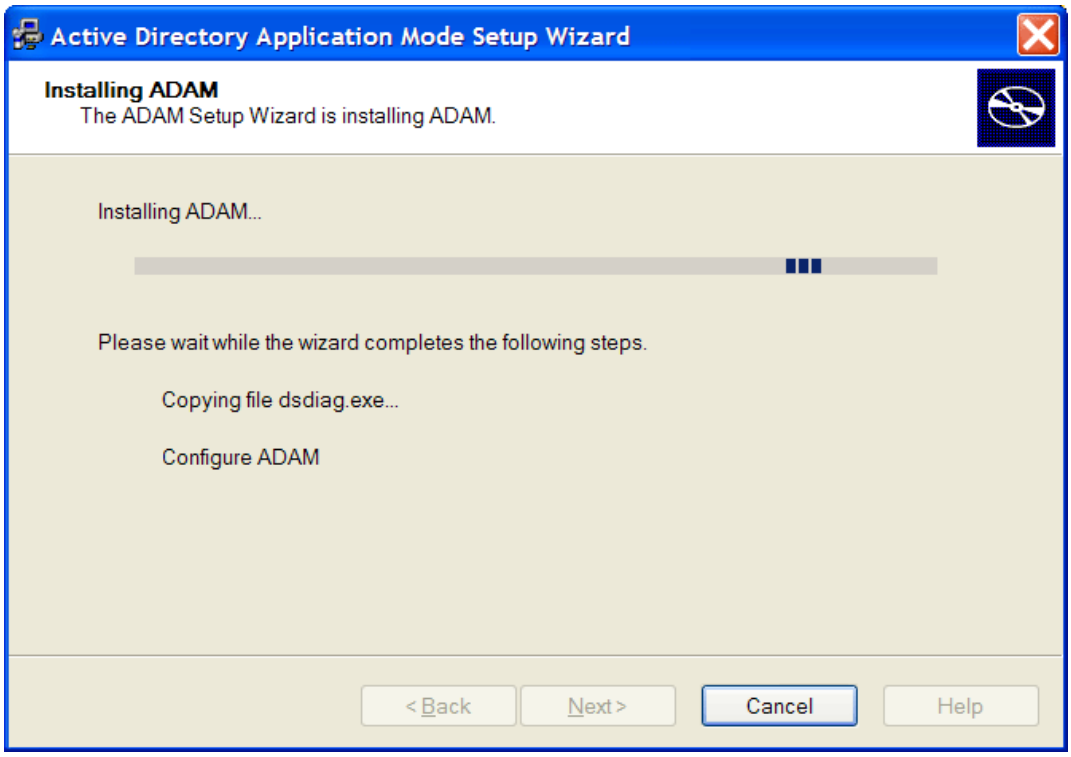


22 Review the setup options in the Selections window to confirm that the required options are selected.

23 Click *Next* to continue with the installation.

or

Click *Back* to change selected options and continue the installation.



24 Click *Next* after confirming the ADAM instance creation settings.

25 Click *Finish* to create the ADAM instance. The Completing the Active Directory Application Environment Setup Wizard page is displayed after the ADAM instance is created.

If required, you can review the Windows Event log to ensure the ADAM instance is created without errors.

16.3.1 Reviewing the Windows Event Log

1 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.

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

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

After the ADAM instance is successfully created, execute the instructions provided Section 16.4, “Extending the Schema by Using ADAM Configuration Wizard,” on page 117 to automatically extend the ADAM instance schema and assign Read and Write Rights to directory user objects.

16.4 Extending the Schema by Using ADAM Configuration Wizard

The Novell SecureLogin ADAM configuration wizard extends the ADAM directory schema with Novell SecureLogin attributes, creates ADAM partitions, and assigns selected directory objects read and write permissions to the Novell SecureLogin attributes. The wizards creates corresponding user proxy objects in Active Directory. This includes the directory hierarchy to the ADAM instance. This can be used to synchronize user object structure after the initial configuration of Novell SecureLogin.

The ADAM schema can be extended manually at the command line using the `MSUserProxy. LDF` and `sso-adam-schema.LDF` files. These files are located in the `\SecureLogin\Tools\Schema\ADAM` folder of the Novell SecureLogin 7.0 installer package. We recommend that you perform this procedure with the assistance of our Technical Support.

16.4.1 Prerequisites

Before running the SecureLogin ADAM Configuration Wizard:

1. Download and install the Windows Support Tools for Microsoft Windows XP from the Microsoft Web site. (http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en)

   or

   Download and install the Windows Support Tools for Windows Server 2003 from the Microsoft Web site. (http://www.microsoft.com/downloads/details.aspx?FamilyId=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en)

   Windows Support Tools for Windows include `dsacls.exe`, which is required by the ADAM Configuration Wizard.

   This file is included in a default installation of Windows Server 2003.
2. Copy the `AdamConfig.exe` file found in `\SecureLogin\Tools\Schema\ADAM` to server or the administrator workstation.
3. Copy `dsacls.exe` from Windows Support Tools to the ADAM folder on the server or Administrator workstation.

16.4.2 Using the ADAM Configuration Wizard

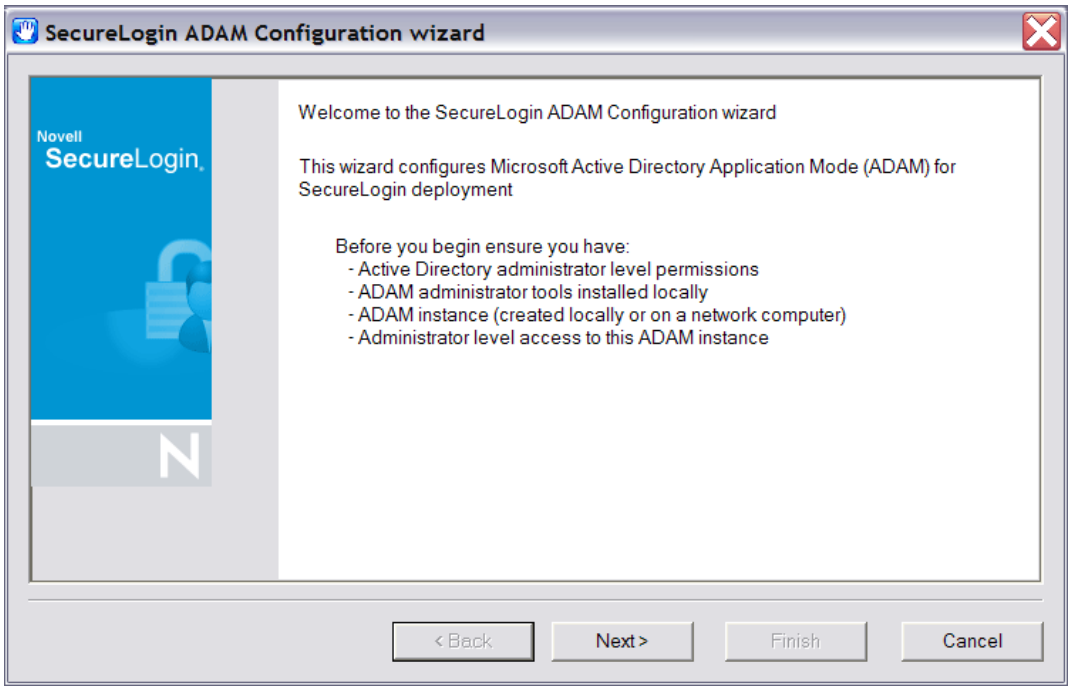
The ADAM Configuration Wizard extends the ADAM directory schema with Novell SecureLogin attributes, creates ADAM partitions, and assigns selected directory objects with read and write permissions to the SecureLogin attributes.

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 user object structure after initial configuration of SecureLogin.

To run the ADAM configuration wizard:

1 Log in to the ADAM instance, server, or the administration workstation (if it is separate) as an administrator or an user with administrator permissions.

2 Browse to the `AdamConfig.exe` file, double-click to run it. The Welcome to the SecureLogin ADAM Configuration Wizard page is displayed.



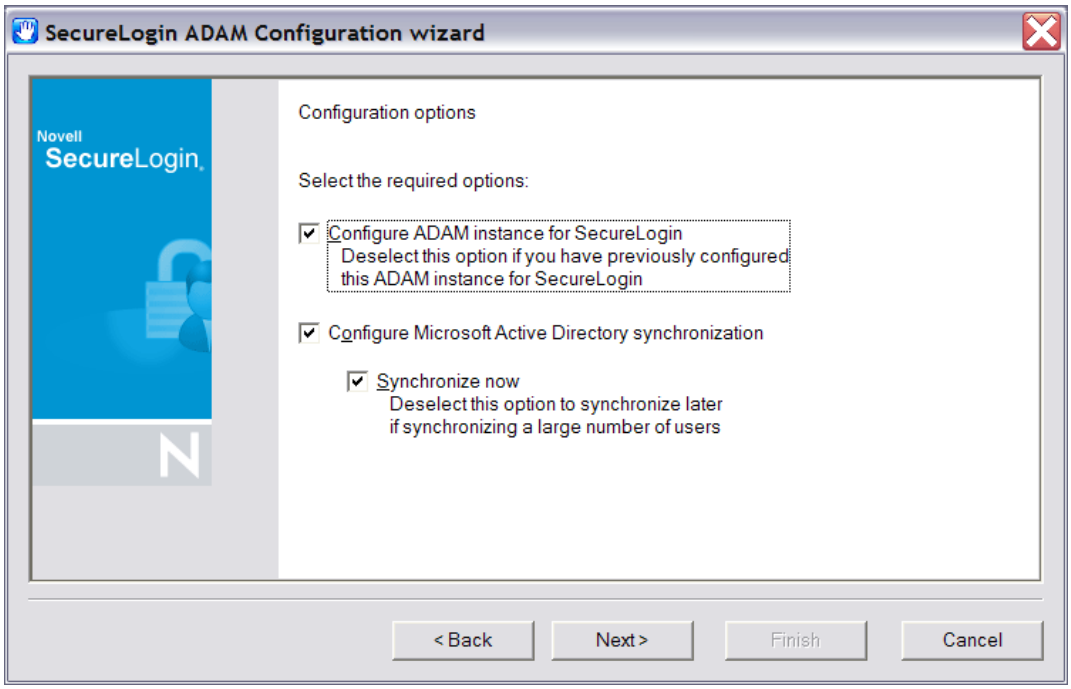
Ensure that you have all the Active Directory and ADAM administrator account details required.

NOTE: The ADAM schema can be extended manually at the command line using the `MS-UserProxy.ldf` and `sso-adam-schema.ldf` files. These files are located in the `Tools` folder of the installer package.

---

3 Click *Next*.

4 Configure ADAM instance for Novell SecureLogin.



Select this option during the first instance of configuration. Although the ADAM configuration is required only once, selection of this option on subsequent executions does not have any adverse effects.

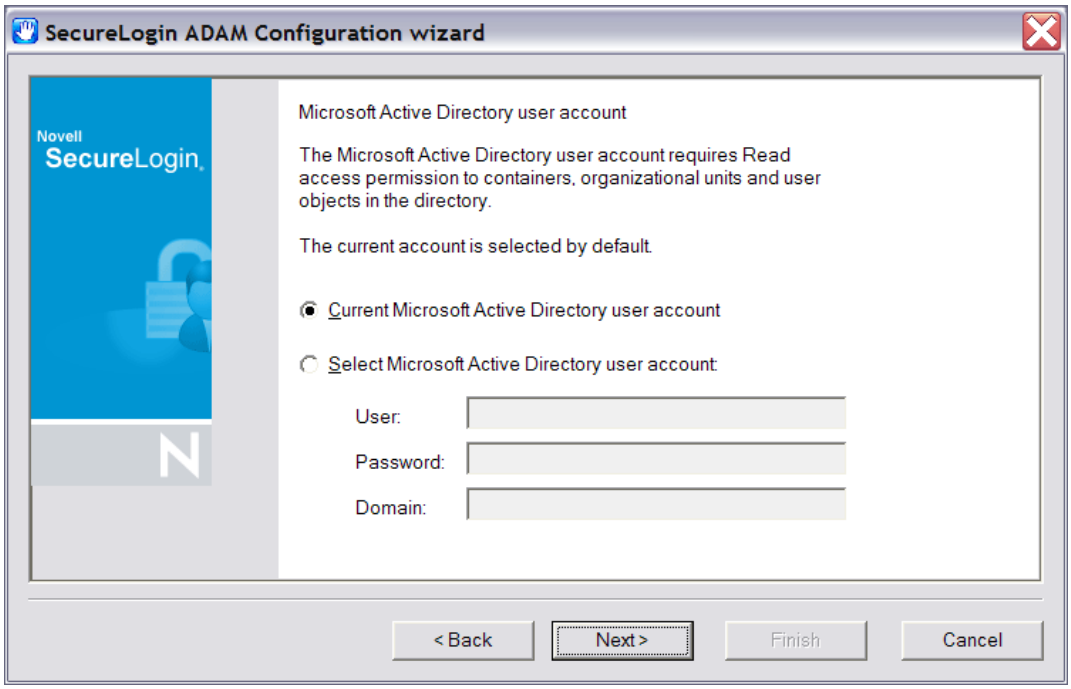
The ADAM configuration wizard copies across the selected Active Directory user data to the ADAM instance, including the directory hierarchy.

NOTE: Directory synchronization for a large number of users can adversely affect the network performance. You can delay the directory synchronization to a more convenient time.

You can run the ADAM configuration wizard at any time to synchronize the updated Active Directory user data.

---

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



6 (Optional) Select *Synchronize now* option.

NOTE: Each time a new organizational unit or user object is created in Active Directory, the ADAM configuration wizard or the `SyncAdam.cmd` command file must be executed to synchronize with the ADAM instance and assigned read and write permissions.

The `SyncAdam.cmd` cannot be run before running the ADAM configuration wizard.

---

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

8 Select *Current Microsoft Active Directory*, the click *Next*.

or

Select *Select Microsoft Active Directory user account* and specify the account details in the *User*, *Password*, and *Domain* fields, then click *Next*. The ADAM instance location page is displayed.

NOTE: 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.

By default, the current account (that is, the one to which you are logged in) is selected. However, any user account that has Active Directory read permission is valid.

9 Click *Next*. The ADAM instance location page is displayed.

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

11 Click *Next*. The Microsoft Active Directory containers/organizational units page is displayed.

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

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

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

14 Click *OK*.

If the specified distinguished name of the domain, container, or organizational unit is invalid, an error message is displayed. In that case, click *OK*. You return to the dialog box. Specify the correct distinguished name of the domain, container, or organizational unit.

15 Click *OK* when the required objects are added to the list. The Configuration summary page is displayed.

Review the selected configuration options.

16 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.

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

17 Click *Close*.

16.4.3 Viewing Objects Using the ADAM ADSI Edit Tool

The ADSI Edit Tool is a Microsoft Management Console (MMC) snap-in which you can use to view all objects in the directory, including the schema and configuration information, modify objects, and set access control lists on the objects.

You can use the ADSI Edit tool to check and review Novell SecureLogin ADAM configuration. To do this:

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

2 Select *ADAM 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 *Distinguished name (DN) or naming context*.

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

9 Select *Connect using these credentials*. This is the account through which you wish to connect to the ADAM instance.

In this example, *The account of the currently logged on user* is selected

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

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

12 Select *Properties*. The CN=Users Properties dialog box is displayed.

To confirm if the schema attributes are added successfully or not, scroll down the Attributes table window and verify if the six attributes in Section 16.2, “Configuring ADAM Schema,” on page 108 are listed or not. Repeat this for each container and or organizational unit containing Novell SecureLogin users.

If the attributes are not displayed, run the ADAM configuration wizard again and ensure that you specify the correct container, organizational unit, and user objects.

16.4.4 Synchronizing Data from Active Directory to an ADAM Instance

The Active Directory to ADAM Synchronizer is a command-line tool that synchronizes data from Active Directory forest to a configuration set of an ADAM instance. You can use this to ensure that new users are added to Active Directory have objects representing their Novell SecureLogin data created in the ADAM instance.

To synchronize data from Active Directory to an ADAM instance:

1 Navigate to `SecureLogin\Tools` of the Novell SecureLogin 7.0 installation package.

2 Double-click the `syncadam.cmd` file.

After the synchronization is complete, you can look at the log file - `SyncAdam.log`, to ensure that the synchronization process is complete.

It is recommended that you synchronize regularly, when new organizational units are created or when Active Directory user are changed. You can add the process to the Windows Schedules Tasks.

During the synchronization, 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.

However, 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.

Installing

17

17.1 Prerequisites

Novell SecureLogin 6.0 requires Microsoft Windows Installer 3.0 or later. Windows Installer 3.0 ships as part of Windows XP SP2 and is also available as a redistributable component for Microsoft Windows XP, Microsoft Windows XP1, and Microsoft Windows Server 2003 (32-bit) from the Microsoft Web site. (http://www.microsoft.com/downloads/details.aspx?familyid=889482fc-5f56-4a38-b838-de776fd4138c&displaylang=en)

17.2 Installing on Administrator Workstations

The following procedures apply for manual installation and are applicable to installing Novell SecureLogin on small number of workstations or notebook computers.

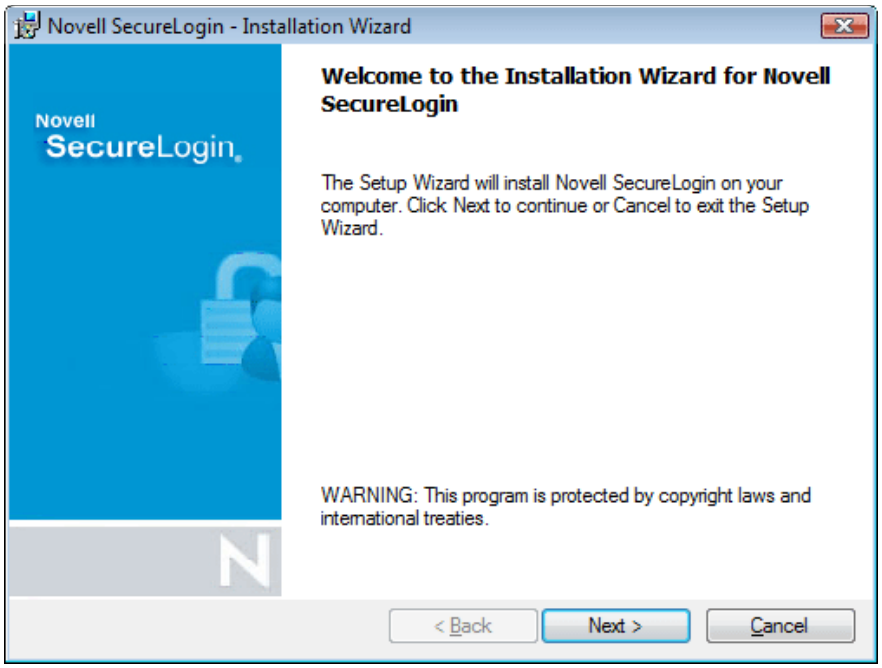
It is recommended that you deploy and manage Novell SecureLogin across large enterprise by using industry standard application distribution packages such as Systems Management Server (SMS), Novell® ZENworks®, and Microsoft IntelliMirror*.

NOTE: The procedures for installing on administrator workstation and user workstations are the same.

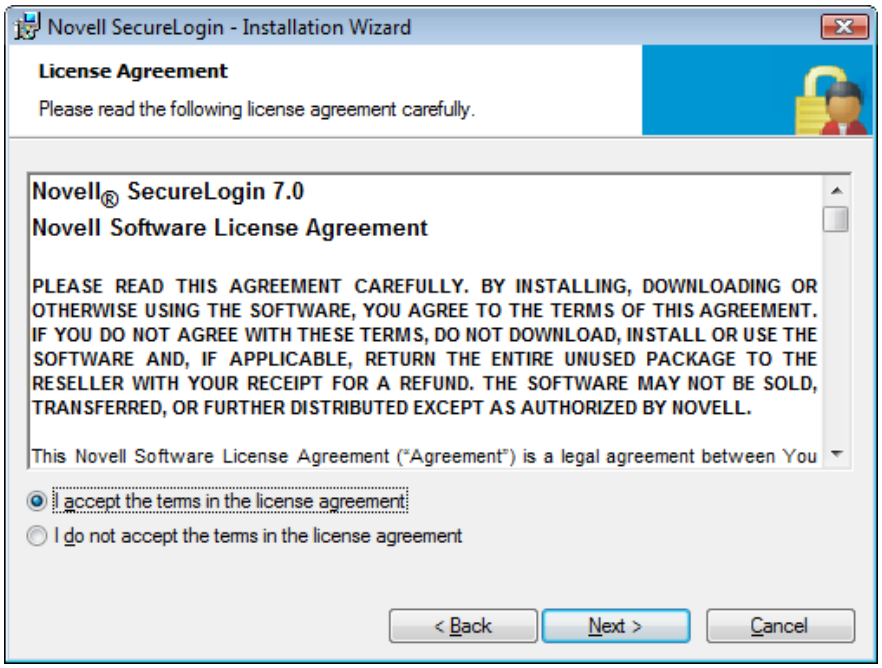
The procedures explained in the following section uses the Microsoft Windows Vista 64-bit installer.

---

1. Log in to the workstation as an administrator.
2. Double-click `Novell SecureLogin.msi` located in the `SecureLogin\Client\x64` directory of the Novell SecureLogin installer package. The Welcome to the Installation Wizard for Novell SecureLogin is displayed.



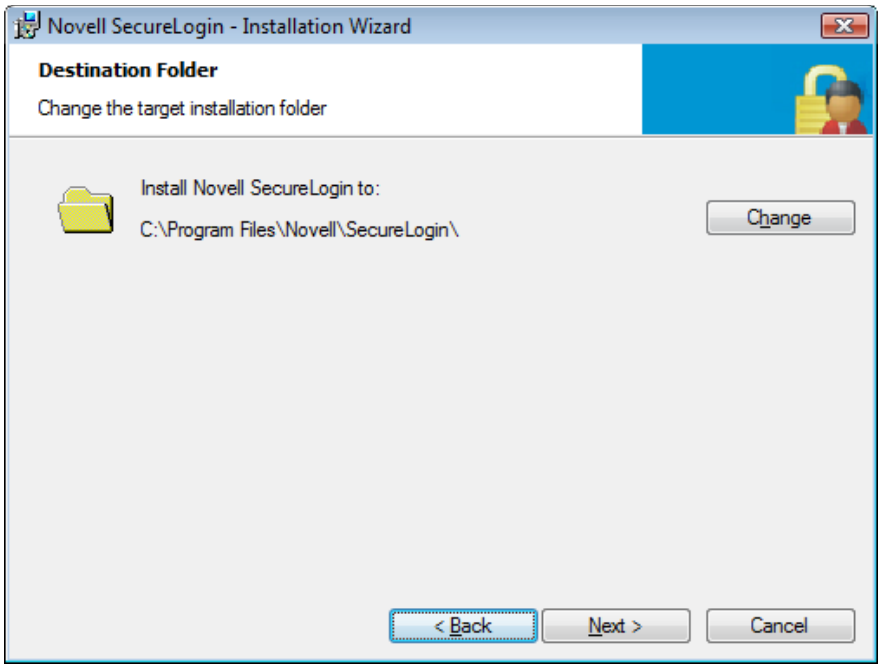
3 Click *Next*. The License Agreement page is displayed.



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

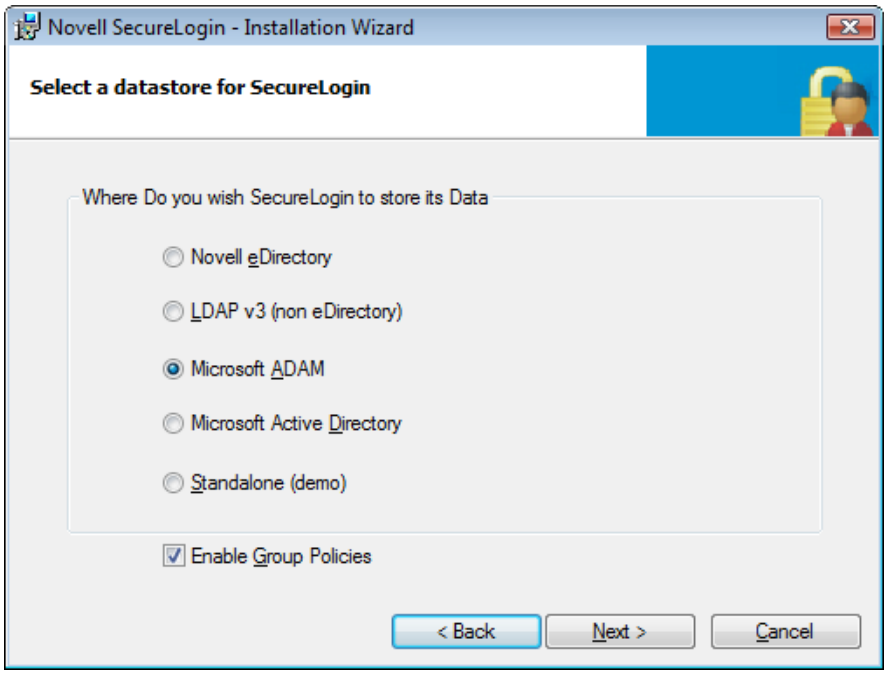
The Destination Folder page is displayed. By default, the program is saved in `C:\Program Files\Novell\SecureLogin\`.You can accept the default folder or choose to change.

To change, click *Change* and navigate to your desired folder.



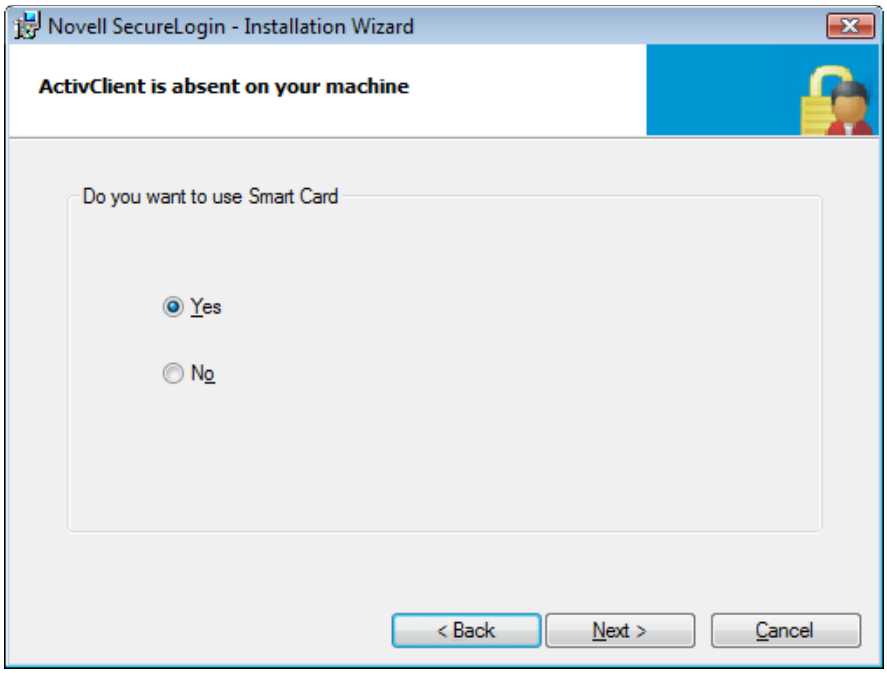
5 Click *Next*. Select a Datastore for SecureLogin (that is, the installation environment) page is displayed.

6 Select *Microsoft ADAM*.



7 (Optional) *Select Enable Group Policies*.

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



The ActivIdentity* ActivClient card settings are used if they are detected.

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 through Public Key Infrastructure (PKI) tokens.

9 (Conditional) If you want to use a smart card, select *Yes* >, click *Next*, then continue with Step 11.

IMPORTANT: If your enterprise policy allows users log in to the workstation by using a smart card, you must select the smart card option.

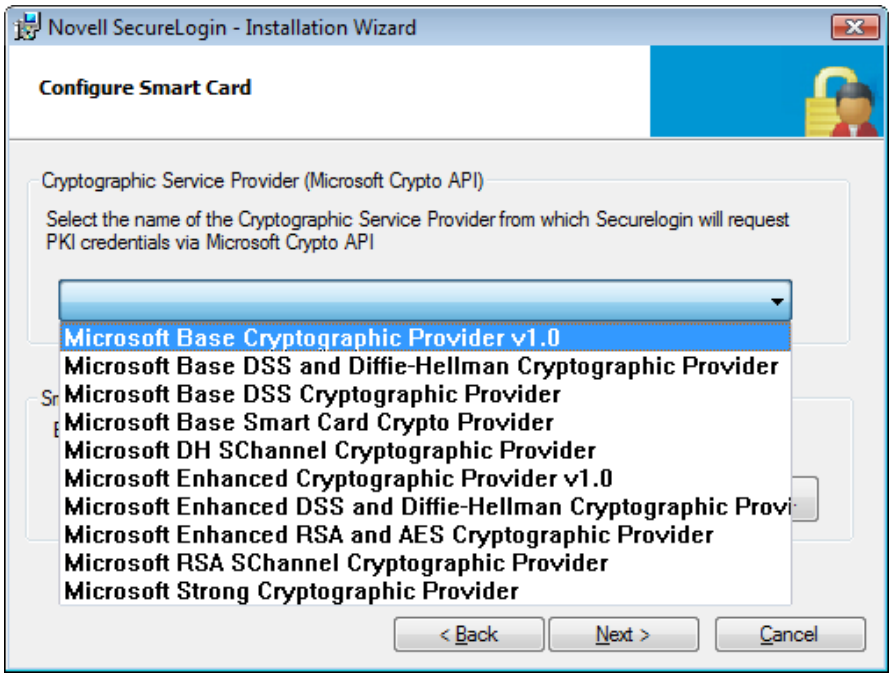
---

10 (Conditional) If you do not want to use a smart card, select *No* > , click *Next*, then continue with Step 17.

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

12 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 Novell SecureLogin to communicate with the smart card.



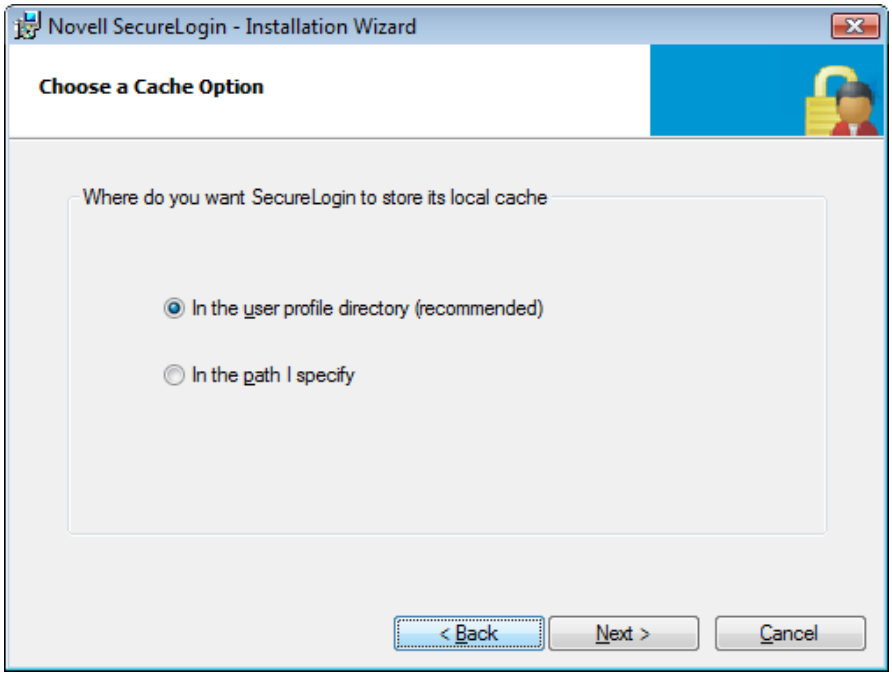
Manually configuring the third-party smart card PKCS library assumes a high level of understanding of the cryptographic service provider's product.

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

14 Select the location where you want Novell SecureLogin to store the local cache.

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

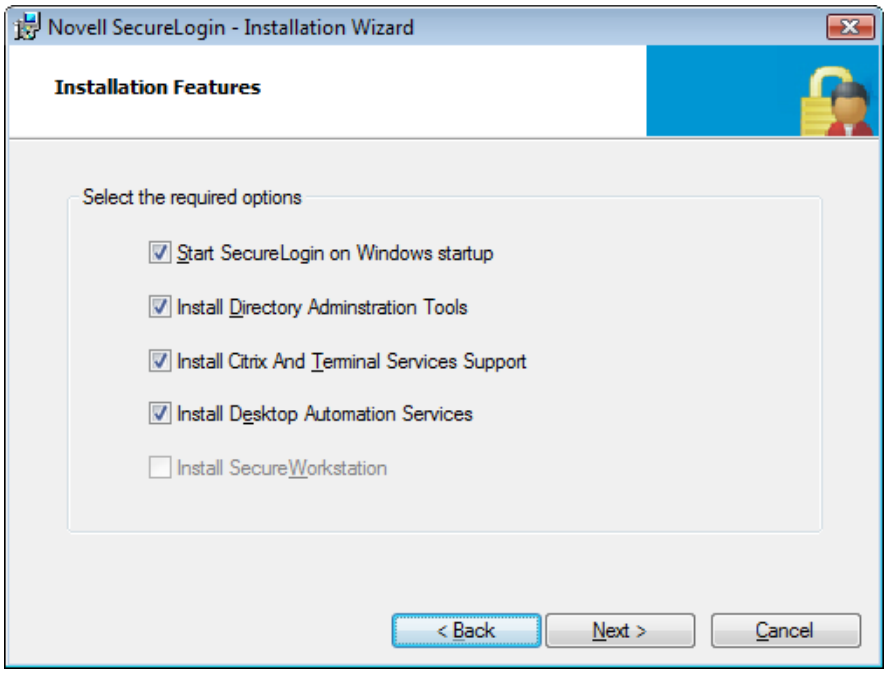
16 (Optional) If you want to change the location of the cache folder, select *In the path I specify* and specify an alternative folder.



IMPORTANT: If you selected *Enable Group Policies* option in Step 7, you must create or locate a unique custom folder for every user of the workstation. Include a user-specific variable such as %USERNAME% in the directory path

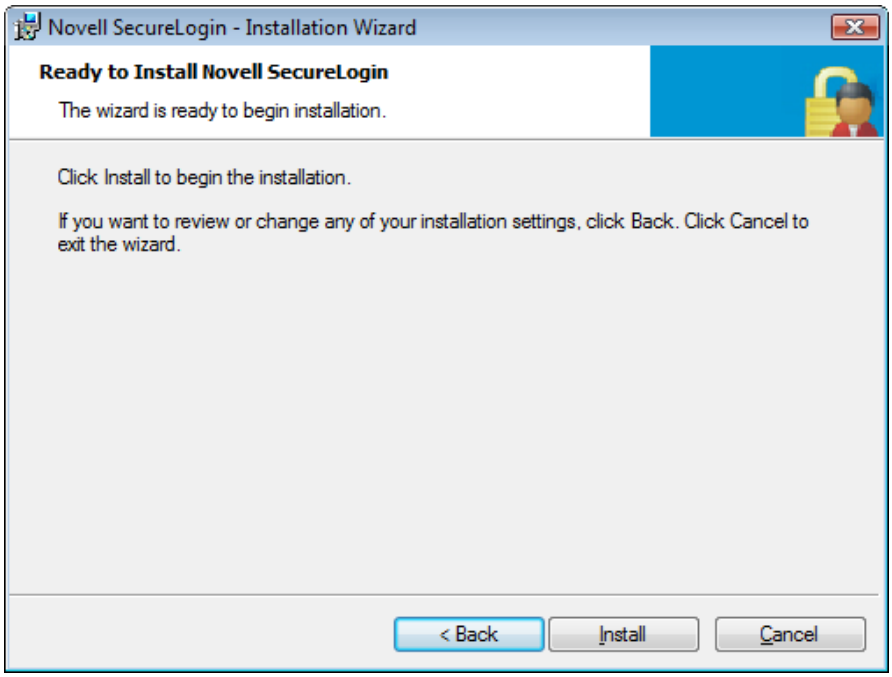
17 Click *Next*. The installation features page is displayed.

Select the options you want to install.

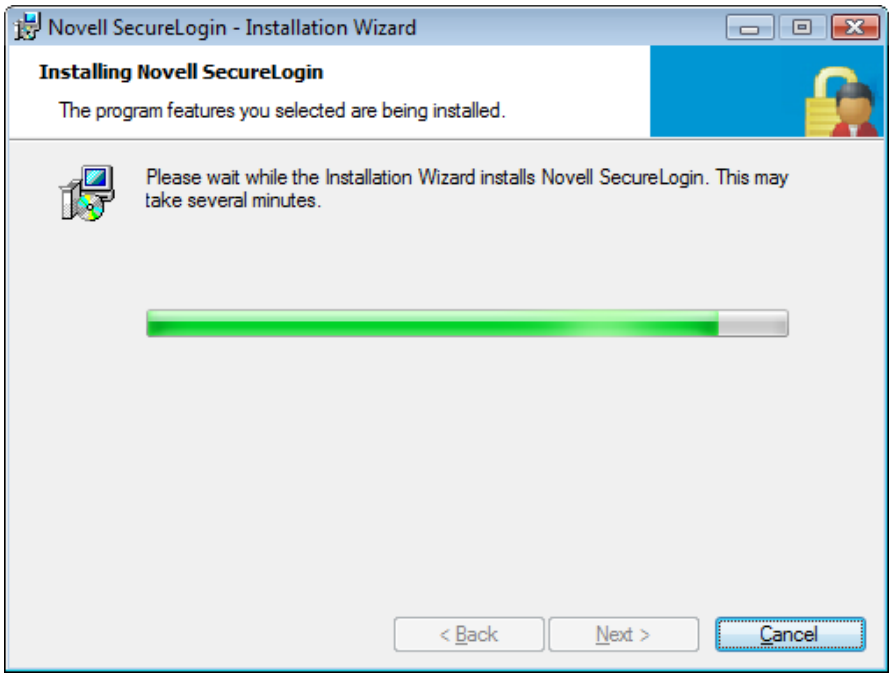


Secure Workstation is not available in ADAM environment.

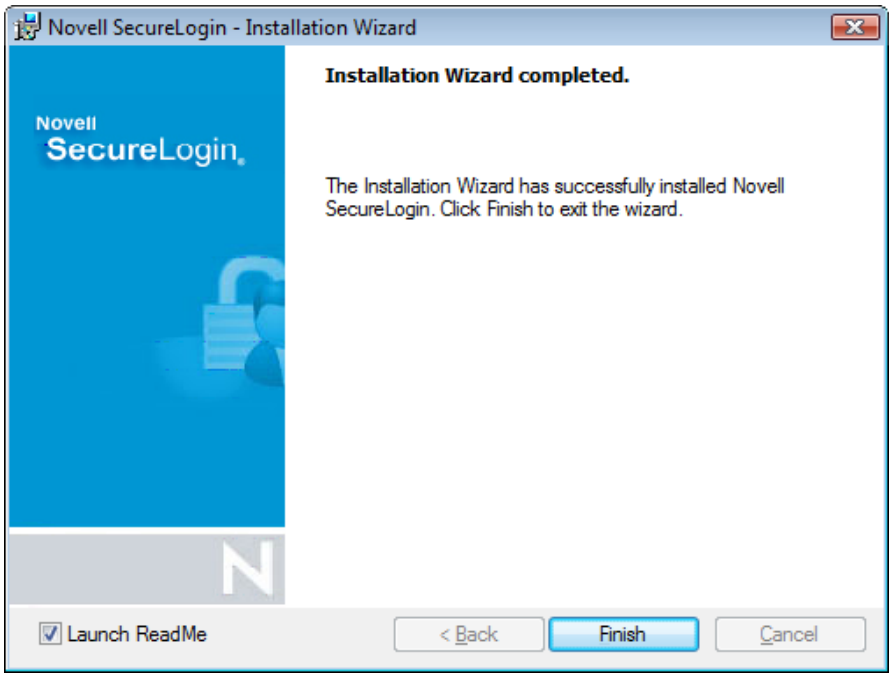
18 Click *Next*. The Ready to Install the Program page is displayed.



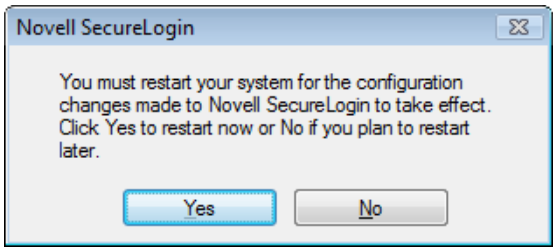
19 Click *Install*. The installation process takes a few minutes.



20 Click *Finish*.



21 You are prompted to restart your system. Select *Yes*.



17.3 Installing Novell SecureLogin on a User Workstation

The procedure for installing Novell SecureLogin 7.0 on a user workstation is the same as the procedure for a administration workstation.

Follow the instructions given in Section 17.2, “Installing on Administrator Workstations,” on page 125.

17.4 Installing for Mobile Users and Notebooks

Installing Novell SecureLogin 7.0 for mobile users and notebooks follows the same procedure as explained in Chapter 17, “Installing,” on page 125.

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.

Deploying

18

SecureLogin provides centralized management and deployment of user configuration by using the directory structure and administration tools.

You can manage users through the Administrative Management Utility accessed from the Windows Start menu.

The following section explain the various tasks involved in deploying Novell SecureLogin 7.0 in an ADAM environment.

18.1 Configuring a User’s Environment

Novell SecureLogin provides a range of options for deployment and distribution of user configurations. We recommend that Novell SecureLogin configuration is installed on test user accounts prior to deployment.

Configuring a user’s Novell SecureLogin 7.0 includes:

- Setting preferences
- (Optional) Creating password policies
- Enabling single sign-on for required applications.
- (Optional) Creating passphrase questions for user selection

18.2 Administering Novell SecureLogin In an ADAM Environment

Novell SecureLogin users are managed through the Administrative Management utility. Through this you can manage users at the container, organizational unit, and user object levels.

NOTE: You can administer Novell SecureLogin 7.0 either through the SLManager or through Novell iManager®.

Throughout this document, the phrase Administrative Management utility refers to Novell iManager.

---

1. Launch iManager.
2. Specify your username, password, and 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 administrative rights to the tree.

For detailed information on accessing iManager, visit the iManager documentation on Novell Documentation Web site. (http://www.novell.com/documentation/imanager27/imanager_admin_271/index.html?page=/documentation/imanager27/imanager_admin_271/data/bsxrjzp.html)

18.3 Setting Up a Passphrase

After you have successfully installed Novell SecureLogin 7.0 on a user workstation, set up a passphrase for the user.

Refer Chapter 3, “Setting Up a Passphrase,” on page 23 for more information.

18.4 SecureLogin and FireFox

Novell SecureLogin 7.0 supports Mozilla* Firefox* 1.5, 2.0, and 3.0. We recommend that SecureLogin is installed or upgraded with Firefox version 1.5 or later for SLoMoz.xpi extension to be automatically installed and configured.

Installing and Deploying On Standalone Environment

VI

This section covers installing Novell SecureLogin 7.0 on a standalone environment. Standalone installation operates on a workstation that is independent of a network or corporate directory system. Standalone installation is intended for individual users, in addition to providing a platform for SecureLogin SSO version control, review and testing.

Getting Started

19

Novell SecureLogin can be installed in a standalone mode that operates on a user's workstation. It is independent of a network or corporate directory system. Standalone mode installation allows single sign-on to applications on individual workstations, provides a platform for SecureLogin version control, review, and testing.

This section contains information on the following:

19.1 New Installations

A new installation of Novell SecureLogin 7.0 that is installed in standalone mode is installed in seamless mode. Your workstation login credentials are used to start Novell SecureLogin.

In the previous versions of Novell SecureLogin, you needed an account to log in to the workstation and then choose a user from a list or create a new user.

If you upgrade from a previous versions of Novell SecureLogin, you are prompted to migrate to seamless mode.

19.2 Unsupported Features

The following features are not supported in a standalone install:

- All smart card functionalities, including
  - Smart card configuration for single sign-on.
  - Smart card password login.
- The passphrase question and answer security system.
- AES datastore encryption.

19.3 Prerequisites

- You must have administrator level access to the workstation.
- Have a backup of the existing workstation directory.
- Novell SecureLogin 7.0 requires Microsoft Windows Installer 3.0 or later. Microsoft Windows Installer 3.0 ships as part of Windows XP Service Pack 2 (SP2) and is also available as a redistributable system component for Microsoft Windows 2000 SP3, Microsoft Windows 2000 SP4, Microsoft Windows XP, Microsoft Windows XP SP1, and Microsoft Windows Server 2003 (32-bit systems). You can download this from the Microsoft Download Web site. (http://www.microsoft.com/downloads/details.aspx?familyid=889482fc-5f56-4a38-b838-de776fd4138c&displaylang=en)

19.4 Installation Overview

NOTE: The `?syspassword` variable does not work in standalone mode. Because smart card options cannot be selected in a standalone mode installation, smart card login to standalone mode installs is not supported.

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.

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.

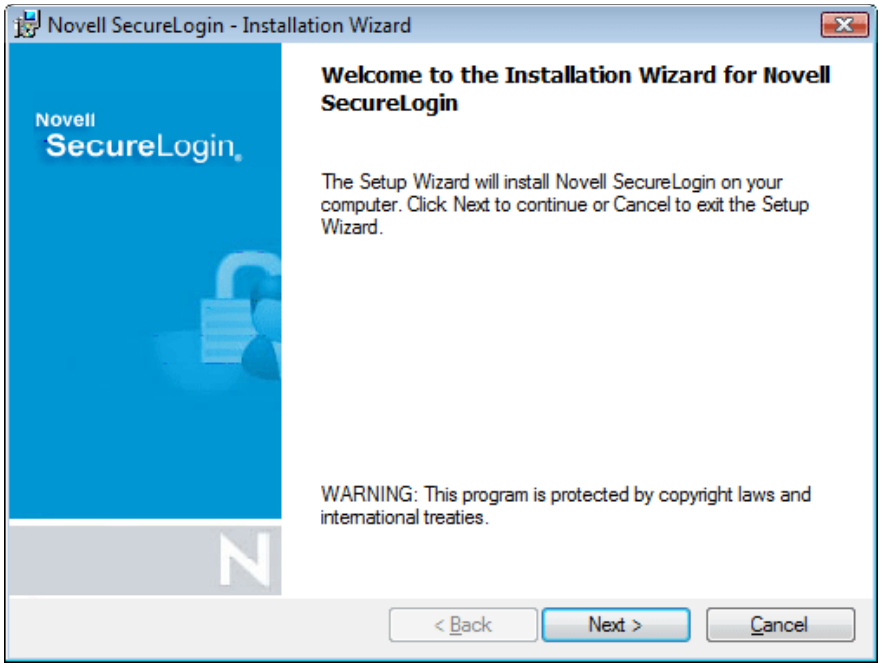
Installing

20

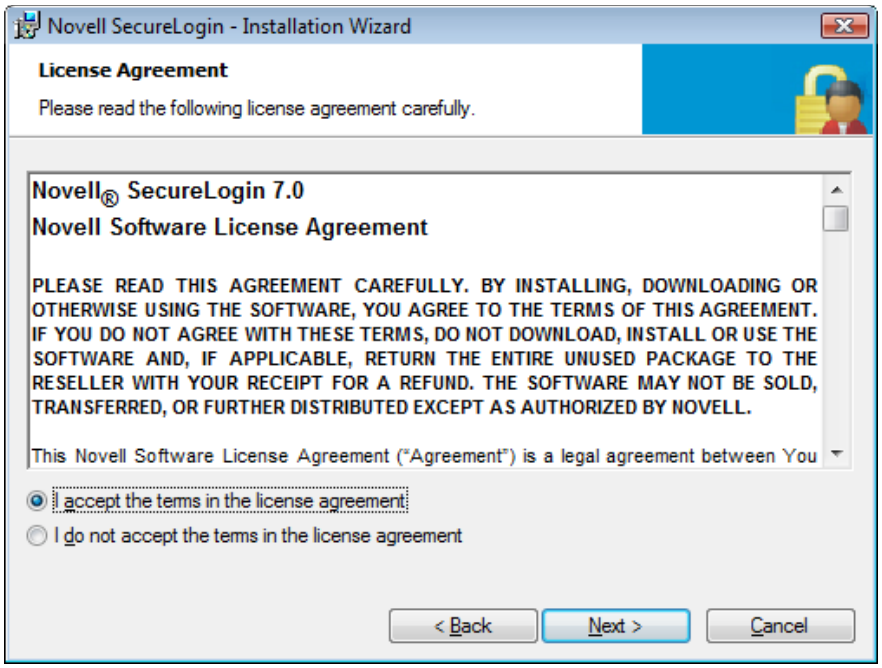
This section contains information on the following:

20.1 Installing On a Standalone Workstation

1. Log in to the workstation as an administrator.
2. Double-click `Novell SecureLogin.msi` located in the `SecureLogin\Client\x64` directory of the Novell SecureLogin installer package. The Welcome to the Installation Wizard for Novell SecureLogin is displayed.



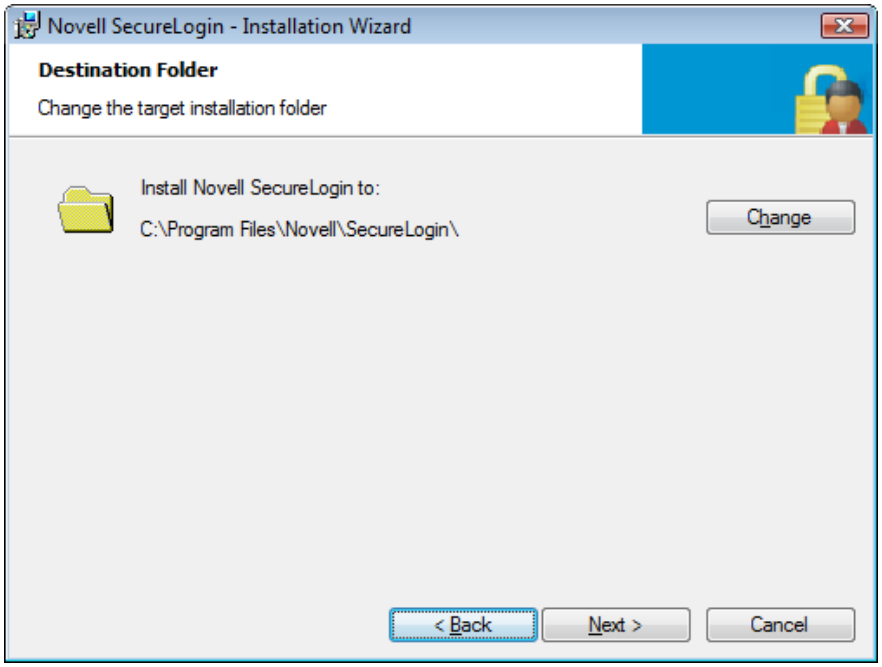
3. Click *Next*. The License Agreement page is displayed.



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

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 Click *Next*. Select a Datastore for SecureLogin (that is, the installation environment) page is displayed.

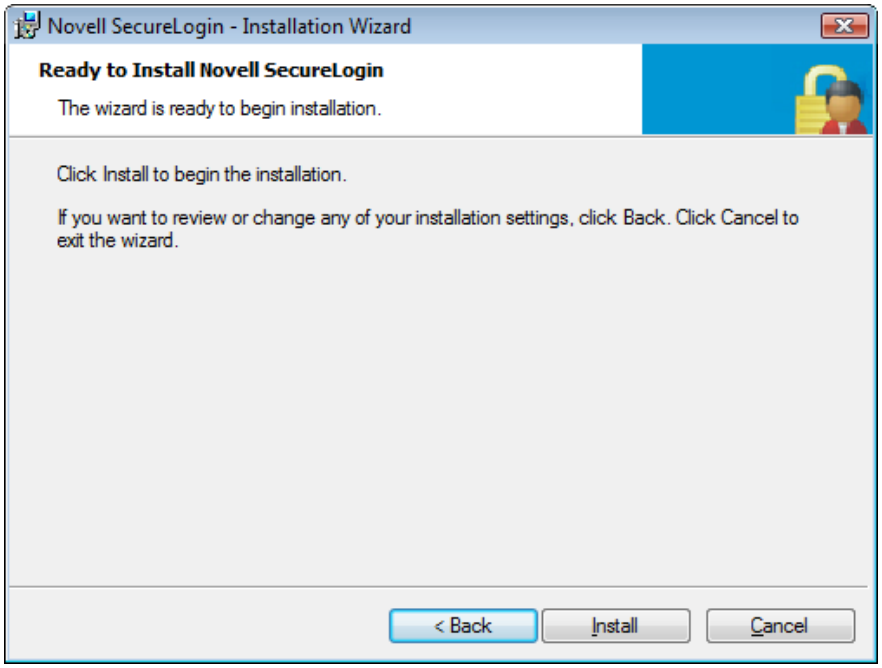
6 Select *Novell eDirectory* as the platform where Novell SecureLogin stores its data, then click *Next*. The cache option dialog box is displayed.

7 Select the location where you want Novell SecureLogin to store the local cache.

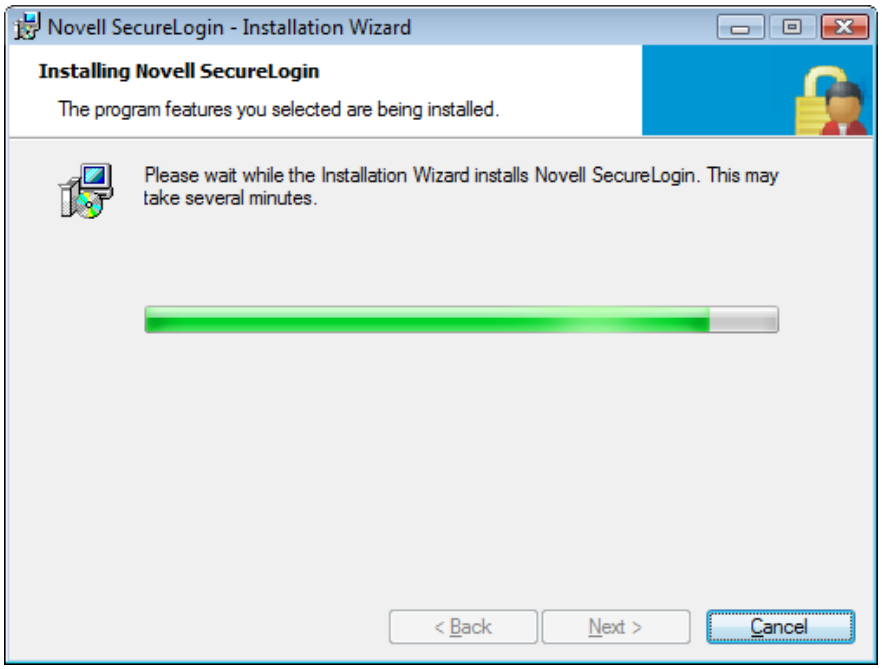
8 Click *Next*. The installation features dialog box is displayed.

9 Only the *Start SecureLogin on Windows Startup option* is available. Select the option.

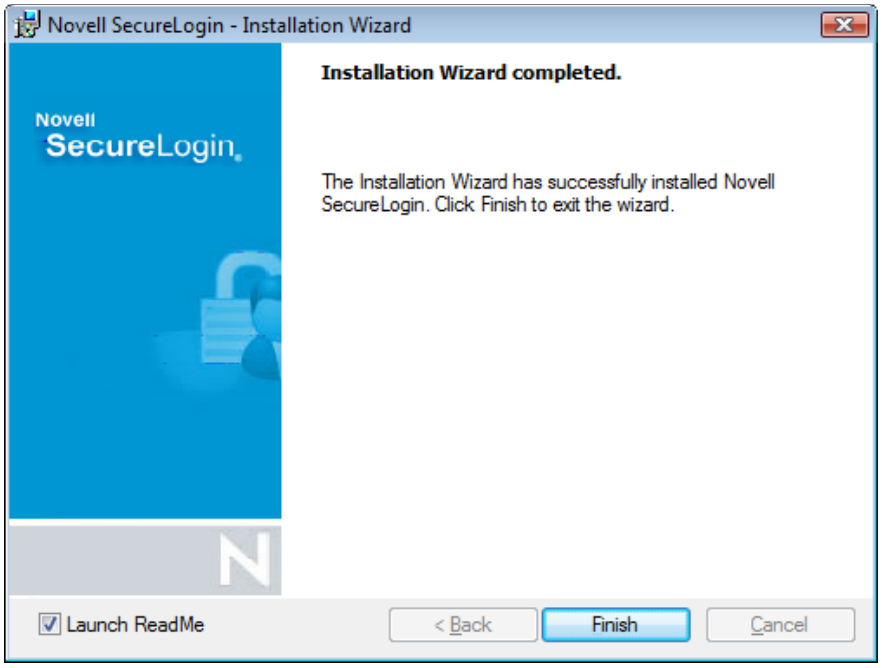
10 Click *Next*. The Ready to Install the Program page is displayed.



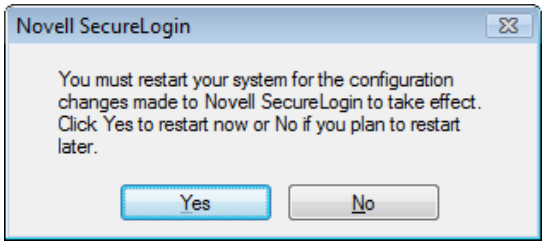
11 Click *Install*.



12 Click *Finish*.



13 You are prompted to restart your system. Select *Yes*. .



20.2 Upgrading from an Earlier Version

The previous versions of Novell SecureLogin supported creating multiple SecureLogin accounts for a single workstation account.

Novell SecureLogin 6.0 has a seamless standalone mode that uses the workstation account to identify the users, thereby eliminating the requirement for the user to log in to Novell SecureLogin after logging in to the workstation.

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

After upgrading, you are prompted to either continue using multiple accounts or choose one account and migrate to seamless standalone mode.

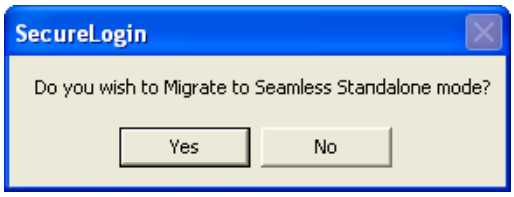
If you have been using Novell SecureLogin in standalone mode in one account, you are automatically migrated to seamless standalone mode after providing your username and password on first log in.

20.2.1 Setting Up Multiple User Accounts

The previous versions of Novell SecureLogin managed multiple accounts on the same workstation by creating multiple SecureLogin accounts for the same Windows account. Novell SecureLogin now consolidates the accounts by leveraging the Windows account to verify the user. This results in one Novell SecureLogin user for each Windows account.

After upgrading, the following message appears.

Figure 20-1 *Seamless migration message*



- If you wish to manage the users through their Windows accounts, click Yes and migrate to seamless standalone mode. This deletes all other user accounts but it does not delete the one you are requested to selected.
- If you have previously configured SecureLogin with multiple users, click No to continue accessing them.

  The SecureLogin Standalone dialog is displayed. The dialog box retains all the user accounts retained from the previous SecureLogin configuration.

  You can then select from two options:

  - If you had earlier selected Yes, select the user or the account that will continue to be user future Novell SecureLogin account.
  - If you had earlier selected No, select the user account that you require now. This list displays all the accounts retained for future log in.

  Specify the password. Novell SecureLogin is now active for the selected user and the Novell SecureLogin icon appears in the notification area.

20.2.2 Managing Novell SecureLogin After upgrading

For mobile users and notebook users, Novell SecureLogin is managed through the Personal Management Utility. To start 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 20.2.3, “Setting Up Single Account,” on page 143

20.2.3 Setting Up Single Account

- “Upgrading From 3.5 Or Later to 7.0” on page 144
- “Upgrading From 3.0 Or Earlier to 7.0” on page 144

Upgrading From 3.5 Or Later to 7.0

If you are upgrading from Novell SecureLogin 2.5 or later, Novell SecureLogin automatically updates the single account to match the workstation account.

Upgrading From 3.0 Or Earlier to 7.0

Novell SecureLogin 3.5 or earlier must be uninstalled before installing Novell SecureLogin 7.0

20.3 Creating a New User Account

When Novell SecureLogin is started after a new installation on a standalone workstation, the SecureLogin Standalone dialog is displayed.

1. Click *Create User*. The Create User page is displayed
2. Specify the Username and Password.
3. Re-enter the password to verify.
4. Click *OK*.

Installing through the Command Line

VII

This section describes how to install Novell SecureLogin through the command line. Novell SecureLogin can be installed, 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.

This section contains the following information.

Installation Overview

21

Prerequisite

Novell SecureLogin requires Microsoft Windows Installer 3.0 or later.

Depending on the operating system and the level of patches and service packs applied to it, download the redistributables from the Microsoft Download Web site. (http://www.microsoft.com/downloads/details.aspx?familyid=889482fc-5f56-4a38-b838-de776fd4138c&displaylang=en).

Microsoft Windows Installer 4.5 is available as a redistributable system component for Microsoft Windows Server 2003 SP2, Microsoft Windows Vista, Microsoft Windows Vista SP1, and Windows Server 2008 (64-bit). You can download these from the Microsoft Download Web site. (http://www.microsoft.com/downloads/details.aspx?FamilyId=5A58B56F-60B6-4412-95B9-54D056D6F9F4&displaylang=en).

1. Log in as an administrator.
2. Launch the command prompt.
3. Browse to the location where you have saved the Novell SecureLogin installer package.
4. Run `Novell SecureLogin.msi`.

The installation options are detailed in the following sections:

- Novell SecureLogin Properties and Values
- Windows Installer Command Line Options

Novell SecureLogin Properties and Values

22

Use the following property values install Novell SecureLogin.

22.1 Installing in eDirectory Environment

Table 22-1 *Command Options for Installing in eDirectory Environment*

Installation Mode	Command Line Parameters	Description
eDirectory™ in NDS® GINA mode	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=EDIR PROTOCOLFOREDIR=NDS`	Use this command to install Novell SecureLogin in Graphical Identification and Authentication (GINA) mode on eDirectory.
eDirectory in LDAP GINA Mode	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=EDIR PROTOCOLFOREDIR=LDAP LDAPMODE=GINA LDAPSERVERADDRESS=192.168.1.255`	Use this command to install Novell SecureLogin in LDAP GINA mode on eDirectory. The default port is 636. To add another port, include the `LDAPPORT` in the command line. For example, `msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=EDIR PROTOCOLFOREDIR=LDAP LDAPMODE=GINA LDAPSERVERADDRESS=192.168.1.255 LDAPPORT=389`

Installation Mode	Command Line Parameters	Description
eDirectory in LDAP Credential Mode	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=EDIR PROTOCOLFOREDIR=LDAP LDAPMODE=CRED LDAPSERVERADDRESS=192.168.1.255`	Use this command to install Novell SecureLogin in Credential Provider mode on eDirectory. The default port is 636. To add another port, include the `LDAPPORT` in the command line. For example, `msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=EDIR PROTOCOLFOREDIR=LDAP LDAPMODE=CRED LDAPSERVERADDRESS=192.168.1.255 LDAPPORT=389`
eDirectory in LDAP Application Mode	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=EDIR PROTOCOLFOREDIR=LDAP LDAPMODE=APP LDAPSERVERADDRESS=192.168.1.255`	Use this command to install Novell SecureLogin in LDAP Application Mode on eDirectory. The default port is 636. To add another port, include the `LDAPPORT` in the command line. For example, `msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=EDIR PROTOCOLFOREDIR=LDAP LDAPMODE=APP LDAPSERVERADDRESS=192.168.1.255 LDAPPORT=389`

22.2 Installing in LDAP v3 (non-eDirectory) Environment

Table 22-2 *Command Options for Installing in LDAP v3 (non-eDirectory) Environment*

Installation Mode	Command Line Parameters	Description
LDAP GINA Mode	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=LDAP LDAPMODE=GINA LDAPSERVERADDRESS=192.168.1.255`	Use this command to install Novell SecureLogin in GINA mode on any LDAP-compliant directories (non-eDirectory). The default port is 636. To add another port, include the `LDAPPORT` in the command line. For example, `msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=LDAP LDAPMODE=GINA LDAPSERVERADDRESS=192.168.1.255 LDAPPORT=389`
LDAP Credential Mode	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=LDAP LDAPMODE=CRED LDAPSERVERADDRESS=192.168.1.255`	Use this command to install Novell SecureLogin in Credential Provider mode on any LDAP-compliant directories (non-eDirectory). The default port is 636. To add another port, include the `LDAPPORT` in the command line. For example, `msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=LDAP LDAPMODE=CRED LDAPSERVERADDRESS=192.168.1.255 LDAPPORT=389`

Installation Mode	Command Line Parameters	Description
LDAP Application Mode	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=LDAP LDAPMODE=APP LDAPSERVERADDRESS=192.168.1.255`	Use this command to install Novell SecureLogin in LDAP Application Mode on any LDAP-compliant directories (non-eDirectory). The default port is 636. To add another port, include the `LDAPPORT` in the command line. For example, `msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=LDAP LDAPMODE=APP LDAPSERVERADDRESS=192.168.1.255`

22.3 Installing in Microsoft Active Directory Environment

Table 22-3 *Command Options for Installing in Active Directory* Environment*

Installation Mode	Command Line Parameters	Description
Complete install	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE="MAD"`	Use this command to install Novell SecureLogin on Microsoft Active Directory, without prompting users for any selection.
With group policies enabled	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE="MAD" X_USEGPO="Yes"`	Use this command to install Novell SecureLogin on Microsoft Active Directory with support for group policy. This command does not display any user interface to the users.

22.4 Installing in Active Directory Application Mode Environment

Table 22-4 *Command Options for Installing in Active Directory Application Mode* Environment*

Installation Mode	Command Line Parameters	Description
Complete install	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE="ADAM"`	Use this command to install Novell SecureLogin on Microsoft Active Directory Application Mode, without prompting users for any selection.

Installation Mode	Command Line Parameters	Description
With group policies enabled	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE="ADAM" X_USEGPO="Yes"`	Use this command to install Novell SecureLogin on Microsoft Active Directory Application Mode with support for group policy. This command does not display any user interface to the users.

22.5 Installing in Standalone Environment

Table 22-5 *Command Options for Installing in Standalone Mode*

Installation Mode	Command Line Parameter	Description
Complete install	`msiexec /i "Novell SecureLogin.msi" /qn X_INSTALLTYPE=STANDALONE`	Use this command to install Novell SecureLogin in a standalone mode, without any user interface.

22.6 Command for Installing the Features

When installing Novell SecureLogin, you can choose to install various features such as Secure Workstation, support for smart card, and support for Citrix.

Use the following table as reference to specify these features when installing Novell SecureLogin.

Table 22-6 *Commands for Installing Features*

Command Line Parameters	Value	Description	Example
`X_USEGPO`	Yes	This is applicable only in Active Directory and ADAM modes of installation. Use this property to use the group policy object option.	`X_USEGPO="Yes"`

Command Line Parameters	Value	Description	Example
X_SMARTCARD	Yes	Installs smartcard support.	X_SMARTCARD="Yes" Smart card support is installed only if ActivIdentity* ActivClient* is detected on the machine. Set the cryptographic service provider and smart card DLL file by defining the X_CSP and X_SMARTCARDLIB properties. X_CSP="ActivCard Gold Cryptographic Service Provider" X_SMARTCARDLIB="C:\Windows\System32\ACPKCS211.dll"
X_INSTALLCITRIX	Yes	Installs Citrix support.	X_INSTALLCITRIX="Yes"
LDAPPORT	port address	Specifies the LDAP port address.	LDAPPORT=389
PCPROX	1 Do not set any value if you do not want to use pcProx.	Installs pcProx.	PCPROX=1
SW_INST	Yes Do not set any value if you do not want to install SecureWorkstation.	Installs SecureWorkstation.	SW_INST=Yes
X_INSTALLADMIN	Yes	Specifies installing the directory administration tools.	X_INSTALLADMIN=Yes
X_RUNATSTARTUP	Yes	Specifies whether Novell SecureLogin must run at startup or not.	X_RUNATSTARTUP=Yes
X_SMARTCARDLIB		Specifies the PKCS#11 encryption library to use. The value is supplied as the name of the desired DLL file.	X_SMARTCARDLIB="C:\Resources\acpkcs201rc.dll"

Command Line Parameters	Value	Description	Example
X_CSP		Specifies a cryptographic service provider. It is typically a string constant from HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider.	X_CSP="ActivCard Gold Cryptographic Service Provider"

22.7 Examples

This section lists some examples that you can use in your environment.

- Selecting Mode and Feature
- Installing with User Interface Option

Selecting Mode and Feature

The following example installs SecureLogin in the following setup.

- Microsoft Active Directory mode
- Support for Group Policy
- SecureLogin is not launched at the completion of the installation

```
msiexec /qb /i "C:\Novell SecureLogin.msi" X_INSTALLTYPE="MAD" X_USEGPO="Yes"
```

Installing with User Interface Option

The following example installs SecureLogin in the following setup.

- eDirectory mode.
- With administration tools, support for smartcard (using ActivClient default settings), and Group Policy.
- SecureLogin is not launched at the completion of the installation
- User is prompted to restart after the installation is complete.

```
msiexec.exe /qb /i "C:\Novell SecureLogin.msi" X_INSTALLTYPE="EDIR"
X_INSTALLADMIN="Yes" X_USEGPO="Yes" X_SMARTCARD="Yes"
X_USEACTIVCLIENTDEFAULTS="Yes"
```

22.8 Silent Install

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

A response file is a text file (`responsefile.ini`) containing sections and keys. 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.

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.

For instance,

- An administrator runs the graphical installer on a single machine. During the install, the administrator selects the configuration he or she wants to roll out to the machines of the target users.
- At the end of the installation a response file is created and available located in `<windows Volume>\NSLFiles`. It contains the command line properties required to replicate the graphical installation the administrator has done.
- The administrator can take this response file and copy it to the target machines or to a mapped network drive for use with target machine installs.
- The administrator runs command line installs on all of the target machines using the following command pointing to the newly created response file:

  ```
  msiexec /i "Novell SecureLogin.msi" PATHTOISS="c:\temp\response.ini"
  ```

If you use the command line installation with a response file on Microsoft Windows Vista* platform, disable the User Access Control before starting the install.

You can create a new response file or edit one from a previous installation. During the installation, the responsefile.ini is created in the `<WindowsVolume>\NSLFiles` folder. It is recommended that you do not modify the `responsefile.ini`.

22.8.1 Example of a Response File

The following is an example of a response file.

```
INSTALLDIR=C:\Program Files\Novell\SecureLogin\

X_CACHEDIR=%APPDATA%

X_INSTALLTYPE=EDIR

PROTOCOLFOREDIR=LDAP

X_USEGPO=

IS_SECRETSTORE=

NMASCLIENT=

LDAPCREDASSOC=

LDAPMODE=APP

LDAPSERVERADDRESS=192.168.1.255

LDAPPORT=636

PCPROX=0
```

```
SW_INST=Yes

X_SMARTCARD=No

X_SMARTCARDLIB=C:\Windows\system32\

X_CSP=

X_RUNATSTARTUP=

X_INSTALLADMIN=Yes

X_INSTALLCITRIX=Yes

DAS_INST=Yes

LOCATIONFORXML=Local

DASSERVER=Tree/Server IP

DASCONFIGOBJECT=cn=ARSConfig.o=system

READERPORT=-1

CARDREADER=1

AIRID=0

RETRIES=0

TREE=defaulttree

SERVER=ldapserveraddress

SEQUENCE=

LDAPSERVER=ldapserveraddress

ALTERNATE1=

ALTERNATE2=
```

Windows Installer Command Line Options

23

Table 23-1 on page 159 lists the Windows Installer command-line options used to manually install, uninstall, and configure software and components.

Table 23-1 *Windows Installer Command Line Options*

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.
/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)

Parameters listed in might be relevant in enterprise environments where the administrators control the installation; however, users can still see the product being installed.

Table 23-2 *Other Install Options*

Install Options	Usage
/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

23.1 Switches Supported by SLProto.exe

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

Table 23-3 *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.

Installing, Configuring, and Deploying Desktop Automation Services

VIII

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 productivity improvements.

Installing Desktop Automation Services

24

This section covers the following topics:

24.1 Overview

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 action triggers such as hot keys provides tremendous flexibility to change the behavior of the workstation to fit your needs.

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.

NOTE: If you have an earlier version of DAS or ARS installed on your workstations, uninstall these versions prior to installing the new version of DAS.

24.1.1 Changes from the Previous Version

In comparison to DAS 2.0, which was a standalone release, some of the install features such as *Disk Cost* and *Install Desktop Automation Services for yourself, or for anyone who uses this computer* are removed from the user interface. They are handled internally.

24.2 Installing in a Novell eDirectory 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 Installation Wizard for Novell SecureLogin is displayed.

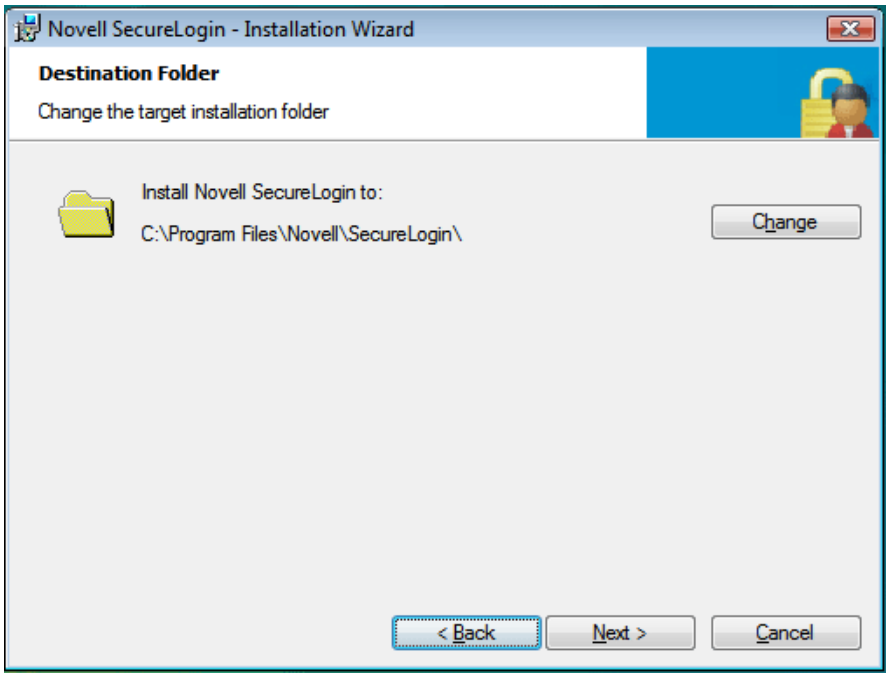
3 Click *Next*. The License Agreement page is displayed.

The Destination Folder page is displayed. By default, the program is saved in `C:\Program Files\Novell\SecureLogin\`.

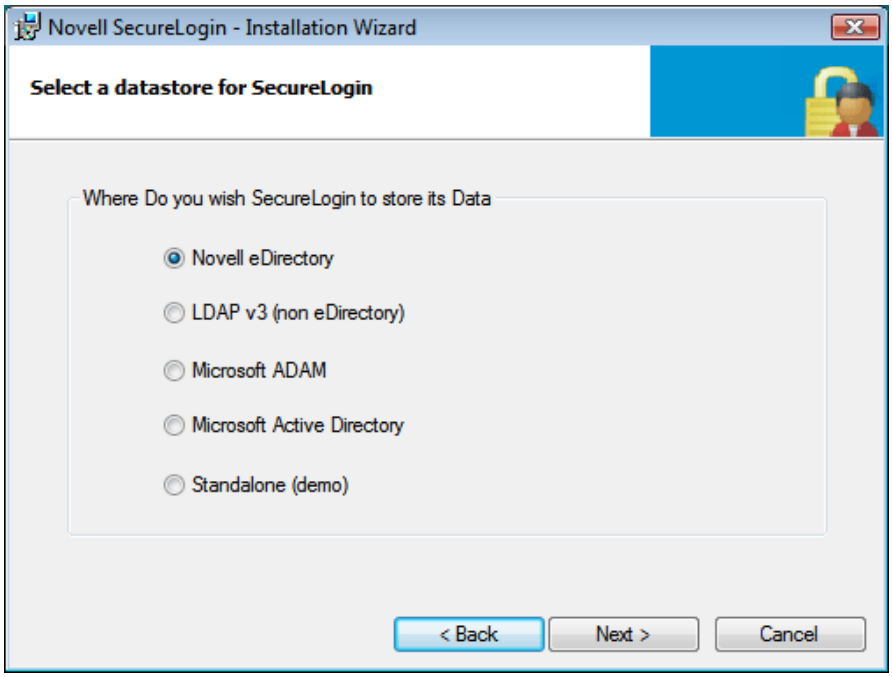
4 Accept the default folder

or

Click *Change* and navigate to your desired folder.



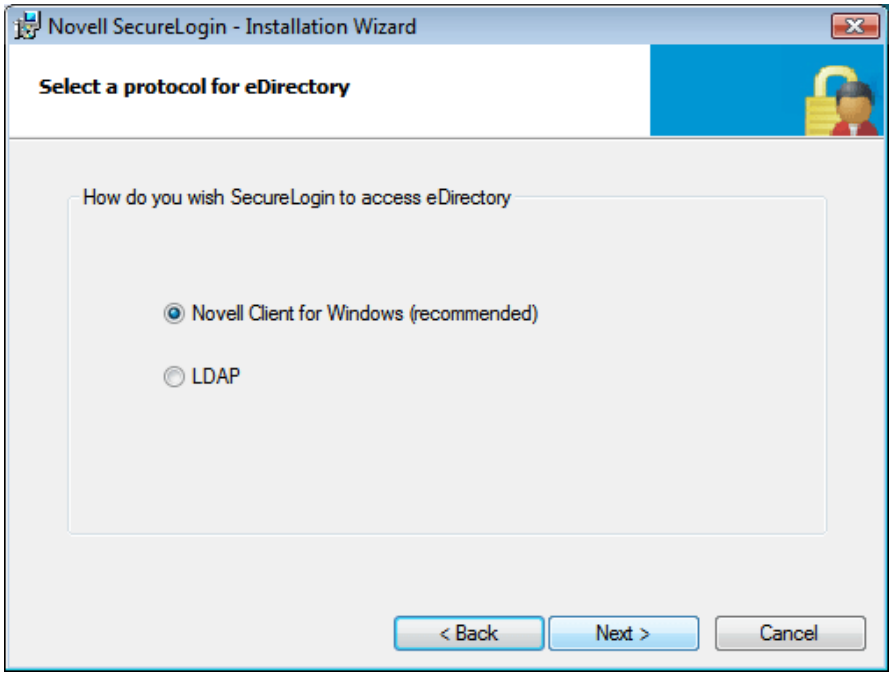
5 Select Novell eDirectory as the directory where Novell SecureLogin stores its data.



6 Click *Next*. The protocols page is displayed

7 Select how you want Novell SecureLogin to access eDirectory.

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



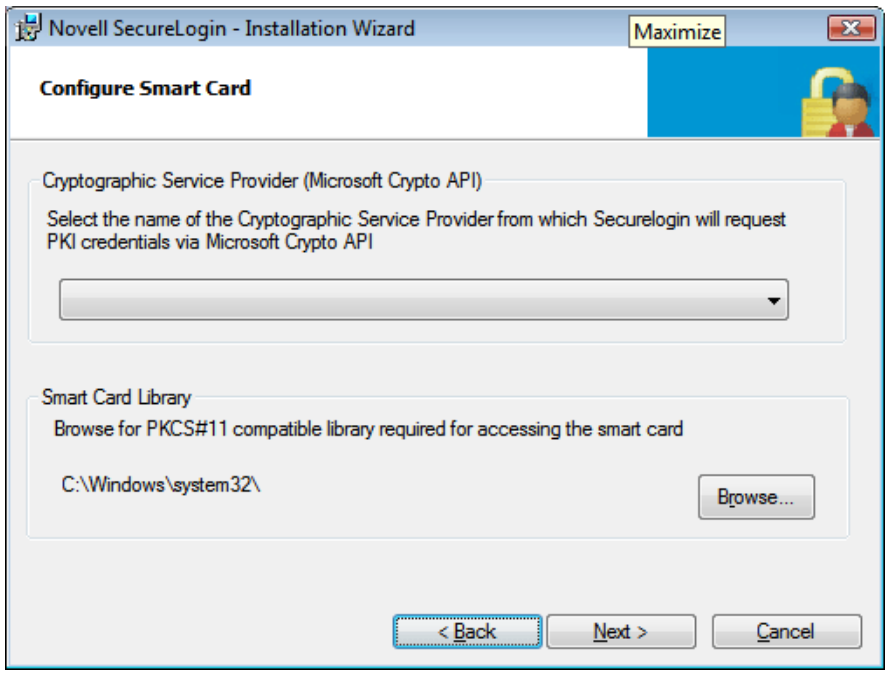
This dialog box is displayed only if you have Novell Client for Windows installed on your machine. Otherwise, LDAP is auto-selected as the protocol.

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

9 Click *Yes* if you want to use a smart card. If you do not want to use a smart card, 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*.



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.

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

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

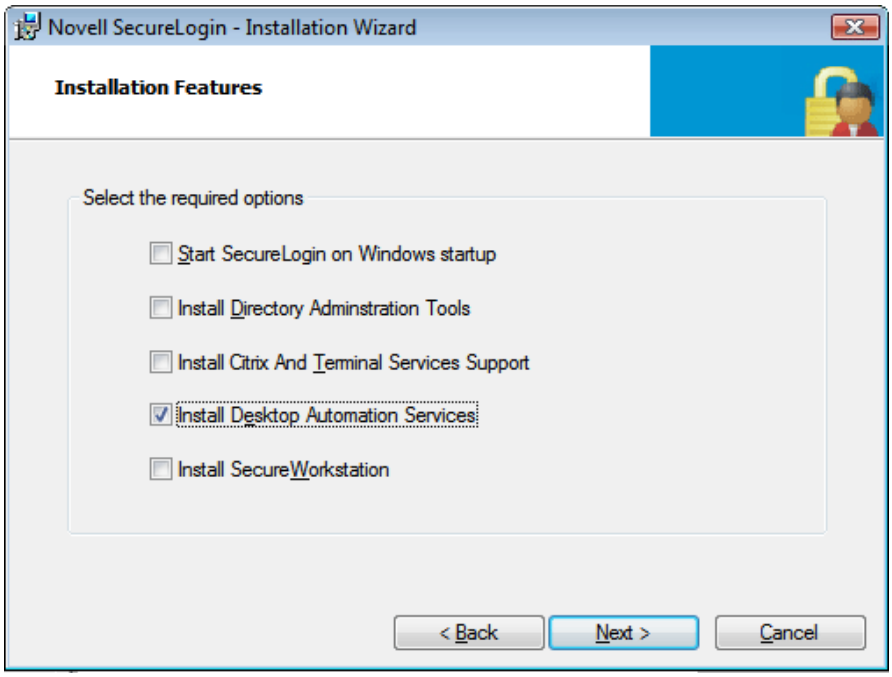
You can select both *Novell SecretStore Client* and *Novell NMAS Methods*.

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

13 Select the NMAS Methods.

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

15 Select *Install Desktop Automation Services*.



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

DAS handles starting and stopping for Novell SecureLogin.

16 Click *Next*. The location for the 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 *Directory*, the `actions.xml` file is managed through eDirectory as described in Section 25.3, “Managing the actions.xml File through eDirectory and iManager,” on page 181. Because you have installed DAS on eDirectory, you can store the configuration file in the directory.

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.

When you install DAS in eDirectory™ mode with the Novell® Client™, you might see an error indicating `Error in parsing xml file during install` appears. This occurs because the server or the specified config object is invalid.

To fix the problem, ignore the message and proceed with the install. After the installation or restart;

1 Log in as an administrator.

2 Set the `ConfigObject` and `ConfigTree` registries values correctly.

The `ConfigObject` is the ArsControl Object and `ConfigTree` - Server or the Tree information. The registry settings are at `HKLM\Software\Novell\Login\ARS`.

3 Run `ARSControl /RegServer`.

24.3 Installing in Other LDAP Environments

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 Installation Wizard for Novell SecureLogin is displayed.

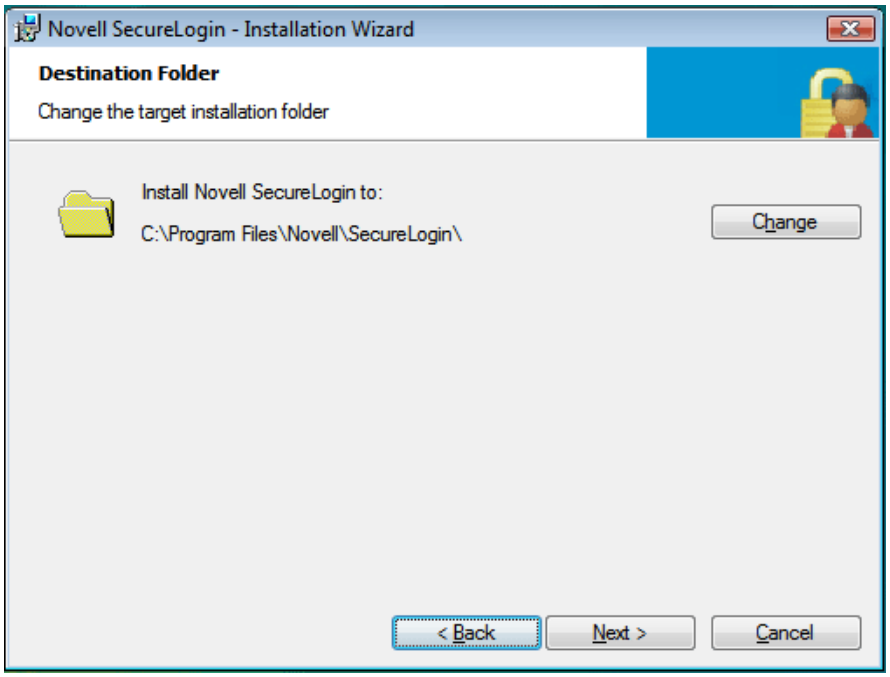
3 Click *Next*. The License Agreement page is displayed.

The Destination Folder page is displayed. By default, the program is saved in `C:\Program Files\Novell\SecureLogin\`.

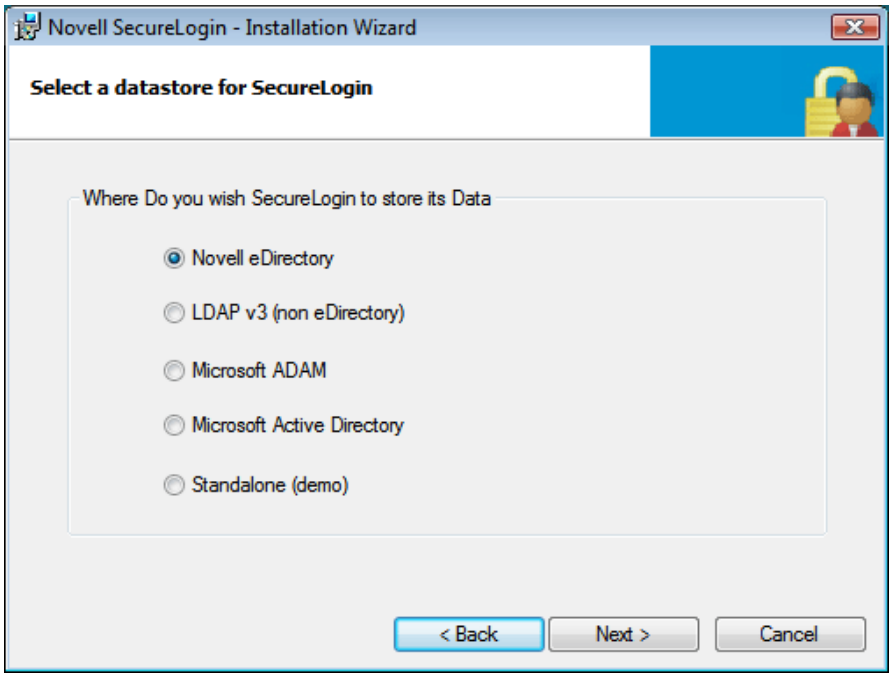
4 ccept the default folder.

or

Click *Change* and navigate to your desired folder.



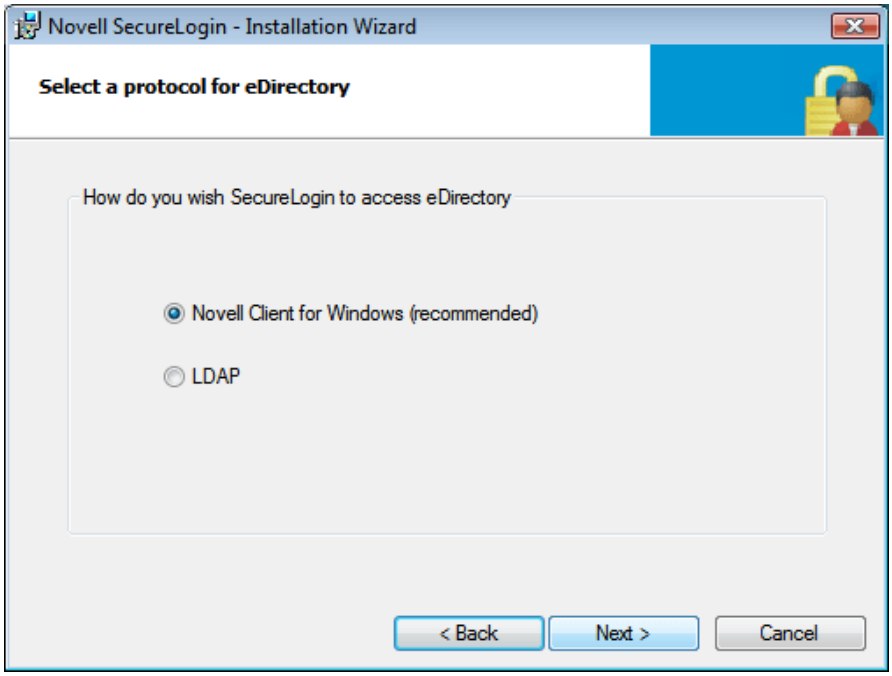
5 Select Novell eDirectory as the directory where Novell SecureLogin stores its data.



6 Click *Next*. The protocols page is displayed

7 Select how you want Novell SecureLogin to access eDirectory.

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



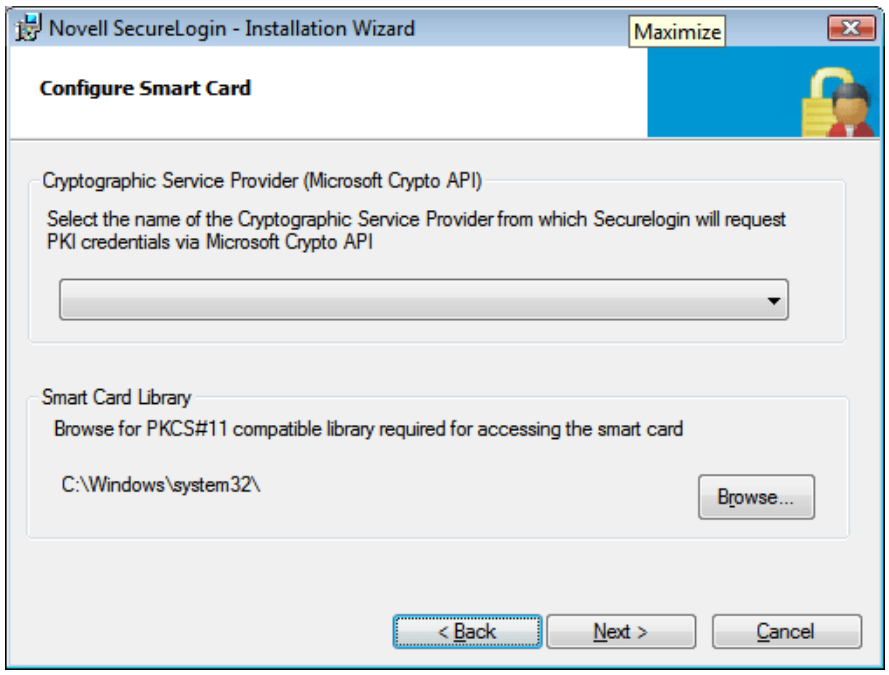
This dialog box is displayed only if you have Novell Client for Windows installed on your machine. Otherwise, LDAP is auto-selected as the protocol.

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

9 Click *Yes* if you want to use a smart card. If you do not want to use a smart card, 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*.



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.

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

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

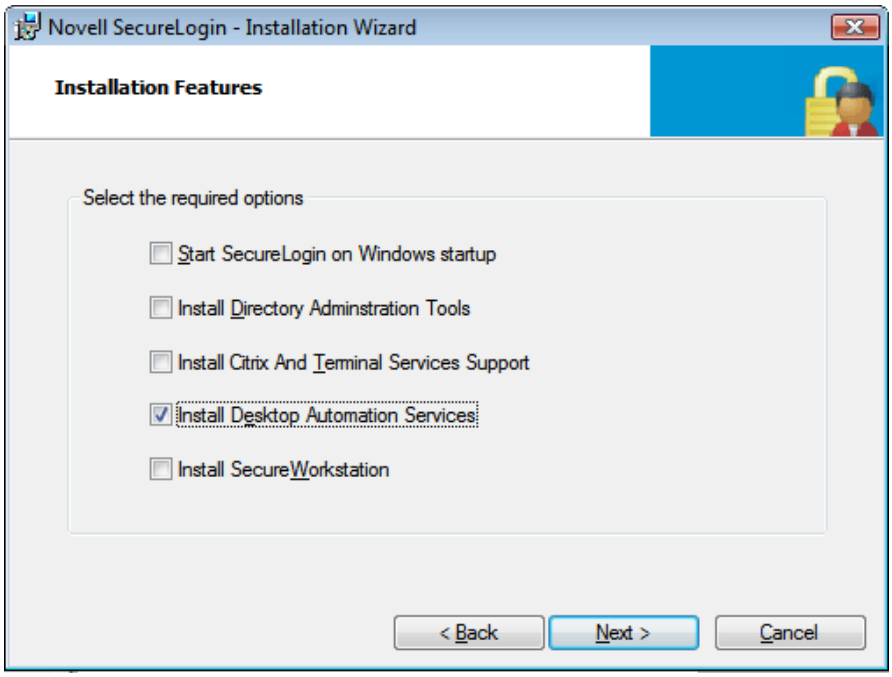
You can select both *Novell SecretStore Client* and *Novell NMAS Methods*.

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

13 Select the NMAS Methods.

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

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



16 Click *Next*. The location for the 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.

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.

24.4 Installing in Active Directory, ADAM, or Standalone Environments

With this release of Novell SecureLogin, you can install DAS in Active Directory* mode, as well as in ADAM mode and standalone 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 Installation Wizard for Novell SecureLogin is displayed.

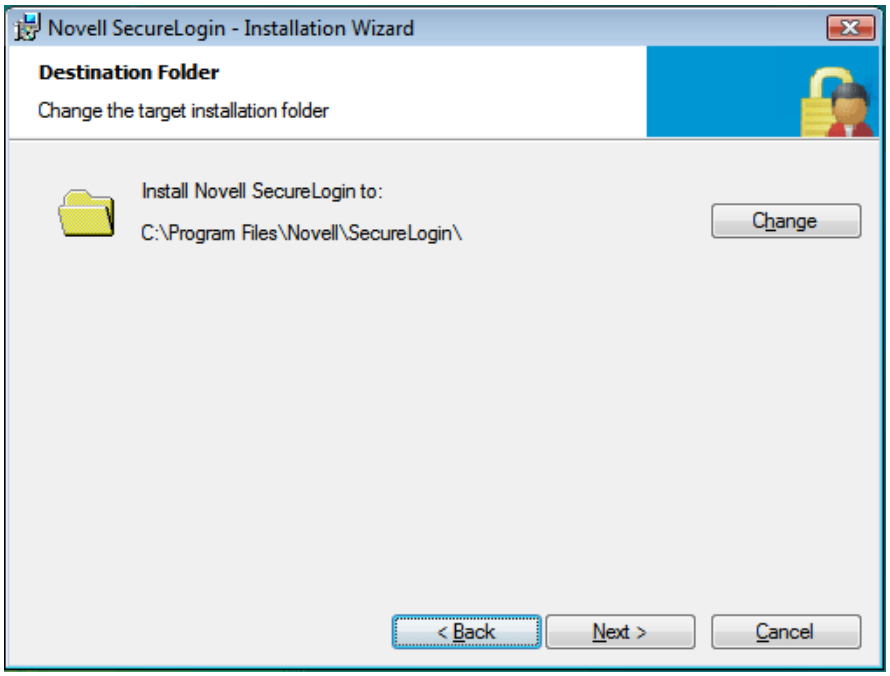
3 Click *Next*. The License Agreement page is displayed.

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..

4 Accept the default folder. or choose to change. To change, click *Change* and navigate to your desired folder.

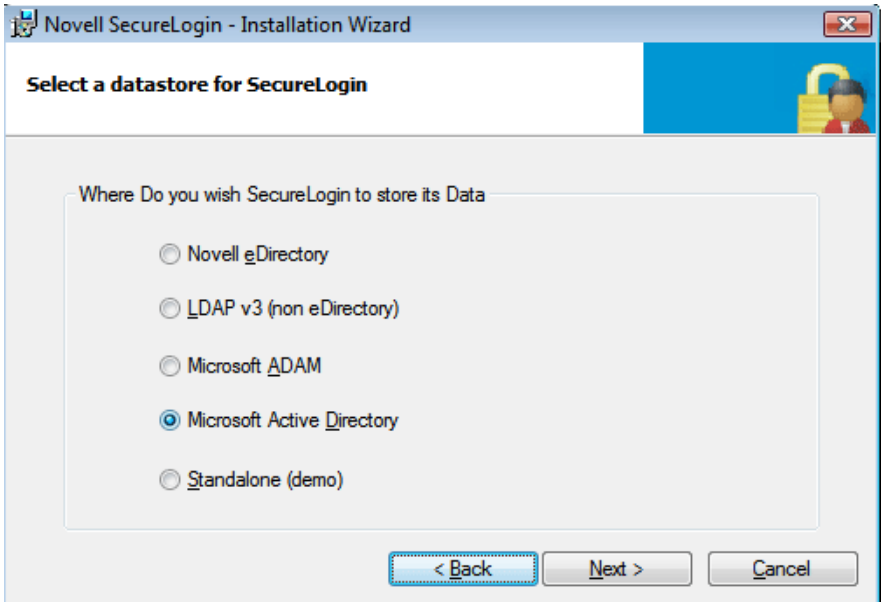
or

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.

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.

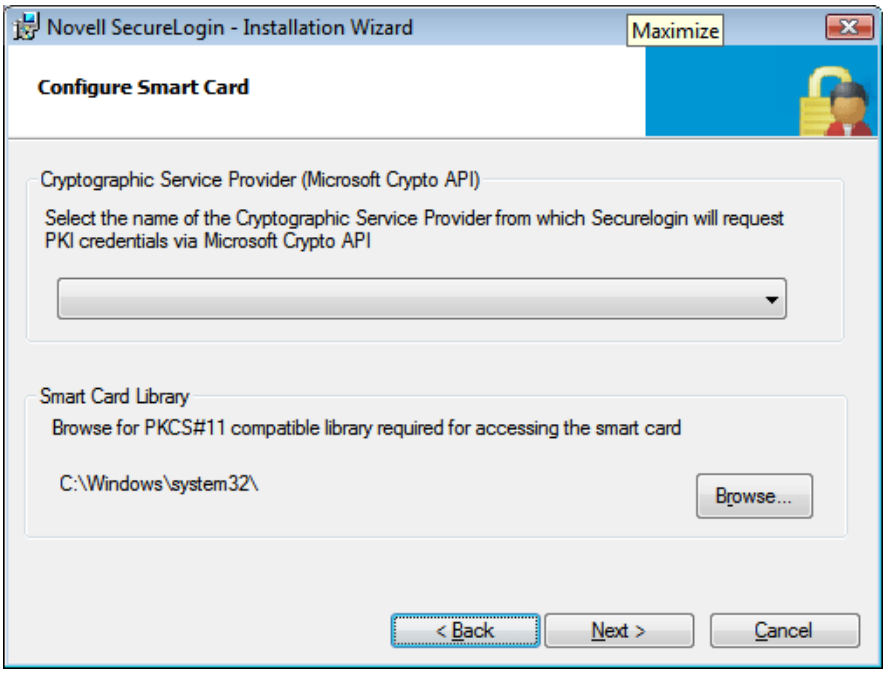
- If you select *After successfully logging into Windows*, you are prompted to associate the login user with your LDAP distinguished name.
- If you select *When SecureLogin starts*, you are prompted to specify the LDAP server information.

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

9 Click *Yes* if you want to use a smart card. If you do not want to use a smart card, 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*.



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.

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

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

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

DAS handles starting and stopping for 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.

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

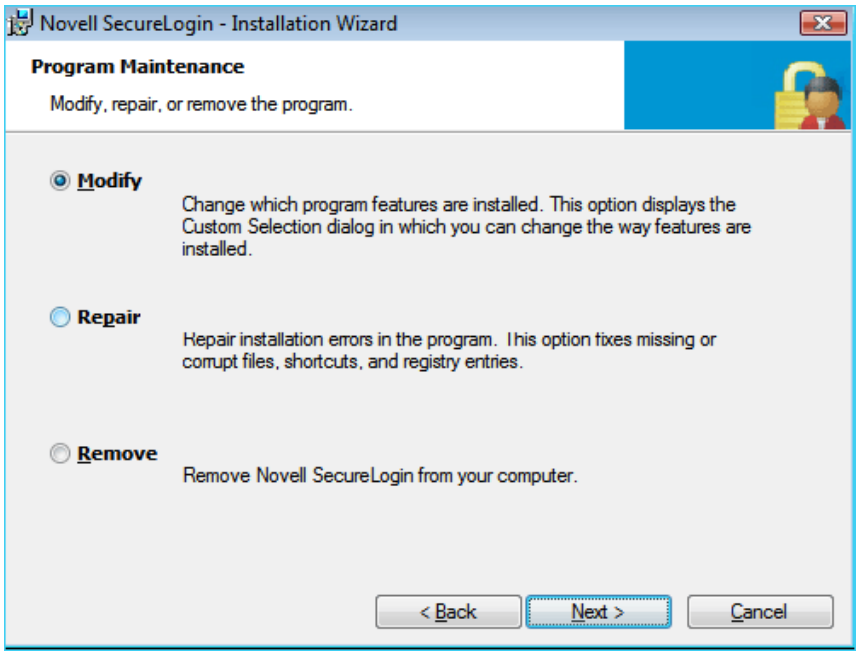
15 Click *Install*.

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

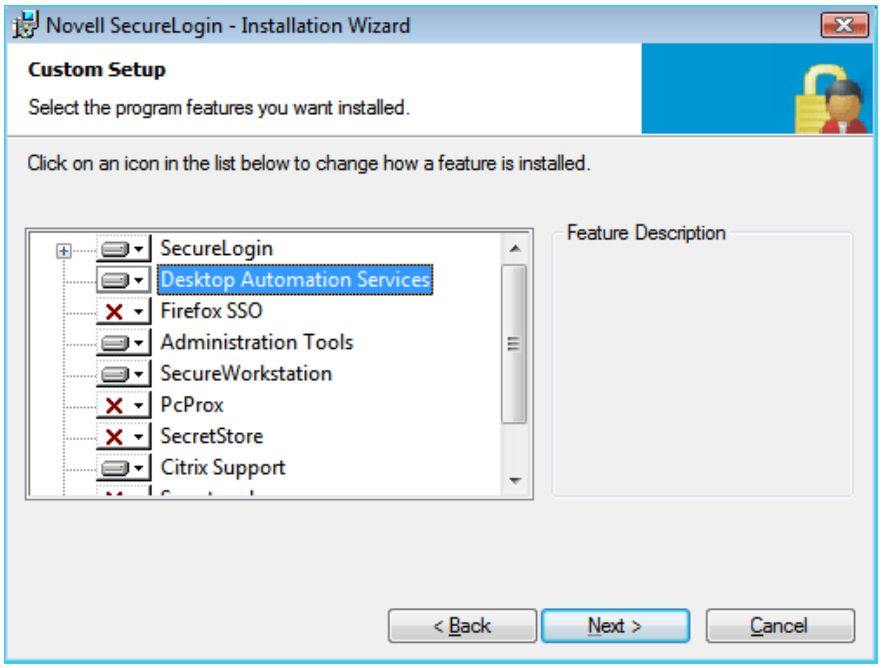
17 You are prompted to restart your system. Select *Yes* to restart the system for Desktop Automation Services to take effect.

24.5 Installing by Using the Modify Option

1 Launch Novell SecureLogin after you have successfully upgraded to or installed version 7.0. 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.

DAS is installed in the same folder as Novell SecureLogin 7.0. 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 179.
- For information on modifying the ConfigTree registry key, see "ConfigTree" on page 180.

24.6 Accessing DAS

After you install DAS, the services are available individually or in combination through a DAS executable that can be accessed from any scripting interface available on Microsoft Windows, such as VBScript, JavaScript, login scripts, and batch files.

24.6.1 Accessing DAS 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.

24.6.2 Accessing DAS through VBScript

```
<SCRIPT LANGUAGE = "VBScript">

      Sub physiciansApps

      Dim as

            Set as = CreateObject("ARS.Control")

            ars.Execute("Run Physicians Applications")

      End Sub

</SCRIPT>
```

24.6.3 Accessing DAS through 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</a>
  ```

- 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 Internet Explorer 6.0 or later. To avoid the warning, select *Tools* > *Internet Options* > *Advanced* within Internet Explorer. Scroll down to the *Security* tab and select *Allow active content to run in files on My Computer*, then click *OK*.

24.6.4 Accessing DAS 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
```

24.7 Tips for Installing DAS

Following are some tips that can help in the installation of DAS:

- You can refresh the DAS configuration through the command line by using the `ARS/refresh` command. For example, `ARS.exe/refresh` refreshes `ARS.exe`.

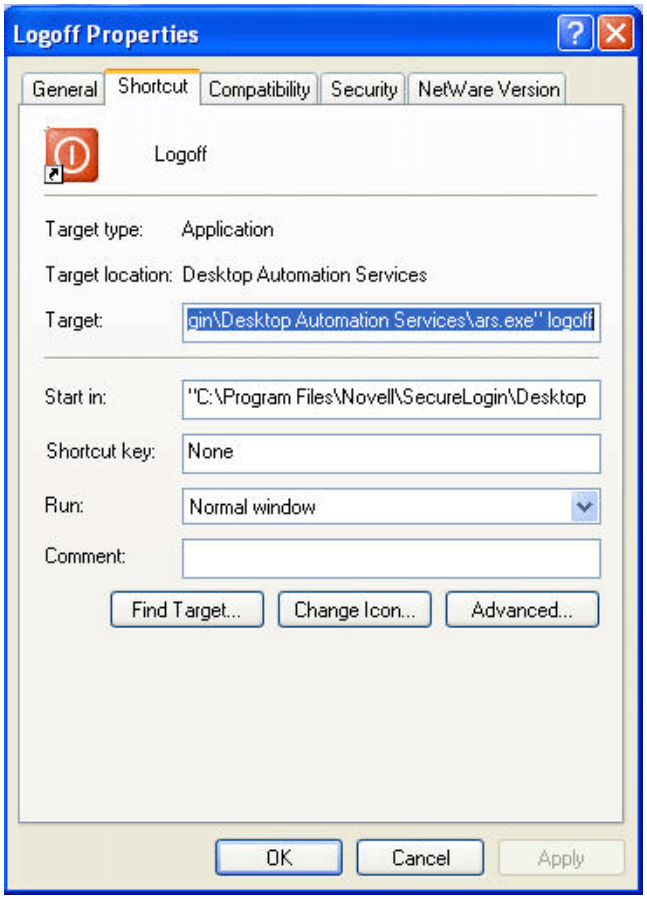
  The other way to refresh the DAS configuration is to restart the `ARSControl.exe` process or reboot the workstation.

  `The ARS/refresh` command is better for managing 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 byusing 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 in order to have special use cases and common workstations pointing to eDirectory.
- Set up eDirectory and iManager after you have stabilized your `actions.xml` file and want to centrally manage the configuration file. For more information, see Section 25.3.1, “Extending the Schema for eDirectory,” on page 181 and Section 28.3, “Installing the Plug-Ins for iManager,” on page 192.
- 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 toolbar and provide a logout icon on the desktop for the convenience of users. You can also provide a hot key combination such as Ctrl+L.

  For example, you can use a shortcut target =“`C:\Program Files\Novell\SecureLogin\Desktop Automation Services\ARS.exe`” logoff. This is your shortcut properties target setting.

Figure 24-1 *Logoff Shortcut Option*



Configuring

25

This section contains the following topics:

25.1 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 dependon the log level that is set.
LogLevel	dword:00000001 The value is the default value.	See Section 25.2, "Logging and Error Notification," on page 180 for the possible settings for this value.

25.2 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 enter 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	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	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	Adds basic information to the log. This information records the actions created from the configuration XML parse operation.
Verbose	4	Produces the maximum output in the log file. Use this only to troubleshoot an existing ARSControl problem or during the development phases of a configuration file.

25.3 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:

- Section 25.3.1, "Extending the Schema for eDirectory," on page 181
- Section 25.3.2, "Setting Workstation Registry Settings," on page 181
- Section 25.3.3, "Loading the actions.xml File to eDirectory," on page 182

25.3.1 Extending the Schema for eDirectory

1. Locate the `ARSControl.sch` file 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 scema extension procedure see the *Novell eDirectory 8.8 Administration Guide* at the Novell Documentation Web site. (http://www.novell.com/documentation/edir88/index.html)

25.3.2 Setting Workstation Registry Settings

You can configure `ARS.exe` through the Windows registry settings to know where to locate the `actions.xml` configuration file. For information on where the registry keys are stored, see Section 25.1, "Editing Environment Registry Keys," on page 179.

To help you set the registry settings to manage the `actions.xml` file on the eDirectory, the sample registry setup files are located in the `C:\Program Files\Novell\SecureLogin\Desktop Automation Services\Tools` folder.

1. Open `ARS eDir Config.reg`, which is located in the `Tools` folder. You can edit this file by using an editor such as Notepad to set the correct directory setting for your environment.
2. Save the changes.
3. To apply these changes, double-click `ARS eDir Config.reg`.

   If you are prompted to apply the changes, click *Yes*.
4. Verify that the changes are applied.

   After the registry settings are set, the `ARS.exe` points to eDirectory on startup for its `actions.xml` file.

25.3.3 Loading the actions.xml File to eDirectory

The `das.npm` file must be loaded for you to manage the `actions.xml` file in iManager 2.6 and later. The `das.npm` fileis located in the iManager folder of the installer package.

1. Launch iManager.
2. Log in by using your username, password, and eDirectory tree name.
3. Under *Roles and Tasks*, select *DAS Management > Create Configuration*.

   If you are modifying an existing `actions.xml` file, select *Modify Configuration*.
4. Specify the distinguished name (DN) for ARSConfig. The iManager entry is displayed with the contents of the `actions.xml` file.
5. Cut and paste the `actions.xml` text to the browser window.
6. Click *OK* to save the changes.
7. Click *Apply* to apply the changes and exit.

Deploying

26

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.

26.1 Best Practices

When deploying DAS, we recommend that you read and follow the best practices listed here:

- Develop specific use case scenarios with the users on multi-user workstations.
- If you are currently using network login scripts, 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 logout event.
- If a use case requires applications to be shut down as part of user logout or a time-out event, access each applicationcarefully to ensure that Desktop Automation Service does not have any adverse effect in the application sessions. For example, terminal emulator sessions or unsaved logout (graceful logout).

  Analyze each application to determine the best way to handle a fast shutdown.
- When updating `actions.xml` files, if you want to activate the latest changes without rebooting 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`

26.2 Common Debug Issues

Following are some of the common debug issues that you might encounter when deploying DAS:

- The action names are case-sensitive. Ensure that you follow a common naming convention, such as always using lowercase.
- The `DASlog.txt` file 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 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 log level 4 because the file size is large.
- eDirectory can centrally store different workstation behaviors 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, you should provide a pause before forcing the shutdown.

  When DAS tries to shut down the ICA Client, it sends a WM_CLOSE message to the Citrix* client. The Citrix client resends the message to the published application t If there is a timeout or if the application is slow to respond, DAS quickly forces the shutdown and does not allow the Citrix application to gracefully shut down. 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. There might be some timing issues with certain event executions, so you should ensure that you set the correct values for the serial = true or false parameters.

Installing Secure Workstation 27

This section covers the following topics:

27.1 Overview

Secure Workstation is a post-login method.

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.

Supported Versions

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

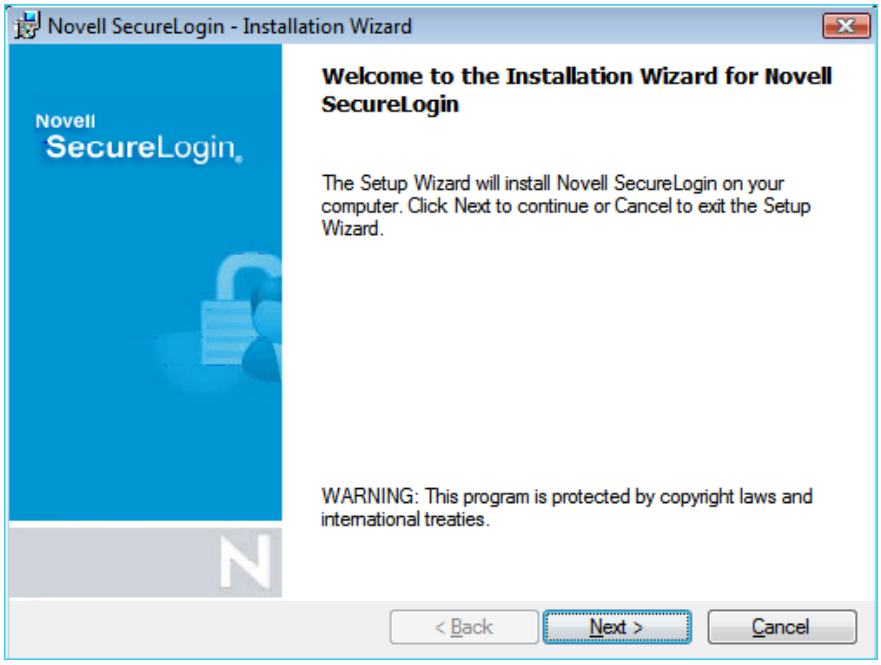
27.2 Installing Secure Workstation through the Modify Option

If you did not select Secure Workstation during the parent install, you can choose to do it later.

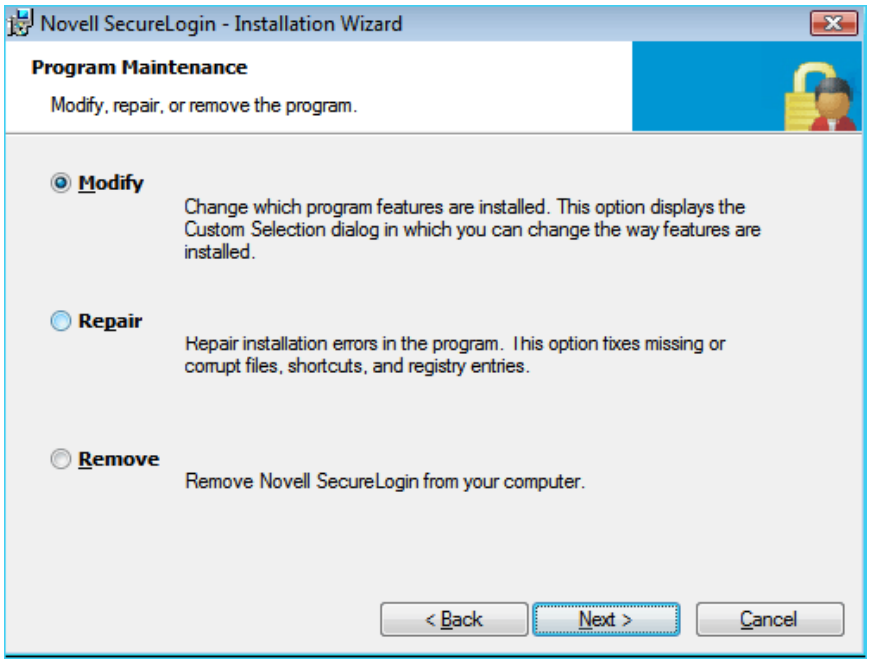
To add Secure Workstation after the parent install:

1 Run the `Novell SecureLogin.msi` found in the `SecureLogin\Client\x64` of the Novell SecureLogin 7.0 Windows Installer Package.

The Installation Wizard is launched.



If SecureLogin is already installed, InstallShield launches the Program Maintenance page.



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

3 Select *Secure Workstation*, then click *Next*.

4 Click *Install*.

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

Installing iManager Plug-Ins

IX

This section explains the process for installing Novell® iManager plug-ins for SecureLogin.

Accessing iManager and Installing the iManager Plug-In

28

Novell SecureLogin 7.0 supports iManager 2.7.2. The plug-in for iManager 2.7 are available as part of the Novell SecureLogin Windows Installer Package. They are located in the `IManager\2.7` folder of the product installer package.

NOTE: Novell SecureLogin 7.0 includes the plug-in for Desktop Automation Services (`das.npm`)

28.1 Accessing iManager

Accessing iManager varies based on the iManager version (server-based or workstation) and the platform on which iManager is running.

28.1.1 Accessing Server-based iManager

To access server-based iManager:

1. Enter one of the following in the Address (URL) field of a supported Web browser.

   1a. Because iManager 2.7 uses only Tomcat 5 for its Web server requirements, on platforms other than Novell Open Enterprise Server 2 (OES 2) you must specify the Tomcat port as part of the iManager URL. The default URL to start iManager 2.7 is as follows:

   - **Secure URL:** `https://<server ip address>:8443/nps/iManager.html`

   iManager 2.7 on the OES 2 platform, both Linux and NetWare, use the following default iManager URL:

   - **Secure URL:** `https://<server ip address>/nps/iManager.html`

   Although slightly different iManager URLs might work on some platforms, Novell recommends using these URLs for consistency.

2. Log in by using your username, password, and the treename.

28.1.2 Accessing iManager Workstation

To access iManager Workstation:

1. Browse to the iManager set up on your workstation.
2. Execute `imanager\bin\iManager.bat`.
3. Log in by using your username, password and treename.

28.2 iManager Plug-In

Novell iManager is a state-of-the-art Web-based administration console that provides customized secure access to network administration utilities and content from any location in the world. With a global view of users' network from one browser-based tool, user can proactively assess and respond to changing network demands. Using iManager, user can administer Novell SecureLogin

The iManager plug-in for Novell SecureLogin are `.npm` files. A plug-in typically provides all the management functionality that a particular product, or feature set within a product, requires. It is assembled as a single file so you can quickly and easily add extend iManager to support the required management functionality.

The plug-in are:

28.2.1 Desktop Automation Services Plug-In

The Desktop Automation Services plug-in, `das.npm` is an add-on to Novell SecureLogin that handles unique use cases associated with shared workstations or kiosks (multiple users using the same workstation during the day). The most common deployment is to provide fast user switching in Clinical Workstation or single sign-on for health care solutions.

28.2.2 pcProx Plug-In

The pcProx plug-in, pcprox.npm is an NMAS log in method that allows you to use the pcProx card to identify to the network. You can also set or remove a pcProx card ID for use by a specific user to authenticate to the network.

28.2.3 SecretStore Plug-In

By using the SecretStore plug-in, `secretstore.npm` you can use a single authentication to Novell eDirectory to access most UNIX*, Windows, Web, and mainframe applications.

28.2.4 Single Sign-On Plug-In

The Single Sign-On plug-in, `sso.npm` manages the Novell SecureLogin data, which includes managing applications, logins, password policies, advanced settings, and distribution of Novell SecureLogin settings.

28.2.5 Secure Workstation Plug-In

The Secure Workstation plug-in, `sw.npm` allows you to configure secure workstation network policy for the NMAS sequence that has secure workstation post-login method configured.

28.3 Installing the Plug-Ins for iManager

The iManager plug-ins for Novell SecureLogin are:

- **Desktop Automation Services:** `das.npm`
- **SecretStore:** *secretstore.npm*

- **Single Sign-On:** `sso.npm`
- **pcProx:** `pcprox.npm`
- **Secure Workstation:** sw.npm

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*. A confirmation message is displayed after the plug-in is successfully installed.
4. Click *Close*.
5. Repeat Step 2 to Step 4 add the other npms.
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 iManager Documentation Web site. (http://www.novell.com/documentation/imanager27/imanager_install_27/index.html?page=/documentation/imanager27/imanager_install_27/data/alw39eb.html)

IMPORTANT: You must install the LDAP schema on the directory, after you have installed the plug-ins.

28.4 Installing NMAS Server Method for pcProx and Secure Workstation

When installing the NMAS Server Method for pcProx and Secure Workstation, it also installs the `pcprox.npm` and `sw.npm`. You need not install it separately.

1. To install, log in to iManager.
2. Select *NMAS* > *NMAS Login Methods* > *New*. The New Login Method page opens.
3. To install pcProx, browse and locate the `pcProx.zip` file containing the installation files for NMAS method that you want to install. This is found in `Nmas\NmasMethods\Novell\pcProx` found in the Novell SecureLogin Windows Installer Package.

   When installing the pcProx NMAS server method, 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 Secure Workstation, browse and locate the `SecureWorkstation.zip` file containing the installation files for NMAS method that you want to install. This is found in `Nmas\NmasMethods\Novell\SecureWorkstation` found in the Novell SecureLogin Windows Installer Package.

28.5 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 iManager 2.0 Documentation Web site. (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:

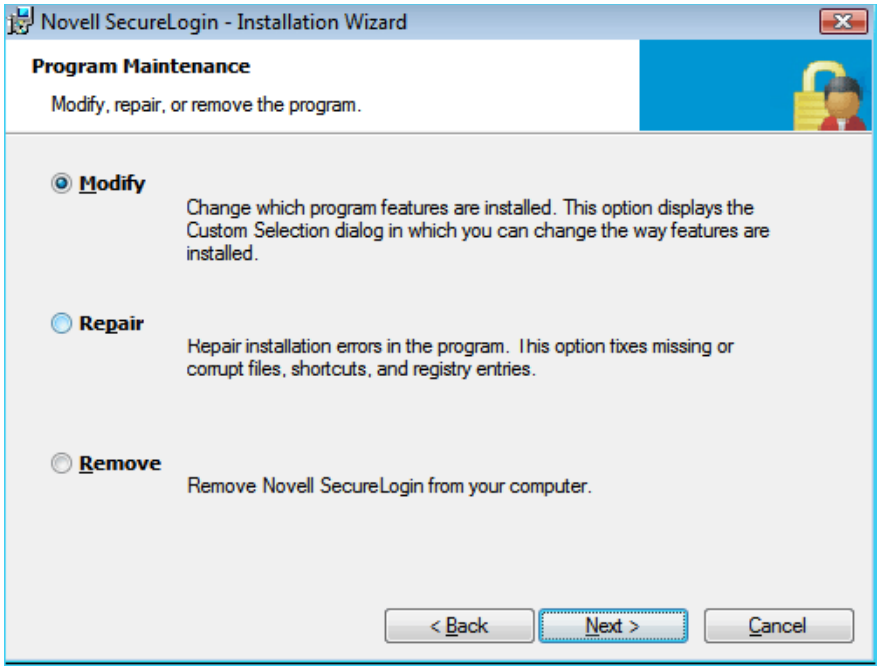
Table 28-1 *Scenarios*

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

Modifying, Repairing, or Removing an Installation

29

If you have Novell SecureLogin already installed, the Installation Wizard 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, restart your workstation (if you are prompted to restart), then reinstall Novell SecureLogin.

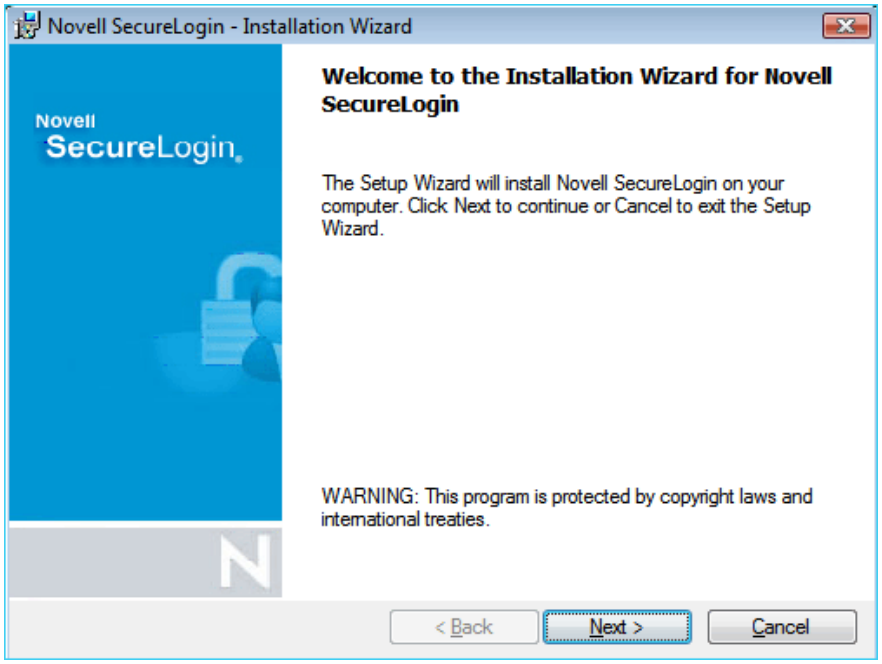
29.1 Using the Modify Option to Install Features of Novell SecureLogin

If you have not installed some of the features such as pcProx or Secure Workstation during the initial installation of Novell SecureLogin, you can to do it later through the *Modify* program..

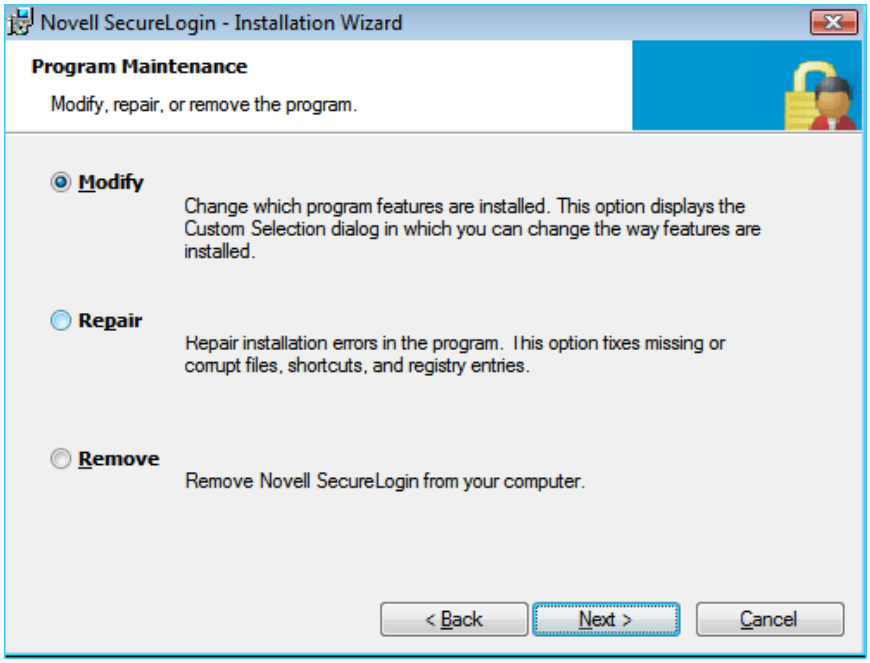
The following example explains installing pcProx through the Modify option.

1 Run the `Novell SecureLogin.msi` found in the `SecureLogin\Client\x64` folder of the Novell SecureLogin 7.0 Windows Installer Package.

The Installation Wizard is launched.

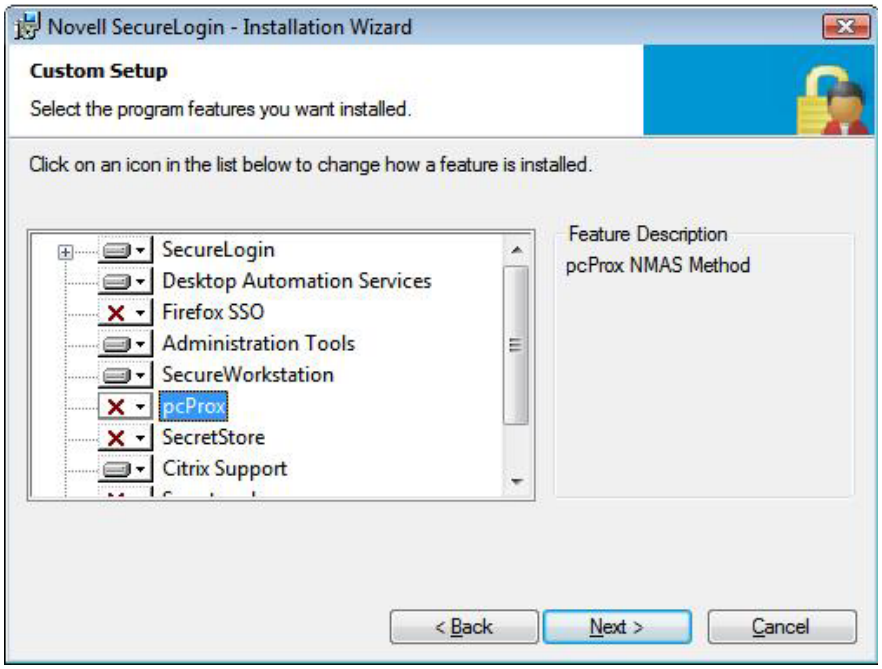


If SecureLogin is already installed, it launches the Program Maintenance page.



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

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



4 Click *Install*.

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

NOTE: The pcProx identification fails in eDirectory after you install pcProx through the *Modify* option. This happens because the *Modify* option does not have an UI. So, it is not possible to do an identification directly after an install.

You must edit the registries with default values. Edit these values with the respective configurations.

29.2 Modify Option and Group Policy Objects Support

During a fresh install of Novell SecureLogin, the Group Policy Objects support can be selected and installed in Active Directory Application Mode (ADAM) or Active Directory (AD) environments only.

If you are using the *Modify* option in a non-AD or ADAM environment the GPO option still shows as an selectable option even though GPO's are not supported in non-AD or ADAM environments.

Upgrading

X

Prerequisites

30

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.
- **Microsoft Redistributable:** Before upgrading from Novell SecureLogin 6.1 and Novell SecureLogin 6.1 SP1 to Novell SecureLogin 7.0 on Microsoft Windows Vista (32-bit), ensure that you have installed Microsoft redistributable 2005 SP1. The redistributable is available with the Novell SecureLogin 7.0 installer package.

  If the redistributable is not found, an error message indicating *SLBroker.exe and slnrmonitorserver.exe have failed to start because the application configuration is incorrect. Reinstalling the application may fix this problem*, is displayed and the upgrade fails.
- **NICI and NMAS:** Before upgrading to Novell SecureLogin 7.0 in eDirectory environment from the previous versions (3.5.*x*, 6.0, 6.1, and 6.1 SP1), upgraded NICI and NMAS client.

  The required versions are:

  - NICI - 2.7.2
  - NMAS Client - 3.4.3

NOTE: The version of NICI and NMAS Client are the same for both 32 bit and 64 bit installation.

Phased Upgrading

31

31.1 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.

31.2 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 *7.0*.

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.

31.3 Running Novell SecureLogin in a Mixed Environment

When SecureLogin 7.0 runs in the same environment as SecureLogin 3.0*.x*, SecureLogin 7.0 does the following:

- Versions the SecureLogin data store.
- Saves SecureLogin 7.0 data in the SecureLogin 6.1 data format.

This mixed mode enables you to gradually deploy SecureLogin 7.0 in a SecureLogin 6.1 environment while still allowing you to perform most administration tasks during the transition.

Deploying SecureLogin7.0 in a mixed environment has the following limitations:

- Limited administrative functionality

  When you run SecureLogin 7.0 in mixed mode, new features such as shadow variables do 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.

31.4 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.

31.5 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.

Upgrading Novell SecureLogin 32

If you are running Novell SecureLogin 7.0 on Microsoft Windows XP or 2003 and, want upgrade to Microsoft Windows Vista, you must

Even if SecureLogin 7.0 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 7.0 and automatically works with it.

1. Uninstall Novell SecureLogin on the older operating system.
2. Upgrade the operating system.
3. Reinstall Novell SecureLogin 7.0 on Microsoft Windows Vista.

When you try to upgrade to Novell SecureLogin 7.0 from version 6.0 or later, a message `Click Proceed to upgrade SecureLogin with the current Language Settings`, is displayed. Click *Proceed* to continue with the upgrade.

This section explains the following upgrade scenarios.

32.1 Upgrading from Novell SecureLogin 6.1, 6.1 Hotfixes, and 6.1 SP1

1. Run `Novell SecureLogin.msi` found in the `\securelogin\client` directory in the Novell SecureLogin 7.0 installer package.
2. The Installation 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*.

32.2 Upgrading from Novell SecureLogin 6.0 and 6.0 Patches

1. Run `Novell SecureLogin.msi` found in the `\securelogin\client` directory in the Novell SecureLogin 7.0 installer package.
2. You are prompted to proceed with the upgrade with the current language settings. Click *Proceed*.
3. The Installation 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*.

32.3 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 7.0 installer package.

32.4 Upgrading from Novell SecureLogin 3.0.x

IMPORTANT: Uninstall Novell SecureLogin 3.0.*x* before you can upgrade to the new version.

The procedures explained here uses 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.

32.5 Upgrading Through The Command Line

1 Use the following command to update silently:

```
msiexec /i <Path to NSL msi> /qb
```

Upgrading Desktop Automation Services

33

This release of Novell SecureLogin provides an option to install Desktop Automation Services during the installation of Novell SecureLogin. Previously, Desktop Automation Services was a standalone release. However, it required Novell SecureLogin to function.

You can not uninstall Desktop Automation Services through the Novell SecureLogin Windows Installer Package when upgrading to Novell SecureLogin 7.0.

IMPORTANT: You cannot upgrade Desktop Automation Services by using Novell SecureLogin 7.0

You must manually uninstall Desktop Automation Services before upgrading or installing afresh Novell SecureLogin 7.0

Upgrading and Modifying pcProx

34

During an upgrade if pcProx is already present, the program upgrades pcProx and is a part of Novell SecureLogin. The configuration of the old pcProx is retained.

Uninstalling

35

Remove the Novell SecureLogin installation programs through the *Add/Remove Programs*.

1. Click *Start* > *Control Panel* > *Add /Remove Programs*.
2. From the list of installed programs and updated, select *Novell SecureLogin*.
3. Click *Remove*.

Known Issues

- The `SlnrmonitorServer.exe` service continues to run even after Novell SecureLogin is shutdown by using the `/shutdown` switch. The service continues to run in the memory.

  This is an expected behavior because the SlnrmonitorServer.exe service cleans anything that SecureLogin leaves behind.

- Mozilla Firefox Displays an Error After Uninstalling SecureLogin. If you uninstall SecureLogin, the Mozilla Firefox browser displays an error message when it restarts. This error occurs because the Firefox extensions do not have command line parameters for uninstalling.

  If this happens, uninstall the Firefox extension manually as follows:

  1. Click *Tools* > *Extensions*.
  2. Select the extension files that you want to delete.
  3. Click *Uninstall*.
  4. Restart the browser.

-

Documentation Updates

A

This section lists the updates made to the *Novell SecureLogin Administration Guide*, after the initial release in September 2009.

A.1 February 05, 2010

- Rectified the description for LDAP authentication types in Installing on eDirectory platform and Section 8.1, “Installing Novell SecureLogin in Non-eDirectory LDAP Environment,” on page 51.

A.2 January, 20, 2010

- Included information on upgrading through the command line. See Section 32.5, “Upgrading Through The Command Line,” on page 208.