SecureLogin 8.6

Installation Guide

February, 2018

Legal Notice

Contents

About This Guide

This manual provides information on installing, deploying, and upgrading SecureLogin.

This document contains the following sections:

Additional Documentation

For the latest version of SecureLogin guides, see www.netiq.com/documentation/securelogin/

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Getting Started

The section explains the prerequisites to be met before installing SecureLogin.

Prerequisites

For information about hardware and software configurations required for the successful installation and deployment of SecureLogin, see NetIQ SecureLogin Quick Start Guide.

Setting Up a Passphrase

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

During installation, the passphrase security is enabled to enforce passphrase setup during the initial login. You can disable the passphrase policy by deselecting **Use Passphrase Policy** option in the **Advanced Settings** pane of the Administrative Management utility. If a passphrase has previously been configured, this dialog box does not display and the installation is complete.

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

WARNING: Remember the passphrase answer. 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.

2 Introduction

NetIQ 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. NetIQ 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.

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

Features of SecureLogin Installer

Evaluation build for 30-days trial: You can use the evaluation version that can be downloaded from the NetIQ Products page. Using the evaluation version you can try out all the features of SecureLogin on a 30-day trial mode, without buying licenses.

Upgrading to a license model from the evaluation version is not supported. If you plan to buy the licenses of SecureLogin, uninstall the evaluation version and install the licensed version.

Audit log for Windows and Syslog messages : In the Custom Setup window, the Auditing feature helps to configure syslog, and enable or disable the logging Windows event messages.

Configure Syslog Server during installation: The Syslog server is installed and configured during the installation of SecureLogin. The Syslog server can be configured by using the installation wizard, command line and by modifying the registry settings.

Option to Disable Logging of Windows Event Messages By Using the Installation Wizard: In NetIQ SecureLogin, logging of windows event messages are enabled by default. SecureLogin provides a facility to disable logging of Windows event messages during installation.

Using this option administrators can decide if workstation event messages should be logged for each workstation. For more information refer "Logging Event Messages" on page 13.

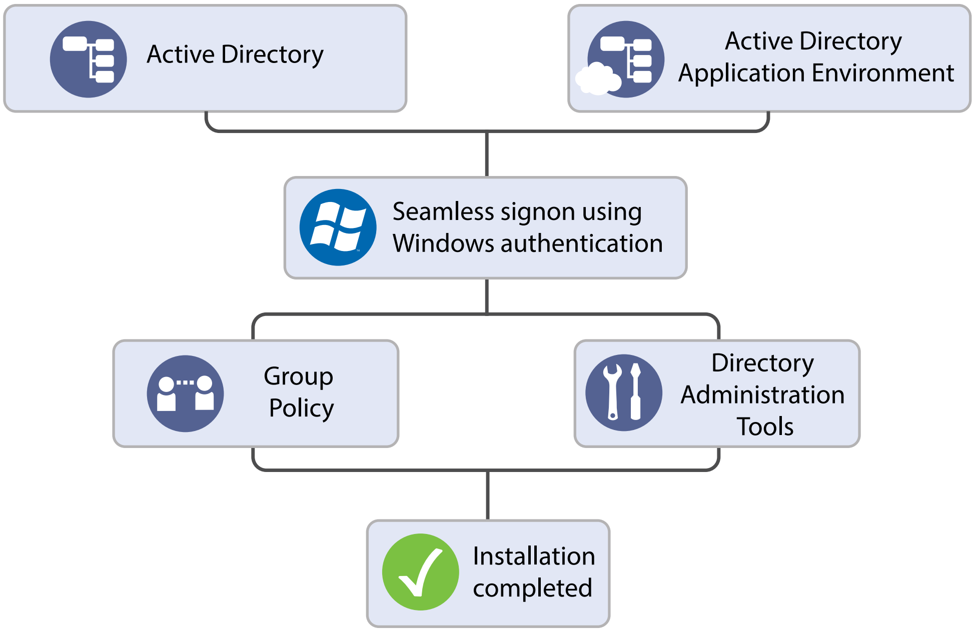
Advanced Authentication: In the Custom Setup window, the Advanced Authentication feature supports different methods of authentication for logging in to Active Directory, ADAM/AD LS, eDirectory and LDAP v3.

Installation Overview

- Launch the SecureLogin executable.
- Select the datastore. Valid datastore options are:
    - Microsoft Active Directory
    - Microsoft ADAM/AD LS
    - NetIQ eDirectory with Novell Client

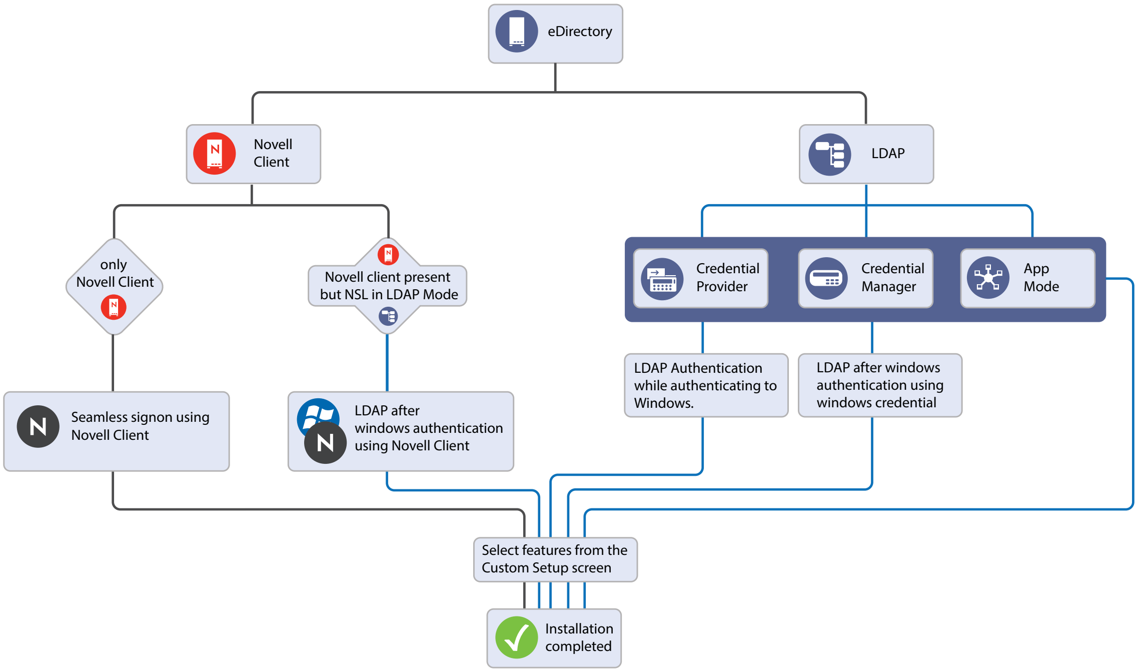
  - NetIQ eDirectory with LDAP
  - LDAP v3 (non-eDirectory)
  - Standalone
- If you select to install in **NetIQ eDirectory with Novell Client** or **NetIQ eDirectory with LDAP** mode, then you can also choose to enable SecretStore.
- Select the features you want to install from the **Custom Setup** screen. Click the feature and choose to install the feature.
- If Novell Client is installed, the default account association is Novell Client.
- If you select to install in an Active Directory or Active Directory Application Environment, the windows authentication credentials are used for Seamless signon.

***Figure 2-1** Installing Features in an Active Directory environment*


Active Directory
Active Directory Application Environment
Seamless signon using Windows authentication
Group Policy
Directory Administration Tools
Installation completed

- While installing in an LDAP mode, choose between the Credential Manager, Credential Provider and the Application mode.

Figure 2-2 *Seamless Signon Using Novell Client or LDAP*


eDirectory
Novell Client
LDAP
only Novell Client
Novell client present but NSL in LDAP Mode
Credential Provider
Credential Manager
App Mode
LDAP Authentication while authenticating to Windows.
LDAP after windows authentication using windows credential
Seamless signon using Novell Client
LDAP after windows authentication using Novell Client
Select features from the Custom Setup screen
Installation completed

Logging Event Messages

You can log events through Windows event log and view the events by using Event Viewer. In NetIQ SecureLogin, logging of windows event messages are enabled by default. If you require to send the events through Syslog, use one of the following options:

Forward to Syslog Server: Selecting this option allows only a single connection from a SecureLogin client to Syslog server and caches the events in **EventLog**. For example, on a citrix or a terminal server, where users are allowed to access a single service there will be a single connection to Syslog and all the events get cached to **EventLog**. This option is disabled by default.

Syslog Server: Selecting this option connects each SecureLogin client to Syslog server and the events gets cached only for an active SecureLogin session. This option is disabled by default.

SecureLogin provides a facility to disable logging of Windows event messages during installation. Using this option administrators can decide if workstation event messages should be logged for each workstation.

Disabling Logging to Windows Event Log By Using Installation Wizard

To disable logging of Windows event messages, perform the following:

1. Launch NetIQ SecureLogin installation wizard. Review and accept the license agreement.
2. Select the datastore.
3. In the Custom Setup screen, traverse to the **Auditing** menu option. **Windows EventLog** is enabled by default. Deselect the option to stop logging of windows event logs to the workstation.

NOTE: If you have disabled logging of Windows event messages using the Installation Wizard, you must run the installation wizard once again if you want to enable it.

Installing SecureLogin with the **Windows EventLog** option enabled, updates the registry and creates a registry entry named `EnableWindowsEventLog`. The details of this registry are as following:

Purpose	Enable/Disable sending audit events to windows event logger
Location	`HKEY_LOCAL_MACHINE\Software\Protocom\SecureLogin`
Type	REG_DWORD
Value	1 - Enable 0 - Disable (Default)o

This setting when used in conjunction with the **Enable logging to Windows Event log** preference helps to log Windows event messages for a specific user.

NOTE: SecureLogin preferences can be managed using administrative utilities like iManager or Slmanager. To ensure that the administrative utilities are installed, ensure that you select the **Directory Administration Tools** option while installing SecureLogin.

Disabling Logging to Windows Event Log After the Installation

1. Launch Administrative Utility.
2. Click **Preferences** > **Auditing**. The **Enable logging to Windows EventLog** option is enabled by default. To disable logging, deselect this option.

Logging of Syslog Audit Messages

SecureLogin includes a facility to log Syslog audit messages. During installation, NetIQ SecureLogin is configured on each host such as Citrix, terminal servers, and so on to connect and generate logs to a specific syslog service.

This enhances the auditing mechanism and removes the need of having another Security Information and Event Management (SIEM) solution.

Installing and Configuring Syslog Auditing

- “Installing Syslog Auditing Feature Using the Windows Installer Wizard” on page 15
- “Configuring Syslog Auditing Using the Windows Installer Command-Line Option” on page 15
- “Modifying the Registry Settings” on page 16

Installing Syslog Auditing Feature Using the Windows Installer Wizard

1. Select **Syslog Server** option under **Auditing** to enable the Syslog auditing feature.

   If the **Forward to Syslog Server** option under **Windows EventLog** is also selected, duplicate events gets generated on the Syslog server. For more information about this option, refer "Logging Event Messages" on page 13.

2. Specify the name of the server that is to be configured as the Syslog server. By default the Syslog server address is set to `localhost` and the supported protocols are `UDP`, `TCP`, and `TLS`.

   By default, the Syslog server listens to default ports for each protocol. Such as, for UDP the Syslog server listens to `514`, for TCP there is no specific port, and for TLS the server listens to `6514`.

3. Select the language in which the event message should be sent to Syslog server. The supported languages are:

   - German
   - English
   - Spanish
   - French
   - Japanese
   - Portuguese
   - Chinese (Traditional)
   - Polish

   The default language is English.

4. Click **Next** to install the Syslog Auditing feature on the workstation.

Configuring Syslog Auditing Using the Windows Installer Command-Line Option

To configure Syslog using command-line option, use the following command:

```
APPENDLOCAL=Syslog SYSLOGSERVERURI=protocol-type://server-name:port-number:X_SYSLOGLANGUAGEID=<language-code>
```

Replace language-code with the code from the following supported languages:

- 1028 - Chinese (Traditional)
- 1031 - German
- 1033 - English (Default)
- 1034 - Spanish
- 1036 - French
- 1041 - Japanese
- 1045 - Polish
- 1046 - Portuguese

For example: `APPENDLOCAL=Syslog SYSLOGSERVERURI=udp://localhost:514:1045`

Modifying the Registry Settings

To enable/ disable Syslog audit messages, create the following registry entries:

EnableSysLog

Purpose	Enable/Disable sending audit events to the syslog server
Location	`HKEY_LOCAL_MACHINE\Software\Protocom\SecureLogin`
Type	REG_DWORD
Value	1 - Enable 0 - Disable (Default)

SyslogServerUri

Purpose	Syslog server details in the form of URI
Location	`HKEY_LOCAL_MACHINE\Software\Protocom\SecureLogin`
Type	REG_SZ
Value	<protocol-type>://<server-name>:<port-number>:X_SYSLOGLANGUAGEID=<language-code> For example: `udp://syslog.myserver.com:514:X_SYSLOGLANGUAGEID=1033`

SyslogMessageLanguageId

Purpose	Language that should be used in sending the event message to syslog server.
Location	`HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin`
Type	REG_DWORD
Value	Decimal value of the respective language as mentioned in section 1.3.1.2.

Enabling Logging to Syslog

1. Launch an Administrative Utility.
2. Click **Preferences > Auditing**. The **Enable logging to Syslog Server** option is an administrator setting that is disabled by default. To enable logging of Syslog events on the user's workstation, select this option and set it to `Yes`.

Managing Log Settings for SecureLogin Components

The NSL Log Manager tool is used for managing the log settings for SecureLogin components. This section explains the NSL Log Manager tool.

This tool is included as part of the SecureLogin installer and to launch this tool run the `slLoggingManager.exe` file from `SecureLoginTools\slLoggingManager.`

Understanding the NSLLogManager Functionality

The NSLLogManager tool can perform the following:

- To configure the log settings for Novell SecureLogin components such as LDAP Client (NLdapAuth).
- To Provides support for additional components which are missing in SLLoggingManager tool shipped with Novell SecureLogin.

Using NSLLogManager

To use NSLLogManager, perform the following steps:

1. Launch the `NSLLogManager.exe` file.

   It displays the current status of log settings for SecureLogin components such as LDAP Client (NLdapAuth).
2. From the **Component** list, select the component for which you want to enable the log.
3. From the drop-down list in the Log Settings column, select either **Disabled** or **Enabled** as per your requirement.

   The new setting is automatically updated in the registry.

Installing SecureLogin with Advanced Authentication

Prerequisite:

If you are using Advanced Authentication with TLS 1.2, you must have .NET 4.5 installed in the system.

To install SecureLogin, perform the following steps:

1. Run the `NetIQSecureLogin.exe` file.

   The **License Agreement** screen is displayed.
2. Accept the license agreement.
3. Click **Next** to view the **Setup Options** screen.
4. Select the desired datastore.
5. Click **Next** to view the **Ready to Install** screen.
6. Click **Install**.
7. Click **Next** to view the **Custom Setup** screen.
8. From the **Custom Setup** screen, select **Advanced Authentication**.
9. Click **Next** to view the **Cache File Location** screen.

The location is auto-populated, but you can click **Browse** to select an alternative folder to store the user settings.

NOTE: Ensure the users have write access for the specified folder.

---

10 Click **Next** to view the **Advanced Authentication Server** screen.

11 In the **Advanced Authentication Server** screen, enter the **Server Address**, **Port** and **Event Name**.

12 Click **Next**.

SecureLogin is by default installed in `C:\Program Files\NetIQ\SecureLogin` folder.

Installing SecureLogin Browser Extensions

SecureLogin supports single sign-on for web applications using Internet Explorer, Mozilla Firefox, and Google Chrome browsers. To enable single sign-on for web applications in Mozilla Firefox and Google Chrome, you must install the Single Sign-on Assistant extension or NetIQ Securelogin SSO Extension in the respective browser.

Single Sign-on Assistant provides a secure single sign-on experience for Access Manager, CloudAccess and SecureLogin users by allowing automatic authentication for configured applications. NetIQ recommends that you use Single Sign-on Assistant instead of NetIQ SecureLogin SSO Extension.

IMPORTANT: The Single Sign-on Assistant extension is supported from SecureLogin 8.5.3 and above. You must remove the NetIQ SecureLogin SSO Extension from your browser before installing Single Sign-on Assistant extension.

Download and install the required SecureLogin browser extension for Google Chrome and Mozilla Firefox using the following information:

- "Installing Single Sign-on Assistant in Google Chrome" on page 18
- "Installing Single Sign-on Assistant in Mozilla Firefox" on page 19
- "Installing NetIQ SecureLogin Extension in Google Chrome" on page 19
- "Installing NetIQ SecureLogin Extension in Mozilla Firefox" on page 19

Installing Single Sign-on Assistant in Google Chrome

1. If NetIQ SecureLogin SSO Extension is installed, perform Step 2. Otherwise, continue from Step 3.
2. Perform the following steps in the Google Chrome browser to remove NetIQ SecureLogin SSO Extension:
    1. Click **More Tools** **> Extensions**.
    2. Locate NetIQ SecureLogin SSO Extension.
    3. Click the delete icon to remove NetIQ SecureLogin SSO Extension.
3. In the Google Chrome browser, click **More Tools** **> Extensions > Get more extensions**.
4. Specify **Single Sign-on Assistant** in the search field.
5. Locate and click **Single Sign-on Assistant** in search results.
6. Click **ADD TO CHROME**.

7 Click **Add extension**.

8 To perform auto update in the chrome browser, click **Settings > Extensions > Update extensions now** to force update the extension manually.

Installing Single Sign-on Assistant in Mozilla Firefox

NOTE: Single Sign-on Assistant is supported in Mozilla Firefox version 50 and above.

---

1 If NetIQ SecureLogin SSO Extension is installed, perform Step 2. Otherwise, continue from Step 3.

2 Perform the following steps in the Mozilla Firefox browser to remove NetIQ SecureLogin SSO Extension:

1. Click **Add-ons > Extensions**.
2. Locate NetIQ SecureLogin SSO Extension.
3. Click **Remove** to remove NetIQ SecureLogin SSO Extension.

3 In the Mozilla Firefox browser, click **Add-ons > Extensions**.

4 Specify **Single Sign-on Assistant** in the **Search all add-ons** field.

5 Locate **Single Sign-on Assistant** in the search results and click **Install**.

6 Click **Accept and Install...** in the **End-User License Agreement** window.

7 Click **Add** when the Mozilla Firefox browser prompts to add Single Sign-on Assistant extension.

8 Click **OK**.

For accessing applications that are local to your system, after installing the extension select **Allow access to file URLs** under the Single sign-on Assistant. This allows SecureLogin to login and fill the form for local files such as `file:///C:/dev/test.html`.

Installing NetIQ SecureLogin Extension in Google Chrome

1 In the Google Chrome browser, click **Settings > Extensions > Get more extensions**.

2 Specify **NetIQ Securelogin SSO Extension** in the search field.

3 Click **NetIQ Securelogin SSO Extension** and follow the on-screen prompts.

If you already have an older version of **NetIQ Securelogin SSO Extension** installed, it is recommended to install the Single Sign-on Assistant plug-in.

Installing NetIQ SecureLogin Extension in Mozilla Firefox

NOTE: NetIQ SecureLogin SSO Extension is supported only in Mozilla Firefox version 50 and above.

---

1 Download NetIQ Securelogin SSO Extension for Mozilla Firefox from the NetIQ Product download site.

1a In the product download site, select the product as **SecureLogin** and the version as **SecureLogin 8.5**, then click **Submit Query**.

1b From the search result click **NetIQ SecureLogin 8.5**.

1c In the NetIQ SecureLogin 8.5 page, click **proceed to download** and follow the on-screen prompts to download the extension.

2. In the Mozilla Firefox browser, click **Add-ons > Extensions**.
3. Drag and drop the downloaded NetIQ Securelogin SSO Extension to the Extensions page of Mozilla Firefox.

   NOTE: If you download the extension using Google Chrome, the extension is downloaded as a `.zip` file. You must drag and drop the complete zip file to install the extension in Mozilla Firefox.

4. Click **Install** in the pop-up dialog box.

For accessing applications that are local to your system, after installing the extension select **Allow access to file URLs** under the NetIQ SecureLogin SSO Extension. This allows SecureLogin to login and fill the form for local files such as `file:///C:/dev/test.html`.

3 Installing and Configuring in Active Directory Environment

This section provides information on installing, configuring, and deploying SecureLogin 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" on page 21
- "Configuring" on page 24
- "Installing" on page 28
- "Deploying" on page 29

Before You Begin

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.

- "Prerequisites" on page 21
- "Requirements for Microsoft Windows Server" on page 22
- "Installation Overview" on page 22
- "Microsoft Active Directory" on page 23

Prerequisites

- Ensure that you meet the hardware and software requirements listed in the NetIQ SecureLogin Quick Start Guide.
- 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.
- Back up the existing directory.
- You must install Java 1.7 or 1.8 to enable single sign-on to Java applications on the workstation.
- For multiple-directory environments:
  - Identify the domain controller to determine the directory where you will install SecureLogin and the order of replication.
  - Have access to the domain controller.

Requirements for Microsoft Windows Server

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

- "Internet Explorer Enhanced Security" on page 22
- "Enabling Single Sign-On for Internet Explorer" on page 22

Internet Explorer Enhanced Security

By default, Microsoft Windows Server 2008 and 2012 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 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).

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 SecureLogin.

You can do this by:

- "Enabling Web Browser Extensions" on page 22
- "Enabling Browser Help Objects in Internet Explorer" on page 22

Enabling Web Browser Extensions

- **On both Windows Server 2008:** Go to **Internet Options** > **Advanced** > **Browsing**, then select the **Enable Third party web browser extension (requires restart)** option.

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 `SecureLogin IE SSO Helper object Class` entry is displayed as **Enabled**.

Installation Overview

1. Uninstall any 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 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 Java 1.7 or 1.8 on the server and workstations, if single sign-on to Java applications is required.
6. Install SecureLogin on the administration workstation.
7. Create test users on the administration workstations.
8. Define and configure the SecureLogin user environment, including enabling the required applications for single sign-on.
9. Copy the test users' configuration to relevant objects.
10. Install the SecureLogin application on user workstations.

Microsoft Active Directory

- "SecureLogin on Windows" on page 23
- "LDAP Environment" on page 23
- "ADAM" on page 23

SecureLogin on Windows

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

LDAP Environment

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 "Extending the LDAP Directory Schema and Assigning Rights on the Server" on page 49

ADAM

SecureLogin supports deployment in an ADAM instance. For more information, see Part 4, "Configuring, Installing, and Deploying In Active Directory LightWeight Directory Services," on page 31.

Configuring

SecureLogin uses the directory structure and administration tools to provide centralized management and deployment of users. In the Active Directory environment, 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 SecureLogin, you must first extend the Active Directory schema. You can also configure the user's environment or create roaming profiles.

- "Extending the Active Directory Schema and Assigning Rights" on page 24
- "Configuring a User's Environment" on page 27
- "Configuring Roaming Profiles" on page 28

Extending the Active Directory Schema and Assigning Rights

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

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 SecureLogin directory schema attributes is referred to as *assigning user rights.*

The SecureLogin Microsoft Active Directory schema extension executable extends the schema on the server and enables you to assign user rights. You must determine which containers and organizational units need SecureLogin access, and 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 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.

- "Extending the Schema" on page 25
- "Assigning User Rights" on page 26
- "Refreshing the Directory Schema" on page 27

Extending the Schema

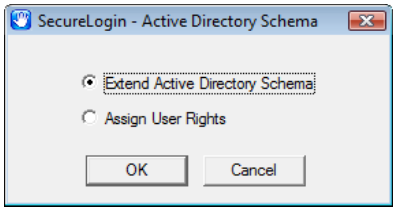
The following instructions apply to the configuration of the Microsoft Active Directory instance stored and administered on a separate server from the Active Directory server domain controller.

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

   or

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

   The SecureLogin Active Directory Schema dialog box is displayed.

   ● Extend Active Directory Schema

   ○ Assign User Rights

3. Select **Extend Active Directory Schema**.
4. Click **OK**.

   The following 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 `adsschema.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 previously extended the schema, a message listing the existing schema appears. Ignore this message.

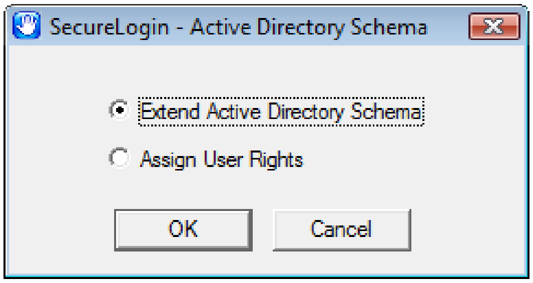
6. Click **OK** in the Active Directory Schema dialog box.
7. Continue with "Assigning User Rights" on page 26 to assign user access rights to the relevant containers and organizational units.

Assigning User Rights

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

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

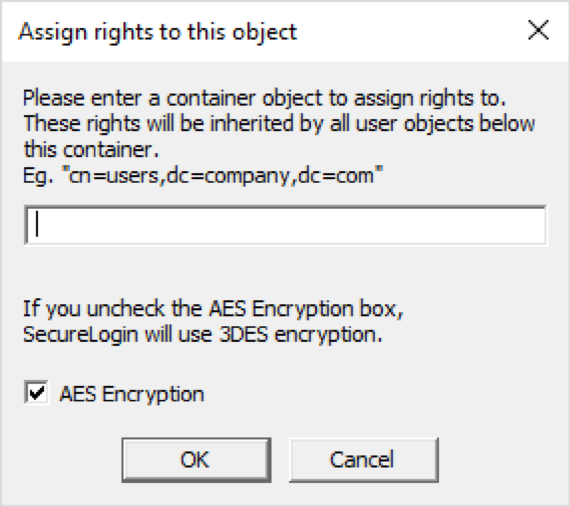
1 Run `adsschema.exe`, which is found in the `Securelogin\Tools\Schema\ADS` directory.



● Extend Active Directory Schema

○ Assign User Rights

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



Please enter a container object to assign rights to. These rights will be inherited by all user objects below this container.
Eg. "cn=users,dc=company,dc=com"

If you uncheck the AES Encryption box, SecureLogin will use 3DES encryption.

☑ AES Encryption

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`

IMPORTANT: The **AES Encryption** option is selected by default to use AES256 Encryption. If you unselect this option then the container will use 3DES encryption. It is recommended to use AES256 encryption.

IMPORTANT: You can run adsschema.exe again with AES Encryption option unselected but it does not change to 3DES encryption. Use `slmanager.exe` to enable 3DES encryption.

NOTE: Rights Assignment does not work on top level Domain (root) or Group. It is recommended to assign rights on organizational unit using adsschema.exe.

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 SecureLogin data to write to the directory.

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.

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 SecureLogin environment includes:

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

Configure 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 *NetIQ SecureLogin Administration Guide*.

Table 3-1 Deployment and Distribution Options

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

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, SecureLogin loads the users profile, effectively locking that profile and preventing the users credential data from being copied to the roaming profile.

To prevent SecureLogin from causing problems with existing user roaming profiles, select the enable Roaming Profile feature.

This feature gets installed by default, if the workstation is a Citrix or Terminal Server. You can also set the registry setting ForceHKLMandNoDPAPI to 1 for Roaming Profile activation, if it was not initially installed.

Installing

After you have extended the Active Directory schema as described in "Extending the Schema" on page 25 and assigned permissions to the required directory objects as described in "Assigning User Rights" on page 26, you can install the SecureLogin application on the administration and user workstations.

- "Installing on Administrator Workstations" on page 28
- "Installing on a User Workstation" on page 29
- "Installing for Mobile Users and Notebook Users" on page 29

Installing on Administrator Workstations

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. Run the `NetIQSecureLogin.exe` file.
2. Accept the license agreement.Click **Next**. The License Agreement page is displayed.
3. Select **Microsoft Active Directory**. Click **Install**.
4. Click **Next** to view the Custom Setup screen.

   This screen includes all the features. Select the required features.
5. SecureLogin is by default installed in `C:\Program Files\NetIQ\SecureLogin` folder. If you want to change the location, click **Browse** and specify a different location. Select the features you want to install and click **Next**.

Installing on a User Workstation

Installing SecureLogin on user workstations uses the same procedure as Chapter , "Installing," on page 28. Use industry standard application distribution packages such as Microsoft IntelliMirror, System Management Server, or Novell ZENWorks to deploy and manage SecureLogin across large enterprises.

Installing for Mobile Users and Notebook Users

Installing 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

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

Refer to Chapter , "Setting Up a Passphrase," on page 9 for detailed information on setting up a passphrase.

4 Configuring, Installing, and Deploying In Active Directory LightWeight Directory Services

This section provides information on configuring, installing, and deploying SecureLogin in Active Directory Application Mode (ADAM) or Active Directory Lightweight Directory Services (AD LDS).

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

SecureLogin supports deployment in an ADAM instance. Active Directory is responsible for the network authentication while ADAM stores and provides 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://msdn.microsoft.com/en-us/library/bb897400.aspx)

Prerequisites

- Ensure that you meet the hardware and software requirements listed in the "NetIQ SecureLogin Quick Start Guide".
- Ensure that your operating system has the latest version of Microsoft Windows Installer.
- 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)
- Install AD LDS server role. For the installation procedure, refer Microsoft Web site (https://technet.microsoft.com/en-au/library/cc754486(v=ws.10).aspx)
- 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 SecureLogin and the order of replication.
    - Have access to the domain controller.

Language Support

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

Supported Platforms

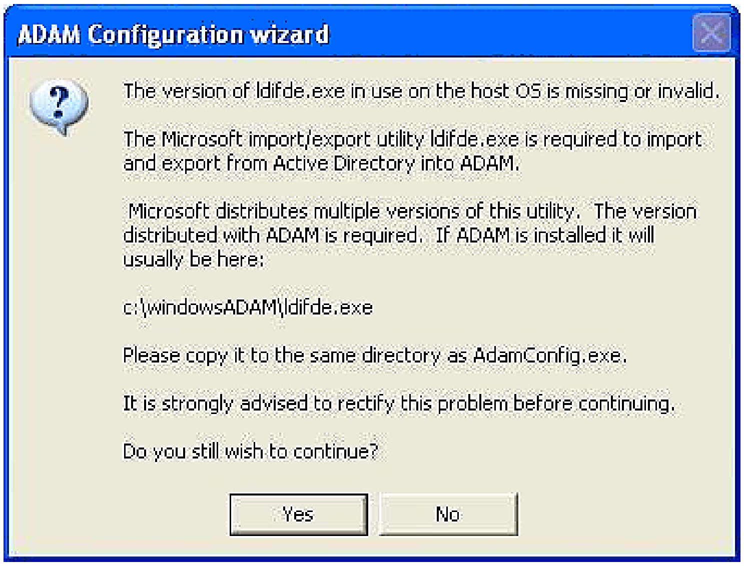
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 R2

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

Figure 4-1 *Warning message*



ADAM Configuration wizard

The version of ldifde.exe in use on the host OS is missing or invalid.

The Microsoft import/export utility ldifde.exe is required to import and export from Active Directory into ADAM.

Microsoft distributes multiple versions of this utility. The version distributed with ADAM is required. If ADAM is installed it will usually be here:

c:\windowsADAM\ldifde.exe

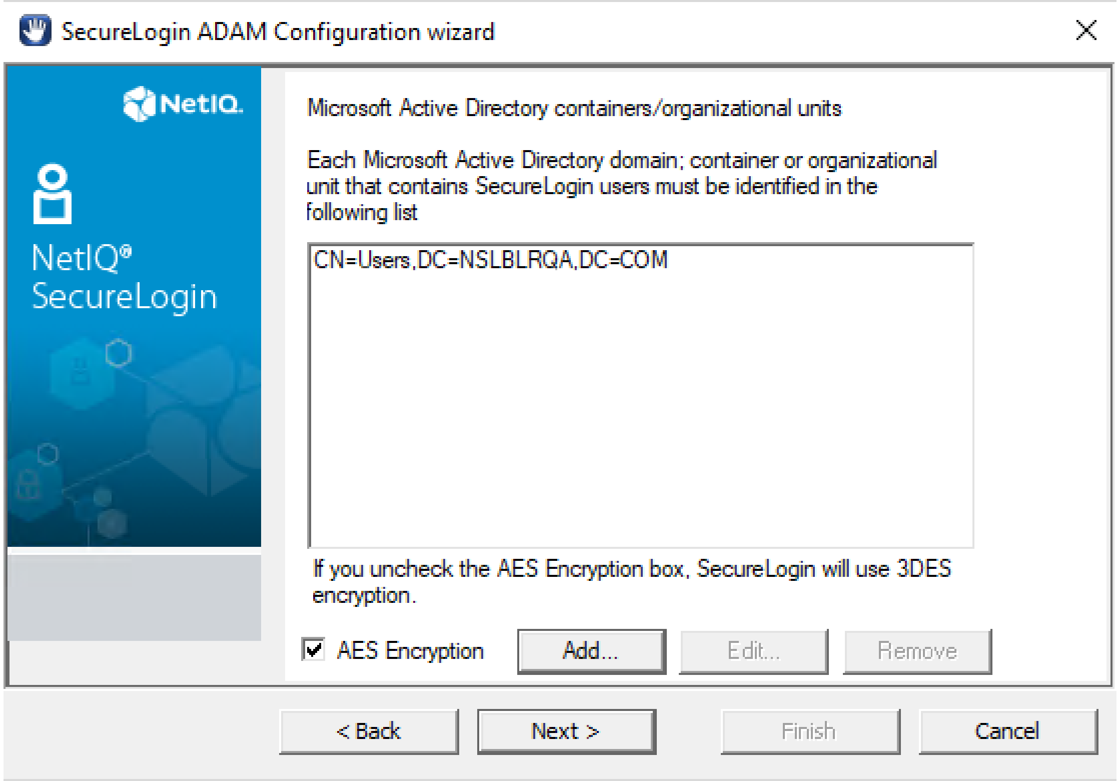
Please copy it to the same directory as AdamConfig.exe.

It is strongly advised to rectify this problem before continuing.

Do you still wish to continue?

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 4-2 ADAM Configuration Wizard



Microsoft Active Directory containers/organizational units

Each Microsoft Active Directory domain; container or organizational unit that contains SecureLogin users must be identified in the following list

CN=Users,DC=NSLBLRQA,DC=COM

If you uncheck the AES Encryption box, SecureLogin will use 3DES encryption.

☑ AES Encryption

IMPORTANT: The **AES Encryption** option is selected by default. If you unselect this option then the container will use 3DES encryption. It is recommended to use AES Encryption for new containers and new deployments.

If you run `ADAMconfig.exe` with AES Encryption option unselected, it will not use 3DES encryption. Use `slmanager.exe` to enable 3DES or AES encryption. It is recommended to use AES256 encryption.

IMPORTANT: You can run ADAMconfig.exe on existing containers with AES Encryption option selected but it does not change the default old encryption. Use `slmanager.exe` to enable AES Encryption for existing containers.

Configuring

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 AD LDS instance

SecureLogin supports deployment in an AD LDS instance. Active Directory is responsible for network authentication, while AD LDS 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 AD LDS for the user's single sign-on data.

For more information on AD LDS, see Microsoft Web site.

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 SecureLogin in an ADAM environment:

- "Creating a Network Service Account and Assigning Permissions" on page 34
- "Configuring ADAM Schema" on page 35
- "Creating an ADAM Instance" on page 35
- "Extending the Schema by Using ADAM Configuration Wizard" on page 37

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 SecureLogin, but allows the ADAM instance to be cleaned properly when it is uninstalled.
9. Click **OK** to close the [Domain] Properties dialog box.

Configuring ADAM Schema

SecureLogin leverages the directory to store and manage 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 SecureLogin data. The 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

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 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.

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 “Extending the Schema by Using ADAM Configuration Wizard” on page 37 to automatically extend the ADAM instance schema and assign Read and Write Rights to directory user objects.

Extending the Schema by Using ADAM Configuration Wizard

The SecureLogin ADAM configuration wizard extends the ADAM directory schema with SecureLogin attributes, creates ADAM partitions, and assigns selected directory objects read and write permissions to the 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 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 SecureLogin installer package. We recommend that you perform this procedure with the assistance of our Technical Support.

Prerequisites

Before running the SecureLogin ADAM Configuration Wizard:

1. Copy the `AdamConfig.exe` file found in `\SecureLogin\Tools\Schema\ADAM` to server or the administrator workstation.
2. Copy `dsacls.exe` from Windows Support Tools to the ADAM folder on the server or Administrator workstation.

Using the ADAM Configuration Wizard

The ADAM Configuration Wizard extends the ADAM directory schema with 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 NetIQ 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 SecureLogin users are specified here, so you can assign 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 SecureLogin ADAM Configuration - Termination dialog box is displayed if the configuration was not able to complete successfully. If this occurs, review the text box to investigate cause of termination. If a solution to the problem is determined, click **Close** and repeat execution of the SecureLogin ADAM Configuration Wizard.

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

17. Click **Close**.

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 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 "Configuring ADAM Schema" on page 35 are listed or not. Repeat this for each container and or organizational unit containing 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.

Adding Users or User Groups to Manage SecureLogin In ADAM Instance

To assign LDS rights to a specific user or user group, perform the following steps:

1. Click **Start > Administrative Tools > ADSI Edit**.
2. In the console tree, click **Configurations > CN=Roles**.
3. Double click **CN=Administrators** to open **CN=Administrators Properties**.
4. In **Attribute Editor**, select the **member** attribute and click **Edit**.

5 Click **Add Windows Account...** or **Add DN...** in the **Multi-valued Distinguished Name With Security Principal Editor** window to add users or user groups that you want to assign LDS rights.

6 Click **OK**.

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 SecureLogin data created in the ADAM instance.

To synchronize data from Active Directory to an ADAM instance:

1 Navigate to `SecureLogin\Tools` of the SecureLogin 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

Installing on Administrator Workstations

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

It is recommended that you deploy and manage 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. Run the NetIQSecureLogin.exe file.
3. Accept the license agreement.Click **Next**. The License Agreement page is displayed.
4. Click **Next**. The License Agreement page is displayed.
5. Select **Microsoft ADAM/AD LS**

   Click Install.
6. Click **Next** to view the Custom Setup screen.
7. SecureLogin is by default installed in `C:\Program Files\NetIQ\SecureLogin` folder. If you want to change the location, click **Browse** and specify a different location. Select the features you want to install and click **Next**.

Installing SecureLogin on a User Workstation

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

Follow the instructions given in "Installing on Administrator Workstations" on page 41.

Installing for Mobile Users and Notebooks

Installing SecureLogin for mobile users and notebooks follows the same procedure as explained in Chapter , "Installing," on page 40.

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

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 SecureLogin in an ADAM environment.

- "Configuring a User's Environment" on page 42
- "Administering SecureLogin In an ADAM Environment" on page 42
- "Setting Up a Passphrase" on page 42

Configuring a User's Environment

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

Configuring a user's SecureLogin includes:

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

Administering SecureLogin In an ADAM Environment

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 SecureLogin either through the SLManager or through iManager.

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

Setting Up a Passphrase

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

Refer Chapter , "Setting Up a Passphrase," on page 9 for more information.

5 Installing, Configuring, and Deploying in an eDirectory Environment

This section provides information on configuring, installing, and deploying SecureLogin in an eDirectory environment.

Choosing to install SecureLogin in an eDirectory environment installs 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.

- "Installing SecureLogin" on page 43
- "Configuring and Deploying" on page 44

Installing SecureLogin

- "Prerequisite" on page 43
- "Installation Procedure" on page 43

Prerequisite

Ensure that you meet the hardware and software requirements listed in the Quick Reference Guide (https://www.netiq.com/documentation/securelogin8/quick_start/data/quick_start.html)

Installation Procedure

1. Log in to the workstation as an administrator.
2. Run the `NetIQSecureLogin.exe` file.
3. Accept the license agreement.Click **Next**. The License Agreement page is displayed.
4. Select **NetIQ eDirectory with Novell Client**. Click **Install**.
5. Click **Next** to view the Custom Setup screen.
6. SecureLogin is by default installed in `C:\Program Files\NetIQ\SecureLogin` folder. If you want to change the location, click **Browse** and specify a different location. Select the features you want to install and click **Next**.

Configuring and Deploying

To make 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.

- "Extending the eDirectory Schema" on page 44

Extending the eDirectory Schema

You must extend the eDirectory schema to enable SecureLogin to save users' single sign-on information. The `ndsschema.exe` file is found in `Securelogin\Tools\Schema\`NDS directory extends the eDirectory schema and grants rights to existing users so that they can use SecureLogin.

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

NOTE: If you use iManager to administer SecureLogin, you must also extend the LDAP schema. For information on extending the LDAP schema "Extending the LDAP Directory Schema and Assigning Rights on the Server" on page 49.

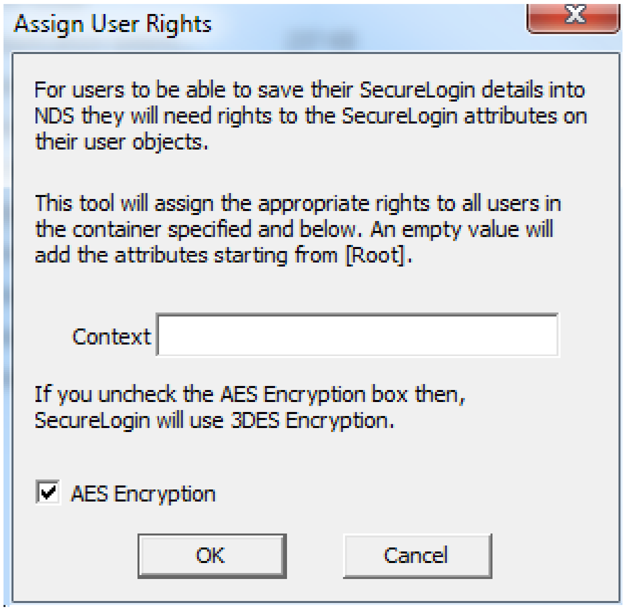
---

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 SecureLogin can assign rights to User objects under that context.



Assign User Rights

For users to be able to save their SecureLogin details into NDS they will need rights to the SecureLogin attributes on their user objects.

This tool will assign the appropriate rights to all users in the container specified and below. An empty value will add the attributes starting from [Root].

Context

If you uncheck the AES Encryption box then, SecureLogin will use 3DES Encryption.

☑ AES Encryption

IMPORTANT: The **AES Encryption** option is selected by default to use AES256 Encryption. If you unselect this option then the container will use 3DES encryption. It is recommended to use AES256 encryption.

IMPORTANT: You can run ndsschema.exe again with AES Encryption option unselected but it does not change to 3DES encryption. Use `slmanager.exe` to enable 3DES encryption.

NOTE: Rights Assignment works on root level and organizational unit level.

---

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 sub-containers, 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 Installing, Configuring, and Deploying in an LDAP Environment

This section explains installing, configuring, and deploying SecureLogin in a 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.

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 NetIQ Support for help.

This section consists of the following sections:

Prerequisites

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

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

☐ Ensure that you meet the hardware and software requirements listed in the "NetIQ SecureLogin Quick Start Guide"

☐ Server Certificates are installed and available on your LDAP server.

> **IMPORTANT:** Ensure that the `Subject Name` or `Subject Alternative Name` of the certificate in eDirectory matches with the SecureLogin LDAP server name. If it does not match, create a new eDirectory certificate with the `custom` option in iManager.

☐ Have administrator access to the server, directory, and administration workstation.

☐ If you intend to enable single sign-on for Java applications, install Java 1.7 or 1.8 on workstations prior to installing SecureLogin. You can download this from the Java Web site. (http://www.java.com)

☐ Back up the existing directory.

Installing

- "Installing SecureLogin in LDAP Environment With eDirectory" on page 48

Installing SecureLogin in LDAP Environment With eDirectory

The LDAP option installs SecureLogin into an LDAP environment with eDirectory (for example, eDirectory 8.8 or later).

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

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

1. Log in to the workstation as an administrator.
2. Run the NetIQSecureLogin.exe file.
3. Accept the license agreement.Click **Next**. The License Agreement page is displayed.
4. Select NetIQ eDirectory with LDAP as the datastore. Click Install.
5. Click Next to view the Custom Setup screen.
6. The SecureLogin is by default installed in C:\Program Files\NetIQ\SecureLogin folder. If you want to change the location, click Browse and specify a different location. Select the features you want to install and click Next.

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

Configuring

To install or upgrade SecureLogin in an LDAP directory environment, you must extend the LDAP schema with 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, NetIQ does not provide a specific tool for assigning permissions to directory attributes.

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

- "Extending the LDAP Directory Schema and Assigning Rights on the Server" on page 49
- "Using LDAP on eDirectory" on page 50

Extending the LDAP Directory Schema and Assigning Rights on the Server

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

SecureLogin Attributes

Extending the directory schema adds the following six SecureLogin attributes:

Table 6-1 *Attributes*

Attribute To Be Mapped	LDAP Mapping
Prot:SSO Auth	
Prot:SSO Entry	protocom-SSO-Entries
Prot:SSO Entry Checksum	protocom-SSO-Entries-Checksum
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 intend to use Microsoft Group Policy (GPO) support, NetIQ 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 SecureLogin installer package, then you need to copy the entire LDAP folder containing the LDAP schema files to your preferred location.

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 SecureLogin distribution package. The 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.

Assigning Rights to Schema Attributes

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

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

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

The following permissions are recommended for successful implementation:

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

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.

Deploying

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 SecureLogin on a test user account before deployment.

Use the industry standard application distribution packages such as ZENWorks, Systems Management Server, and Microsoft IntelliMirror to deploy and manage SecureLogin across large enterprises.

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

Prior to installing SecureLogin, ensure the LDAP certificate file is saved in the default certificate location of the LDAP log, for example, `securelogin\rootcert.der`. This certificate is used onlyin non-eDirectory environments.

NOTE: Copying the LDAP Certificate is necessary only in the Active Directory or Non-eDir LDAP compliant directories. This step is not necessary in default eDirectroy environments.

- "Distribution Options" on page 51
- "Configuring in a Non-eDirectory LDAP or Active Directory Environment" on page 51
- "Logging in to LDAP Directory" on page 52
- "Contextless Login" on page 53
- "Setting Up Passphrase" on page 54

Distribution Options

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

***Table 6-2** Distribution Options*

Options	Descriptions
Copy settings	Copies 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.

Configuring in a Non-eDirectory LDAP or Active Directory 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.

NOTE

- Anonymous bind needs to be enabled on the server for Non-eDirectory, Active Directory and also eDirectory environments.
- To encrypt LDAP credentials and update the system registry when anonymous bind is disabled in Active Directory, see "Updating the System Registry" on page 52.
- To encrypt LDAP credentials and update the system registry when TLS is enabled in eDirectory, see "Updating the System Registry" on page 52.

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 login dialog, click **Advanced** to expand the dialog box. If this information is blank, then populate as needed.

- **Server:** Specify the name of the LDAP server.
- **Port:** Specify the port used by the LDAP server. The default port number is 636.
- **NMAS authentication:** Select NMAS if you want to use advanced authentication to login to eDirectory.

As an administrator, you might need to include a system registry update as part of the SecureLogin deployment strategy. See "Updating the System Registry" on page 52.

Updating the System Registry

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. The values that populate the **Advanced** tab of the SecureLogin dialog box are located at:

```
HKLM\Software\Novell\Login\LDAP
```

Configuration Settings

- *Server History List (3.51.100 or later)*

  ```
  HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\Servers\server#
  ```

  Replace the # by using a numeric value. In SP1, each server item should be a multistring value (`REG_MULTI_SZ`), and can be either an IP address, or DNS name of the server. These values can be set from the installation dialogs or by an installation script. The port value can also be specified along with the server in a new line. By default, port 636 will be used.

- *Context Based Search (3.51.109 or later)*

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\LDAPSearch\ContextBasedSearch
  ```

  `DWORD` value, set to ' 1' for context-based search. Also, specify the set of contexts to search, such as `Context1, Context2 or Context3` of type `REG_SZ`, each specifying the exact context to search.

No explicit context validation is done except that LDAP search returns an appropriate error in case an invalid context is specified

- *Search Attributes (3.51.109 or later)*

  `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\LDAPSearch\SearchAttributes`

  `REG_MULTI_SZ` value, set to list of search attributes to be used in LDAP search. Any publicly readable attribute can be specified, for example `fullName`, `givenName`, `sn`, `cn`, `uid` and in AD environment you can specify `samAccountName`.

- *CertFilePath (3.51.200 or later)*

  `HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\CertFilePath`

  `REG_SZ` value lets the user to specify a valid certificate file path for non-eDirectory servers. This requires the user to create another registry entry `NonEdirLdap` of type `REG_DOWORD`. CertFilePath is considered only if `NonEdirLdap` is present and set to 1.

For more information on Configuration Settings see Registry Settings for SecureLogin in LDAP mode (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=3790292&sliceId=2&docTypeID=DT_TID_1_1&dialogID=148103339&stateId=0%200%20148101352)

Contextless Login

If you configure SecureLogin to use LDAP mode, a login page is displayed when 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 6-3 *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.

To enable LDAPAuth to perform search even when anonymous bind is disabled,ldapce.exe utilty is used. Using this utility, an administrator can create encrypted credentials for any user. The encrypted credentials must be stored in a specific registry. For detailed information on LDAPCE Utility, see "Using the LDAPCE Utility to Encrypt LDAP Credentials" on page 54.

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.

Location	Type	Name
`HKEY_LOCAL_MACHINE/SOFTWARE/ Protocom/ SecureLogin/LDAPSettings`	REG_SZ	LDAPContextlessSearchBindcreds

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

Setting Up Passphrase

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

Refer Chapter 1, "Getting Started," on page 9 for detailed information on setting up a passphrase.

7 Installing and Deploying On Standalone Environment

This section covers installing SecureLogin 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

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:

- "Prerequisites" on page 55
- "New Installations" on page 55
- "Unsupported Features" on page 55
- "Installation Overview" on page 56

Prerequisites

- You must have administrator level access to the workstation.
- Take a backup of the existing workstation cache directory.

New Installations

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

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

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

- Audits using syslog server
- Citrix and Terminal services
- Advanced Authentication
- Desktop Automation Service
- Directory Administration Tools

Installation Overview

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

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 SecureLogin review and testing, the standalone mode is intended to provide SecureLogin for individual workstations.

1. Backup the existing workstation directory.
2. Uninstall any 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 SecureLogin environment, including enabling single sign-on of the required applications.
5. Copy test user configurations to relevant objects.
6. Install the SecureLogin application on user workstation.

Installing

This section contains information on the following:

- "Installing On a Standalone Workstation" on page 56
- "Upgrading from an Earlier Version" on page 57
- "Creating a New User Account" on page 58

Installing On a Standalone Workstation

1 Log in to the workstation as an administrator.

2 Run the NetIQSecureLogin.exe file.

3 Accept the license agreement.Click **Next**. The License Agreement page is displayed.

4 Select Standalone (Trial/Testing/Demonstration) as the datastore. Click Install. If dependant components like NICI, NMAS are not present, they are installed.

5 Click Next to view the Custom Setup screen.

6 The SecureLogin is by default installed in C:\Program Files\NetIQ\SecureLogin folder. If you want to change the location, click Browse and specify a different location. Select the features you want to install and click Next.

Upgrading from an Earlier Version

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

To maintain backward compatibility, 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.

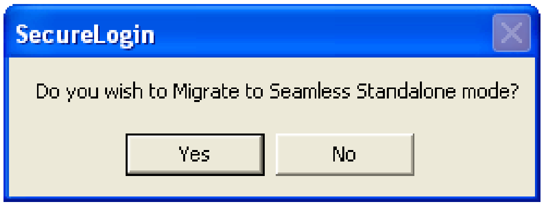
If you have been using SecureLogin in standalone mode in one account, you are automatically migrated to seamless standalone mode after providing your username and password on first log in.

Setting Up Multiple User Accounts

SecureLogin consolidates the accounts by leveraging the Windows account to verify the user. This results in one SecureLogin user for each Windows account.

After upgrading, the following message appears.

Figure 7-1 *Seamless migration message*



Do you wish to Migrate to Seamless Standalone mode?

- 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 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. SecureLogin is now active for the selected user and the SecureLogin icon appears in the notification area.

Managing SecureLogin After upgrading

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

Creating a New User Account

When SecureLogin is started after a new installation on a standalone workstation, the 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**.

8 Installing through the Command Line

This section describes how to install SecureLogin through the command line. 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 or above.

This section contains the following information.

Installation Overview

Prerequisite

SecureLogin requires the latest Microsoft Windows Installer.

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

The installation options are detailed in the following sections:

- SecureLogin Properties and Values
- Windows Installer Command Line Options

SecureLogin Properties and Values

Use the following property values to install SecureLogin.

- “Installing NSL Using response.ini File” on page 65
- “Example of a Response File” on page 66

NOTE: All the commands described in this section display details on the user interface. Use option `/quiet` to stop displaying details on the user interface displays and option `/passive` for minimal display of details on the user interface. For example : NetIQSecureLogin.exe /install /quiet X_PRIMARYSTORE=MAD.

Installing in eDirectory Environment

Table 8-1 *Command Options for Installing in eDirectory Environment*

Installation Mode	Command Line Parameters	Description
eDirectory in NDS GINA/ Credential Provider mode	`NetIQSecureLogin.exe /install X_PRIMARYSTORE=NDS`	Use this command to install SecureLogin in Graphical Identification and Authentication (GINA/Credential Provider) mode on eDirectory.
eDirectory in LDAP Credential Provider Mode/ GINA Mode	`NetIQSecureLogin.exe /install X_PRIMARYSTORE=LDAP APPENDLOCAL=SeamlessLDAPGina LDAPSERVERADDRESS=192.168.1.255`	Use this command to install SecureLogin in LDAP Credential Provider Mode/GINA mode on eDirectory. The default port is 636. To add another port, include the `LDAPPORT` in the command line. For example,`NetIQSecureLogin.exe /install X_PRIMARYSTORE=LDAP APPENDLOCAL=SeamlessLDAPGina LDAPSERVERADDRESS=192.168.1.255 LDAPPORT=359`
eDirectory in LDAP Credential Manager Mode	`NetIQSecureLogin.exe /install X_PRIMARYSTORE=LDAP APPENDLOCAL=SeamlessLDAPCred LDAPSERVERADDRESS=192.168.1.255`	Use this command to install SecureLogin in Credential Manager mode on eDirectory. The default port is 636. To add another port, include the `LDAPPORT` in the command line. For example, `NetIQSecureLogin.exe /install X_PRIMARYSTORE=LDAP APPEND_LOCAL=SeamlessLDAPCred LDAPSERVERADDRESS=192.168.1.255 LDAPPORT=389`

Installation Mode	Command Line Parameters	Description
eDirectory in LDAP Application Mode	`NetIQSecureLogin.exe /install X_PRIMARYSTORE=LDAP APPENDLOCAL=LDAPApp LDAPSERVERADDRESS=192.168.1.255`	Use this command to install 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, `NetIQSecureLogin.exe install X_PRIMARYSTORE=LDAP APPENDLOCAL=LDAPApp LDAPSERVERADDRESS=192.168.1.255 LDAPPORT=389`

Installing in LDAP v3 (non-eDirectory) Environment

Table 8-2 *Command Options for Installing in LDAP v3 (non-eDirectory) Environment*

Installation Mode	Command Line Parameters	Description
LDAP Credential Provider mode/GINA mode	`NetIQSecureLogin.exe /install X_PRIMARYSTORE=LDAP APPENDLOCAL=SeamlessLDAPGina X_NONEDIRLDAP=1 LDAPSERVERADDRESS=192.168.1.255`	Use this command to install SecureLogin in LDAP Credential Provider mode/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, `NetIQSecureLogin.exe /install X_PRIMARYSTORE=LDAP APPENDLOCAL=SeamlessLDAPGina X_NONEDIRLDAP=1 LDAPSERVERADDRESS=192.168.1.255 LDAPPORT=389`
LDAP Credential Manager Mode	`NetIQSecureLogin.exe /install X_PRIMARYSTORE=LDAP X_NONEDIRLDAP=1 APPENDLOCAL=SeamlessLDAPCred LDAPSERVERADDRESS=192.168.1.255`	Use this command to install SecureLogin in Credential Manager 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, `NetIQSecureLogin.exe /install X_PRIMARYSTORE=LDAP X_NONEDIRLDAP=1 APPENDLOCAL=SeamlessLDAPCred LDAPSERVERADDRESS=192.168.1.255 LDAPPORT=389`

Installation Mode	Command Line Parameters	Description

LDAP Application Mode	`NetIQSecureLogin.exe /install`
	`X_PRIMARYSTORE=LDAP`
	`X_NONEDIRLDAP=1`
	`APPENDLOCAL=LDAPApp`
	`LDAPSERVERADDRESS=192.168.1.255`
		Use this command to install 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,
		`NetIQSecureLogin.exe /install`
		`X_PRIMARYSTORE=LDAP`
		`X_NONEDIRLDAP=1`
		`APPENDLOCAL=LDAPApp`
		`LDAPSERVERADDRESS=192.168.1.255`
		`LDAPPORT=389`

Installing in Microsoft Active Directory Environment

Table 8-3 *Command Options for Installing in Active Directory Environment*

Installation Mode	Command Line Parameters	Description

Complete install	`NetIQSecureLogin.exe /install`
	`X_PRIMARYSTORE=MAD`
		Use this command to install SecureLogin on Microsoft Active Directory, without prompting users for any selection.

With group policies enabled	`NetIQSecureLogin.exe /install`
	`X_PRIMARYSTORE=MAD`
	`APPENDLOCAL=GPO`
		Use this command to install SecureLogin on Microsoft Active Directory with support for group policy.

Installing in Active Directory Application Mode Environment

Table 8-4 *Command Options for Installing in Active Directory Application Mode Environment*

Installation Mode	Command Line Parameters	Description

Complete install	`NetIQSecureLogin.exe /install`
	`X_PRIMARYSTORE=ADAM`
		Use this command to install SecureLogin on Microsoft Active Directory Application Mode, without prompting users for any selection.

With group policies enabled	`NetIQSecureLogin.exe /install`
	`X_PRIMARYSTORE=ADAM`
	`APPENDLOCAL=GPO`
		Use this command to install SecureLogin on Microsoft Active Directory Application Mode with support for group policy.

Installing in Standalone Environment

Table 8-5 Command Options for Installing in Standalone Mode

Installation Mode	Command Line Parameter	Description
Complete install	`NetIQSecureLogin.exe /install X_PRIMARYSTORE=DUMMY`	Use this command to install SecureLogin in a standalone mode, without any user interface.

Command for Installing the Features

When installing SecureLogin, the GPO and RunAtStartup features are installed by default. You can choose to install various features such as support for smart card and support for Citrix.

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

Table 8-6 Commands for Installing Features

Command Line Parameters	Value	Description	Example

`SMARTCARD`		Installs smartcard support.	`APPENDLOCAL=SmartCard`
			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"`

`CITRIX Server Seamless Logon`		Installs Citrix support.	`APPENDLOCAL=CitrixSeamless`
`Citrix Password Agent`		Installs Citrix support.	`APPENDLOCAL=CitrixAgent`
`LDAPPORT`	port address	Specifies the LDAP port address.	`LDAPPORT=389`
`SecureWorkstation`		Installs SecureWorkstation.	`APPENDLOCAL=SecureWorkstation`
`Admin Tools`		Specifies installing the directory administration tools.	`APPENDLOCAL=Admin`

Command Line Parameters	Value	Description	Example
`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"`
`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"`

`AAF`		Installs the files that are required for configuring Advanced Authentication.	`APPENDLOCAL = AAF`
			`X_AAFSERVERNAME=XXX.XXX.X.X`
			`X_AAFSERVERPORT=443`
			`X_AAFEVENTNAME="WINDOWS LOGON”`

TIP: APPENDLOCAL can be used to install any specific feature using the feature name. For enabling multiple features, specify the feature names separated by a comma.

For example: To install DAS, and SecureWorkstation, use APPENDLOCAL in the following manner:

APPENDLOCAL=DAS, SecureWorkstation

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

```
NetIQSecureLogin.exe
/install X_PRIMARYSTORE=MAD APPENDLOCAL=GPO
```

Installing with User Interface Option

The following example installs SecureLogin in the following setup.

- eDirectory mode.

- SecureLogin is not launched at the completion of the installation
- User is prompted to restart after the installation is complete.

```
NetIQSecureLogin.exe /install X_PRIMARYSTORE=NDS APPENDLOCAL=INSTALLADMIN
```

Silent Install

A silent install provides InstallShield Wizard with instructions for installing 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. It is recommended that you do not modify the `responsefile.ini`.

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

Installing NSL Using response.ini File

To install NSL on all the target machines with the response.ini file, execute the following command:

```
NetIQSecureLogin.exe /install X_PRIMARYSTORE=LDAP PATHTOISS="c:\temp\response.ini"
/quiet /log /log.txt
```

Substitute value of X_PRIMARYSTORE with one of the following values:

- MAD -Microsoft Active Directory
- ADAM - Active Directory Application Mode
- NDS - NetIQ eDirectory with Novell Client
- LDAP - NetIQ eDirectory with LDAP

If you try to install NSL using response.ini in any of LDAP modes (like Gina/CP, CM and App mode), then these modes have certain prerequisites like NICI, NMAS etc. So it is important to pass value for Data store along with response.ini.

For example :

NetIQSecureLogin.exe X_PRIMARYSTORE=LDAP PATHTOISS="C\Users....\response.ini" /quiet

Installation fails if we do not specify the X_PRIMARYSTORE, as prerequisites are not met.

If prerequisites like NICI and NMAS is already present in the workstation, then do not specify X_PRIMARYSTORE value in command line

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.

IMPORTANT: Non-English users must first run `MSI` with transform file and then run the `update` sequentially.

Example of a Response File

The following is an example of a response file.

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

X_CACHEDIR=%LOCALAPPDATA%

X_PRIMARYSTORE=LDAPSecretStore

X_NONEDIRLDAP=No

ADDLOCAL=Help,SecretStore,SeamlessLDAPGina,LDAPApp,WinSSO,JavaSSO,TermSSO,IESSO,FireFoxSSO,DotNetSSO,FlashSSO,DAS,RunAtStartup,Desktop,CredStore,FileExtension,DirectorySignon,SSOAut,ReadMe,PrimaryStore

LDAPSERVERADDRESS=192.168.1.25

LDAPPORT=636

LDAPSERVERADDRESS=192.168.1.26

LDAPPORT=636

LDAPSERVERADDRESS1=192.168.1.25

LDAPPORT1=636

LDAPSERVERADDRESS2=

LDAPPORT2=

X_SMARTCARDLIB=

X_CSP=

X_STOREONCARD=

EA_FAILRETRIES=3

EA_LOCKTIMEOUT=30

EA_SSPRURL=

EA_REQTIMEOUT=300

LOCATIONFORXML=

DASSERVER=

DASCONFIGOBJECT=

READERPORT=-1

CARDREADER=

AIRID=0
```

```
RETRIES=0
TREE=
SERVER=
SEQUENCE=
LDAPSERVER=
ALTERNATE1=

ALTERNATE2=
```

Windows Installer Command Line Options

Table 8-7 on page 67 lists the Windows Installer command-line options used to manually install, uninstall, and configure software and components.

Table 8-7 Windows Installer Command Line Options

Command	Usage
`/install`	Installs or configures a product.
`/repair`	Repairs a product.
`/layout`	Installs or configures a product on a network.
`/uninstall`	Uninstalls 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.
`/log`	Writes a log file after installation. By default, the log file is created in %TEMP% folder.
`/lang`	Installs in a specific locale. The default locale is English (1033). Supported locales are: ◆ 1028 - Chinese ◆ 1036 - French ◆ 1031 - German ◆ 1041 - Japanese ◆ 1034 - Spanish ◆ 1045 - Polish ◆ 1046 - Portugese

Switches Supported by SLTray.exe

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

Table 8-8 *Switches*

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

9 Installing, Configuring, and Deploying Desktop Automation Services

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" on page 69
- "Configuring" on page 76
- "Deploying" on page 79

Installing Desktop Automation Services

This section covers the following topics:

- "Overview" on page 69
- "Installing in an eDirectory Environment" on page 70
- "Installing in Other LDAP Environments" on page 71
- "Installing in Active Directory, ADAM, or Standalone Environments" on page 72
- "Installing by Using the Modify Option" on page 73
- "Accessing DAS" on page 74
- "Tips for Installing DAS" on page 75

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.

Installing in an 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 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\NetIQ\SecureLogin\`.
4. Accept the default folder

   or

   Click **Change** and navigate to your desired folder.
5. Select Novell eDirectory as the directory where SecureLogin stores its data.
6. Click **Next**. The protocols page is displayed
7. Select how you want 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 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 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**.
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 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\NetIQ\SecureLogin\Desktop Automation Services` folder of the workstation.

If you choose **Directory**, the `actions.xml` file is managed through eDirectory as described in "Managing the actions.xml File through eDirectory and iManager" on page 78. 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`.

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 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\NetIQ\SecureLogin\`.
4. ccept the default folder.

   or

   Click **Change** and navigate to your desired folder.
5. Select Novell eDirectory as the directory where SecureLogin stores its data.
6. Click **Next**. The protocols page is displayed
7. Select how you want 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 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 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**.

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\NetIQ\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.

Installing in Active Directory, ADAM, or Standalone Environments

With this release of 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 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\NetIQ\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 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 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 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 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\NetIQ\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.

Installing by Using the Modify Option

1. Launch 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 SecureLogin. It is typically installed at `C:\Program Files\NetIQ\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 77.
- For information on modifying the ConfigTree registry key, see "ConfigTree" on page 77.

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.

- "Accessing DAS through the Command Line Utility" on page 74
- "Accessing DAS through VBScript" on page 74
- "Accessing DAS through JavaScript" on page 74
- "Accessing DAS through Visual Basic" on page 75

Accessing DAS through the Command Line Utility

shortcut target = "`C:\Program Files\NetIQ\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.

Accessing DAS through VBScript

```
<SCRIPT LANGUAGE = "VBScript">

      Sub physiciansApps

      Dim as

            Set as = CreateObject("ARS.Control")

            ars.Execute("Run Physicians Applications")

      End Sub

</SCRIPT>
```

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**.

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
```

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`.

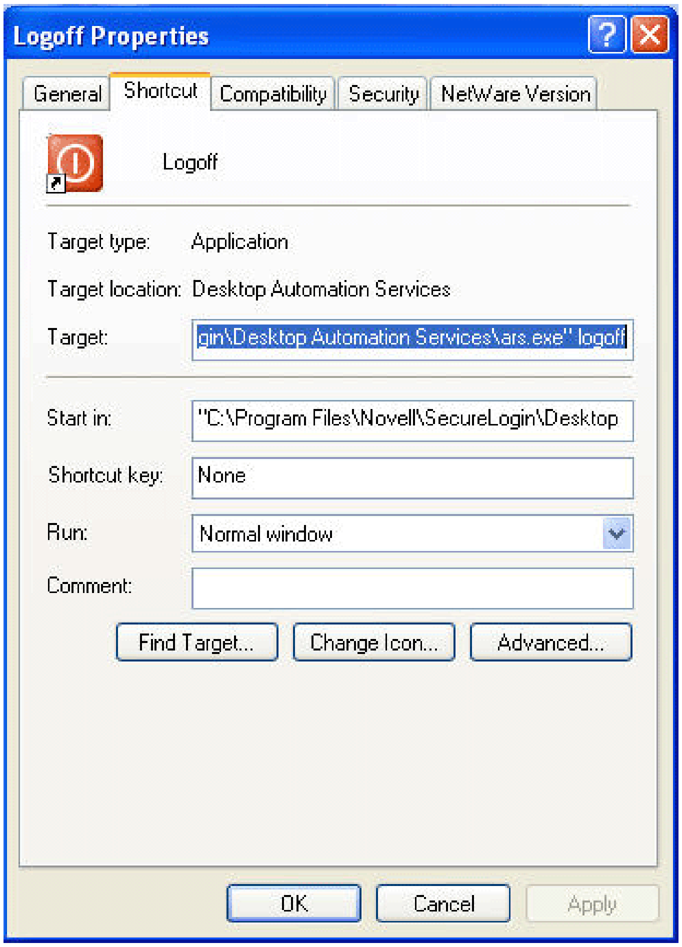
  The other way to refresh the DAS configuration is to restart the `ARSControl.exe` process or reboot the workstation.

  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 “Extending the Schema for eDirectory” on page 78 and “Installing the Plug-Ins for iManager” on page 82.
- 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\NetIQ\SecureLogin\Desktop Automation Services\ARS.exe`” logoff. This is your shortcut properties target setting.

Figure 9-1 *Logoff Shortcut Option*



Logoff

Target type: Application

Target location: Desktop Automation Services

Target: gin\Desktop Automation Services\ars.exe" logoff

Start in: "C:\Program Files\Novell\SecureLogin\Desktop

Shortcut key: None

Run: Normal window

Comment:

Configuring

This section contains the following topics:

- "Editing Environment Registry Keys" on page 76
- "Managing DAS Logs" on page 77
- "Managing the actions.xml File through eDirectory and iManager" on page 78

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\NetIQ\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.

`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.

Managing DAS Logs

You can configure the ARSControl.exe application for four levels of logging. These logs are stored in the location `%localAppdata%\SecureLogin\Logs\SSODebug.txt`. You can enable or disable DAS logging manually by updating the registry settings or using the SecureLogin Logging Manager. For more information on SecureLogin Logging Manager refer, “Managing Log Settings for SecureLogin Components” on page 17.

To enable the DAS logs using the registry settings, perform the following:

1 Click **Start -> Run**, enter `RegEdit`, then click **Ok**. The Registry Editor is displayed.

2 Browse to `HKLM\SOFTWARE\Protocom\SecureLogin\Logging\`

3 Right click and add a new key entry of type DWORD and name it as DAS.

4 Set the value for the DAS key entry as follows:

***Table 9-1** DAS Log Registry Key Values*

Value	Name or Log Type
0	Debug
1	Information
2	Warning
3	Fatal

NOTE: To disable the DAS logs, delete the respective DAS key entry from the registry.

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:

- "Extending the Schema for eDirectory" on page 78
- "Setting Workstation Registry Settings" on page 78
- "Loading the actions.xml File to eDirectory" on page 79

Extending the Schema for eDirectory

1. Locate the `ARSControl.sch` file in `C:\Program Files\NetIQ\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)

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 "Editing Environment Registry Keys" on page 76.

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\NetIQ\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.

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

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.

- "Best Practices" on page 79
- "Common Debug Issues" on page 80

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\NetIQ\SecureLogin\Desktop Automation Services\ars.exe`" /refresh

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 DAS log file(`SSODebug.txt`) indicates the syntax errors (if any) in the `actions.xml` file. If the syntax errors are not indicated, run each section separately to determine the error while parsing the `actions.xml` is executed.
- Enable the log file and set the log level to 3 (Fatal) 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 `SSODebug.txt` file after you have tested at log level 3 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.

10 Installing iManager Plug-Ins

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

Accessing iManager and Installing the iManager Plug-In

SecureLogin supports iManager 2.7.6 and above. The plug-in for iManager 2.7 are available as part of the SecureLogin Windows Installer Package, located in the `Server\IManager` folder of the product installer package.

Accessing iManager

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

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.

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.

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 SecureLogin

The iManager plug-in for 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:

- "Desktop Automation Services Plug-In" on page 82
- "SecretStore Plug-In" on page 82
- "Single Sign-On Plug-In" on page 82

Desktop Automation Services Plug-In

The Desktop Automation Services plug-in, `das.npm` is an add-on to 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.

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.

Single Sign-On Plug-In

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

Installing the Plug-Ins for iManager

The iManager plug-ins for SecureLogin are:

- **Desktop Automation Services:** `das.npm`
- **SecretStore:** **secretstore.npm**
- **Single Sign-On:** `sso.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.

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

11 Modifying, Repairing, or Uninstalling

If you have SecureLogin already installed, the Installation Wizard detects the installation and offers you several options for changing the existing configuration.

Table 11-1 *Installer Options for Changing Existing Configuration*

Option	Description
Modify	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. For more details about installing additional features, see "Using the Modify Option to Install Features" on page 85
Repair	Use the Repair operation if you want to install any missing components. The installation program detects the previously installed components and re-installs them.
Uninstall	Use the **Uninstall** operation if you want to uninstall SecureLogin and do a fresh install. For example, you previously installed an evaluation version of SecureLogin in the standalone mode. After a successful evaluation, you now want to install SecureLogin throughout your organization, which is using eDirectory.

NOTE: When you perform the modify operation, you must not change the data store of SecureLogin. You can modify the features of SecureLogin but should not modify the data store.

Using the Modify Option to Install Features

If you have not installed some of the features such as Smartcard during the initial installation of SecureLogin, you can to do it later through the **Modify** option.

The following example explains installing Smartcard through the Modify option.

1. Run the `NetIQSecureLogin.exe` file.
2. Select **Modify** option.
3. Select a datastore.
4. From the **Custom Setup** screen, select **Smartcard**.
5. Click **Next** to install.

Modify Option and Group Policy Objects Support

During a fresh install of 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.

12 Upgrading

Prerequisites

Before you upgrade:

- Identify mobile and kiosk workstation users.
- Complete your migration plan.
- Back up your SecureLogin data by exporting to an XML file.
- Close SecureLogin. You cannot run the application during an upgrade.
- In iManager, before upgrading SecureLogin single sign-on plug-in(`sso.npm`), you must first delete the existing `jssoapi.jar or jsso-api.jar` from the location `imanager\tomcat\webapps\nps\WEB-INF\lib` and restart the tomcat server that hosts the iManager.

Phased Upgrading

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.

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 SecureLogin version 3.5 is currently implemented. All users are managed from one administration workstation. ZENworks is used for application distribution and deployment generally occurs overnight.

Sales OU users have laptops for mobile access to the network. The Central Administration OUs contain a combination of static workstations and laptop users. Manufacturing and Purchasing OU users are mobile; workstations are accessed in Kiosk mode. Users in the remaining OUs are each allocated a workstation for their sole use.

The Java functionality provided by the new version of SecureLogin is eagerly awaited by users in the Sales group, so they have volunteered to test the upgrade. After the upgrade is successfully deployed to the Sales group, 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 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 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 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 SecureLogin upgrade on workstations associated with the following OUs:

- Accounting
- Marketing

Day 5: Review and resolve any issues.

Day 6: Install the SecureLogin upgrade on workstations associated with the following OUs:

- Manufacturing
- Purchasing

Review any upgrade issues encountered by Central Administration OU users. If 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 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.

Upgrading SecureLogin

- "Supported Upgrade Paths" on page 90
- "Upgrading Using the Installer" on page 90
- "Upgrading Through The Command Line" on page 90

Supported Upgrade Paths

You can upgrade to SecureLogin 8.5 from SecureLogin 8.0.

If you are on earlier version of SecureLogin like 7.0, you cannot upgrade directly to version 8.5. You first need to upgrade to version 8.0 and then run the 8.5 installer to finish the upgrade process.

Upgrading Using the Installer

1. Run `NetIQSecureLogin.exe`.
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**.

Upgrading Through The Command Line

1. Use the following command to update silently:

   NetIQSecureLogin.exe /install **|** / quiet

Upgrading Desktop Automation Services

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

Upgrading Advanced Authentication

During an upgrade, if AA is selected then it copies all files and registries related to the Advanced Authentication feature.

NOTE:

1. After upgrading SecureLogin, the re-authentication method needs to be the same as configured for the Advanced Authentication feature. To ensure this, navigate to Edit Wizard > Re-Authentication and select the appropriate logon method.
2. After upgrading SecureLogin, the older 4.x interface to connect to Advanced Authentication 4.x server is displayed along with newer interface. To resolve this, the user needs to uninstall the 4.x SecureLogin Advanced Authentication plugin and use the latest interface which connects to 5.x Advanced Authentication server.

13 Uninstalling SecureLogin

Remove the 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 **NetIQ SecureLogin**.
3. Click **Remove**.

A Extending OpenLDAP Schema to Support SecureLogin

1. Copy `SecureLoginSSO.schema` and `SecureLoginSSO2.schema` to the `/etc/openldap/schema` folder. The OpenLDAP schema files can be found on the SecureLogin CD in the path of `<CD>/SecureLogin/Tools/Schema/OpenLDAP`.
2. Edit the `slapd.conf` file, and ensure that the following lines are included:

```
#include    /etc/openldap/schema/core.schema
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/misc.schema
include /etc/openldap/schema/openldap.schema
# NetIQ  ADDED THE FOLLOWING LINE
include /etc/openldap/schema/SecureLoginSSO.schema
include /etc/openldap/schema/SecureLoginSSO2.schema
```

3. Edit the `ldap.conf` file and ensure that the following lines are included:

```
#
# LDAP Defaults
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE  dc=example, dc=com
#URI  ldap://ldap.example.com ldap://ldap-master.example.com:666

#SIZELIMIT  12
#TIMELIMIT  15
#DEREF    never

HOST openldap.com
PORT 636
TLS_CACERT /ssl/certs/cacert.pem
TLS_REQCERT demand
```

4. Open the core.schema file and make the following changes:

```
objectclass ( 2.5.6.4 NAME 'organization'
  DESC 'RFC2256: an organization'
  SUP top STRUCTURAL
  MUST o
  MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
    x121Address $ registeredAddress $ destinationIndicator $
    preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
    telephoneNumber $ internationaliSDNNumber $
    facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
    postalAddress $ physicalDeliveryOfficeName $ st $ l $ description $
protocom-SSO-Entries $ protocom-SSO-Auth-Data $ protocom-SSO-Security-Prefs $
protocom-SSO-Entries-Checksum $ protocom-SSO-Security-Prefs-Checksum $
protocom-SSO-Profile ) )
```

```
objectclass ( 2.5.6.5 NAME 'organizationalUnit'
  DESC 'RFC2256: an organizational unit'
  SUP top STRUCTURAL
  MUST ou
  MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
    x121Address $ registeredAddress $ destinationIndicator $
    preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
    telephoneNumber $ internationaliSDNNumber $
    facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
    postalAddress $ physicalDeliveryOfficeName $ st $ l $ description $
protocom-SSO-Entries $ protocom-SSO-Auth-Data $ protocom-SSO-Security-Prefs $
protocom-SSO-Entries-Checksum $ protocom-SSO-Security-Prefs-Checksum $
protocom-SSO-Profile ) )

objectclass ( 2.5.6.6 NAME 'person'
  DESC 'RFC2256: a person'
  SUP top STRUCTURAL
  MUST ( sn $ cn )
  MAY ( userPassword $ telephoneNumber $ seeAlso $ description $ protocom-SSO-
Entries $ protocom-SSO-Auth-Data $ protocom-SSO-Security-Prefs $ protocom-SSO-
Entries-Checksum $ protocom-SSO-Security-Prefs-Checksum $ protocom-SSO-Profile
) )
```