Novell Nsure™ SecureLogin

3.51.2

www.novell.com

ADMINISTRATION GUIDE

April 08, 2005

Novell®

Legal Notices

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

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

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

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

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

www.novell.com

Nsure SecureLogin 3.51.2 Administration Guide
April 08, 2005

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

Novell Trademarks

Third-Party Materials

Contents

About This Guide

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

- Chapter 1, "Overview," on page 11
- Chapter 2, "Managing SecureLogin," on page 19
- Chapter 3, "Using Login Watcher," on page 87
- Chapter 4, "Working with Terminal Emulators," on page 89
- Chapter 5, "Troubleshooting SecureLogin," on page 115
- Appendix A, "Prebuilt Scripts," on page 129
- Appendix C, "MS Terminal Server and Citrix MetaFrame Environments," on page 133
- Appendix D, "Finding Control IDs and Offsets of an Emulator," on page 135
- Appendix E, "Finding HLLAPI Types," on page 147
- Appendix F, "Error Codes," on page 151

Documentation Conventions

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

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

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

User Comments

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

Documentation Updates

For the most recent version of the *Novell SecureLogin 3.51.2 Administration Guide*, see the Novell documentation Web site (http://www.novell.com/documentation).

Additional Documentation

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

- The Help systems in SecureLogin on the desktop as well as SecureLogin snap-ins to ConsoleOne® or Microsoft* Management Console.
- The Nsure SecureLogin 3.51.2 Installation Guide (installing SecureLogin, migrating secrets from earlier versions, and configuring Secure Workstation)
- The Nsure SecureLogin 3.51.2 Scripting Guide (concepts concerning scripting, scripting commands, and example scripts for applications)
- The Nsure SecureLogin 3.51.2 Terminal Services Guide (configuring Citrix servers)
- The Nsure SecureLogin 3.51.2 Configuration Guide for Terminal Emulation (how to configure Terminal Launcher for selected terminal emulators)
- The Nsure SecureLogin 3.51.2 User Guide (using SecureLogin to enable applications for single sign-on)

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

1 Overview

This section provides information about the following:

- "SecureLogin As a Solution" on page 11
- "Understanding SecureLogin" on page 12
- "What's New" on page 18

SecureLogin As a Solution

Novell® SecureLogin's single sign-on technology eliminates the need for users to remember their usernames and passwords beyond their initial network login. Single sign-on stores the usernames and passwords that each user needs and then automatically enters them for the user when required.

Single sign-on increases productivity because users no longer need to enter usernames and passwords. The computer does it for them. As a result, single sign-on greatly reduces the number of calls to help desks concerning forgotten passwords.

Novell SecureLogin is comprised of multiple integrated security systems that provide authentication and single sign-on to networks and applications throughout an organization. The goals are to provide a single entry point to the corporate network and its resources for users, increase security, and improve compliance with corporate security policies.

The separate single sign-on modules (components) of SecureLogin are designed for generic Windows*, Internet, and terminal emulator applications. SecureLogin's unique modular design allows it to be compatible with most new applications.

Security is an important feature of SecureLogin. SecureLogin stores all user credentials encrypted in the directory (Novell eDirectory™, Active Directory*, and other LDAP-compliant directories) and optionally caches details in an encrypted format on the local workstation. The only user who can unlock the encrypted data is the user that the details are stored for. For example, a network administrator with all rights is not able to view or use a user's password credentials.

SecureLogin is easy to use. Wizards, corporate scripts, predefined applications, and eDirectory enable you to centrally configure SecureLogin for use in the corporate network. SecureLogin includes a workstation administration tool that allows users to view their single sign-on details and, if you permit them to, add new applications and Web sites for single sign-on.

Locally encrypted caching enables SecureLogin to maintain single sign-on integrity for all mobile and remote users, regardless of network connectivity. If you permit them to, mobile users can update their single sign-on credentials when disconnected from the network and later update the directory with these details when the users are next attached.

Because SecureLogin is a directory-enabled product, users can

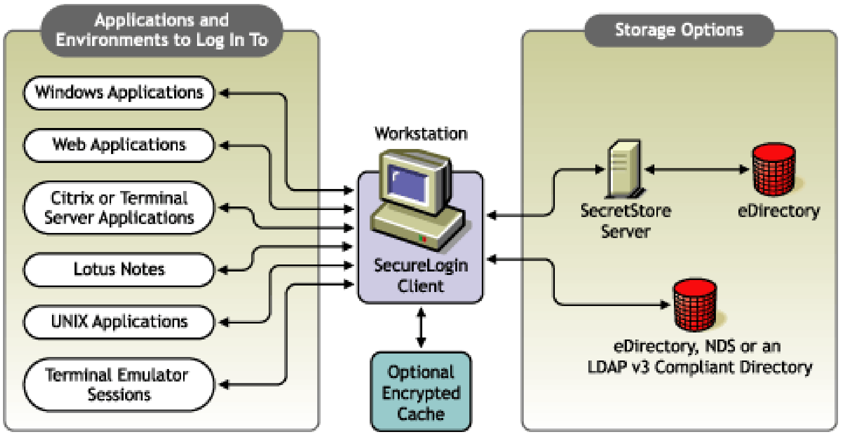
- Log in from anywhere and get the same capabilities as if they were at their own desks.

- Log in and log off quickly, because they only authenticate to the directory, not to Windows itself.
- Roam the enterprise, logging into several different machines during the day.
- Work on a notebook or laptop in a disconnected mode, because their login credentials are saved to a local, encrypted cache.
- Securely use a shared, kiosk-type workstation, where many people log in temporarily for quick work and then log out.

Understanding SecureLogin

SecureLogin Architecture

SecureLogin is a suite of applications for authentication and single sign-on. As the following figure illustrates, it includes components for both client and server:



SecureLogin works by keeping a record of user authentication credentials and instructions on how to use those credentials. SecureLogin stores these credentials in the directory, either directly or through the patented Novell SecretStore® technology. At runtime, SecureLogin detects login opportunities, retrieves the appropriate authentication credentials, then automatically supplies those credentials.

Script Language

The SecureLogin script language is a key feature of SecureLogin single sign-on. This language enables the product to be compatible with almost all network environments and applications.

SecureLogin uses the scripting language to provide a flexible single sign-on and monitoring environment. For example, the SecureLogin Windows Agent watches for application login boxes. When a login box is identified, the agent runs a script to enter the username, password, and background authentication information.

The script language is used in individual application scripts to retrieve and enter the correct login details. These scripts are stored and secured within the directory to ensure maximum security, support for single-point administration, and manageability.

The script language can be used to automate many login processes, such as multi-page logins and login panels requiring other information that can be stored in the directory (such as surname and telephone number). The script language also contains the commands required to automate password changes on behalf of users and request user input when it is required.

The scripting language has the following advantages:

- Enables you to define single sign-on methods for almost any Windows, mainframe, Internet, intranet, Terminal Server, or UNIX* application.
- Allows more sophisticated single sign-on to supported applications, including the ability to seamlessly handle several versions of one application.

  This feature is especially important when you upgrade your applications.
- Provides full control of which applications can be used for single sign-on.
- Provides the ability to update the entire directory database with a new application login script by updating a single object.
- Enables you to store corporate scripts in a Container object rather than individual User objects.

SecureLogin Components

SecureLogin provides the SecureLogin workstation client and snap-ins to ConsoleOne®, Active Directory, and LDAP.

SecureLogin leverages your existing directory so that you can administer single sign-on solutions for applications, users, and the entire organization. With the SecureLogin administration tools, you can centrally manage users and corporate single sign-on applications and configurations.

SecureLogin includes the following utilities:

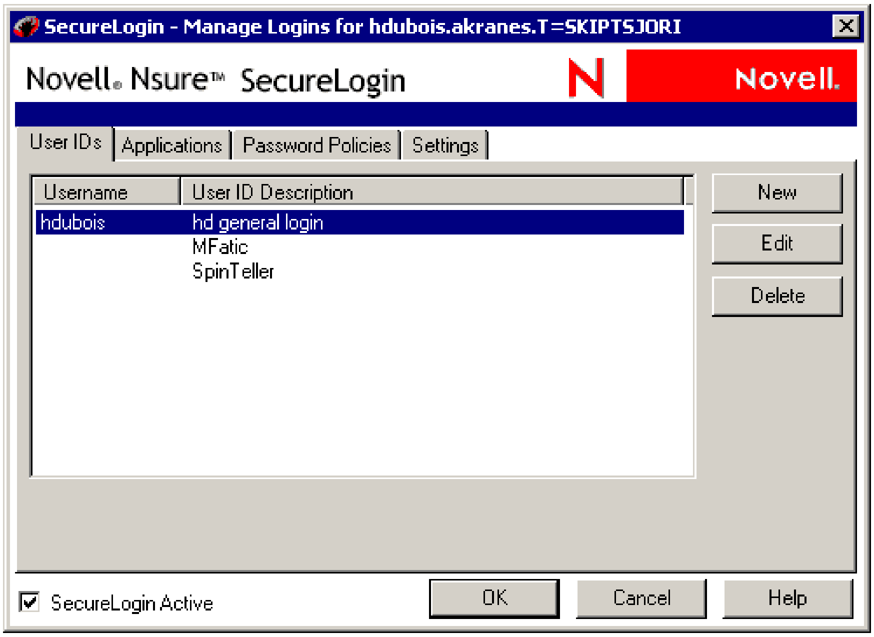
- Workstation Administration
- Container and User object snap-ins
- Terminal Launcher
- Window Finder
- Login Watcher

SecureLogin provides support for

- Mainframes
- Corporate scripts
- Prebuilt scripts for a wide range of Windows applications
- Internet browsers
- Lotus* Notes*
- Mobile single sign-on
- Novell SecretStore
- ConsoleOne, Microsoft Management Console (MMC), and LDAP
- NMAS
- One-time passwords

The SecureLogin Application

Novell SecureLogin runs on the desktop. Users and administrators can use this tool to manage their single-sign-on logins. The following figure illustrates SecureLogin's main window:


SecureLogin - Manage Logins for hdubois.akranes.T=SKIPTSJORI
Novell. Nsure™ SecureLogin
Novell.
User IDs
Applications
Password Policies
Settings
New
Edit
Delete
OK
Cancel
Help

Username	User ID Description
hdubois	hd general login
	MFatic
	SpinTeller

☑ SecureLogin Active

This tool enables users to do the following at their workstations:

- Add new applications for single sign-on
- Manage logins by viewing existing applications and Web sites that single sign-on is enabled for.
- Modify passwords to existing single sign-on enabled sites.
- Change settings and preferences

To access this tool:

- Click Start > Programs > Novell SecureLogin > Novell SecureLogin.
- Double-click the SecureLogin icon on the workstation's task bar (system tray).

Terminal Launcher

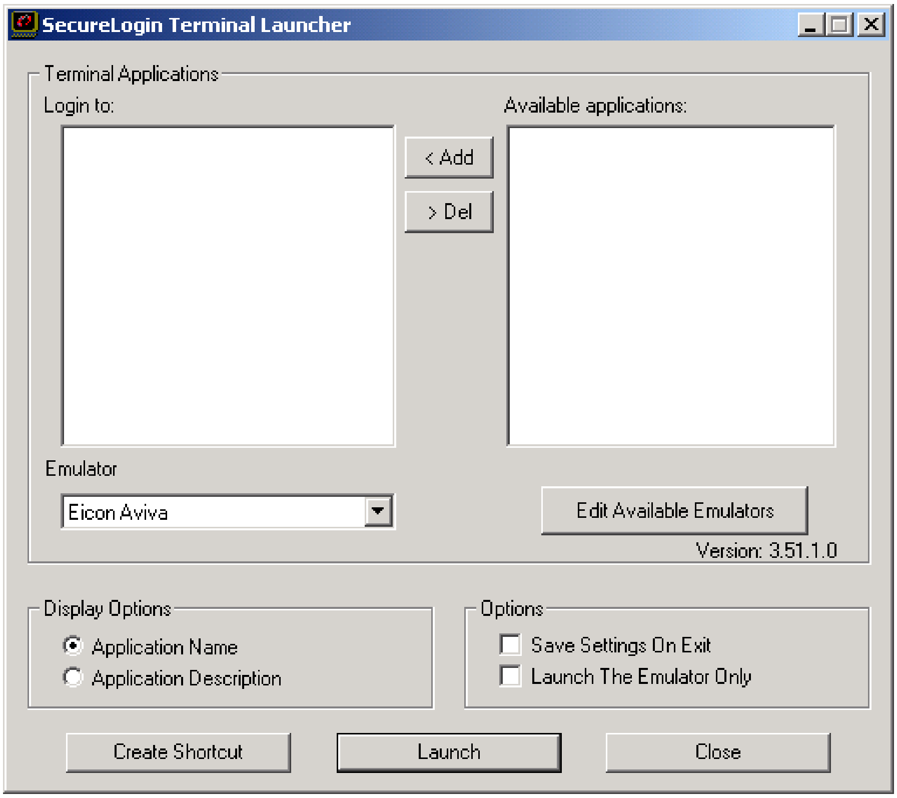
Terminal Launcher enables you to log in to any type of host that requires a user to log in using an emulator (for example, an ACF2 or RACF mainframe, a UNIX host, or a Cisco* router). Either you or the user configures Terminal Launcher to connect to the mainframe or host, wait for the login sequence, and then enter usernames and passwords.

Terminal Launcher enables you to easily launch terminal emulation sessions and to run a script within those sessions.

The script is stored within your configured host directory (for example, eDirectory, Active Directory, or LDAP), which makes it more secure than generic scripts that are written in a particular language for a particular emulator. These scripts are designed to be compatible with many different emulators.

Terminal Launcher can be used to provide shortcut icons to mainframe or UNIX applications, removing the need for user intervention.

The following figure illustrates Terminal Launcher:



Emulator: Eicon Aviva

Version: 3.51.1.0

● Application Name
○ Application Description

□ Save Settings On Exit
□ Launch The Emulator Only

To access Terminal Launcher, click Start > Programs > Novell SecureLogin > Terminal Launcher.

Corporate Login Scripts

SecureLogin is designed for large networks. It supports the ability to use the directory to centralize the setup of the single sign-on applications. This feature is referred to as corporate login scripts.

A corporate login script can be stored in either a file system or in a Container object located in the directory. This feature gives you the ability to write and define single sign-on scripts once for the whole organization, while still allowing for customized subordinate Container objects and User objects. This customization significantly reduces the effort and complexity of enterprise deployment.

If a subordinate object has a different script for the same application defined locally, the local copy will be used instead of the version that is on the higher object. If a script is defined on a User object with the same name as a script defined on a Container object, or if there are two scripts with the same name on different level Container objects, the script from the subordinate object will always be used instead of the script in the higher level object. This strategy allows for specialization in corporate scripts.

Prebuilt Scripts

SecureLogin includes prebuilt scripts for many applications. These allow for quicker and easier integration of single sign-on for a broad range of industry standard applications.

Internet Browsers

The Microsoft* Internet Explorer and Netscape* components enable applications that are accessed through these browsers to use single sign-on. Depending on a workstation's configuration, the browsers might behave differently.

These components also enable sites using http dialogue authentication to use single sign-on.

Lotus Notes

The SecureLogin Lotus Notes component enables you to use single sign-on easily with Lotus Notes. At the end of the Notes password expiration period, SecureLogin can prompt for a new password or automatically populate the password field with a new random value.

In addition to controlling single sign-on, this component supports

- Multiple ID files for each user
- The ability to exclude certain administrative IDs from being enabled for single sign-on

Mobile Single Sign-On

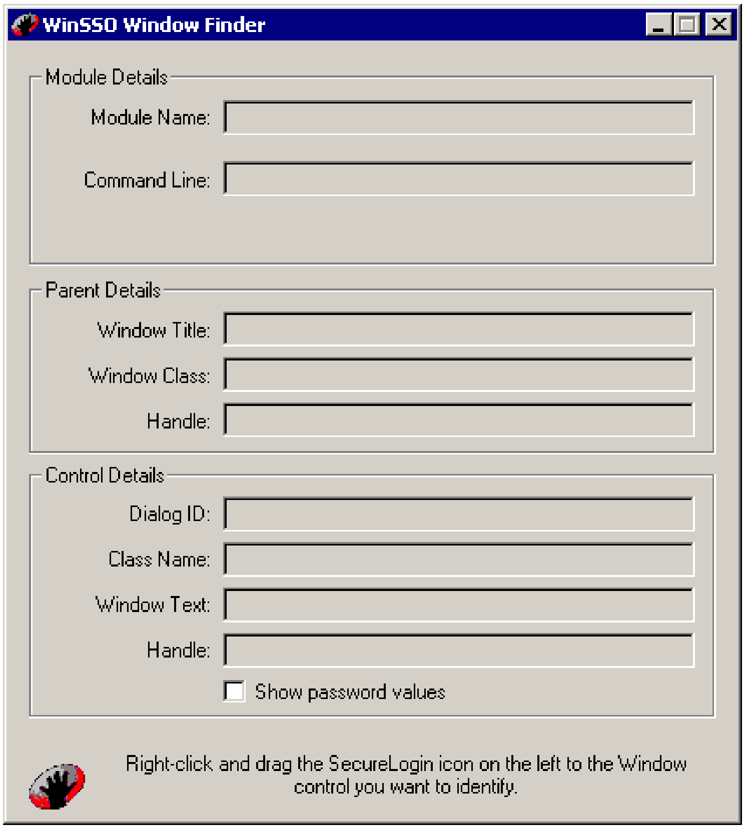
Taking advantage of the directory architecture, SecureLogin allows users to roam with their authentication details. Because there are no workstation dependencies, users can move freely from office to office. Their credentials follow them.

By using the local encrypted cache, SecureLogin also allows notebook users access to single sign-on while those users are disconnected from their network environment.

Window Finder

Window Finder can be used to gather information about a window containing a login box. The information shown by Window Finder can be helpful in creating new SecureLogin scripts for complex environments or to troubleshoot existing ones.

The following figure illustrates Window Finder:



Right-click and drag the SecureLogin icon on the left to the Window control you want to identify.

To access Window Finder, click Start > Programs > Novell SecureLogin > Window Finder.

Login Watcher

Login Watcher can assist with gathering information about an application that a user may want to single sign-on enable. When run at the same time as an application, Login Watcher captures information such as key and button actions used in the application and saves that information to a log file.

SecretStore

When SecureLogin is used with eDirectory, you can use SecretStore, a patented Novell technology, to store your application passwords and other authentication credentials. SecretStore is a repository located within your eDirectory User object.

SecretStore provides an added level of protection and security to SecureLogin. Only the SecretStore server can access secrets, and each secret is stored separately, so that access to data is very compartmentalized and controlled. SecretStore also provides additional capabilities to deter would-be intruders, whether internal or external to your organization.

You can share secrets among services. See “Interoperability Issues” as well as “Sharing Secrets with Novell Portal Services” in the *Novell SecretStore 3.3.3 Administration Guide* (http://www.novell.com/documentation/secretstore33/index.html).

SecretStore runs on all eDirectory platforms: NetWare® 5.1, NetWare 6 or later, Windows NT/XP/2000/2003, Linux*, and Solaris*.

Snap-Ins to Manage SecureLogin

The following tools enable you to manage SecureLogin, so that users have a secure and productive single-sign-on environment:

- SecureLogin snap-in to ConsoleOne
- SecureLogin snap-in to MMC
- SecureLogin Manager (slmanager.exe)

One-Time Passwords

SecureLogin 3.51.2 supports one-time passwords. This method provides background authentication and sign-on to back-end systems. Instead of using a password, this method uses a cryptographic key process to securely authenticate the user to the remote system.

Rather than simply typing in the username and password for a user, SecureLogin can effectively take over the authentication process of the application using a shared cryptographic key between different platforms (such as the LAN and mainframe). This can only be achieved on applications that give programmers interfaces into their products, so that one-time password functionality can happen.

To leverage one-time passwords with SecureLogin, you must purchase a third-party product for the application/server environment supporting the OTP authentication. This third-party product must be installed on the system that SecureLogin authenticates to. For example products, see One Time Password Authentication (http://www.ietf.org/html.charters/otp-charter.html).

What's New

SecureLogin 3.51.2 includes the following new and enhanced features:

General Features

- Improved SecretStore performance

Configurable Features

- LDAPAuth support for file-based certificates

  Now you can specify a certificate file through the registry while authenticating to non-eDirectory™ servers including Active Directory and Sun One directory.
- Configurable LDAP user attribute value in the GINA dialog box
- Configurable printable format for entries in Duplicates Resolution dialog box
- Configurable context-based search
- Configurable LDAP search attributes

NOTE: To make the configurable features mentioned above functional, refer to TID 10093336 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093336.htm) on the Novell Support Web site.

2 Managing SecureLogin

This section provides information on the following:

Accessing Management Tools

You can manage Novell® SecureLogin at the workstation level or at the container or Organizational Unit (OU) level.

- The workstation level

  Each workstation running SecureLogin has a SecureLogin client. This client can only alter the current user's SecureLogin information. However, changes made from SecureLogin's main window on the desktop override settings made at a container or organizational unit level.

  For information on using the SecureLogin client, see the following:

  - The Help system in the SecureLogin client
  - The Nsure SecureLogin 3.51.2 User Guide

- The container or OU level

  You can use the following management utilities:

  - The SecureLogin snap-in to ConsoleOne®, installed on a workstation

    To use ConsoleOne, select the eDirectory™ option while installing SecureLogin.

- The Microsoft Management Console (MMC), which runs on a Windows server

  MMC is installed with Active Directory. The snap-in to MMC is installed if you select the Active Directory option while installing SecureLogin.

- SecureLogin Manager (slmanager.exe)

  SecureLogin Manager is useful if you have selected the LDAP option while installing SecureLogin.

You use the same processes at the workstation as from ConsoleOne or a Windows server. The same functionality exists in ConsoleOne, MMC, or SecureLogin Manager.

Accessing SecureLogin in ConsoleOne

Before you can access ConsoleOne, you must complete the following:

- Extend the eDirectory schema.
- Have ConsoleOne, the SecureLogin snap-in to ConsoleOne, and SecureLogin running on an administrative workstation in an eDirectory environment.

  IMPORTANT: Install ConsoleOne and the SecureLogin snap-in files to the same directory. Otherwise, the SecureLogin snap-in files won't work.

- Install and run SecureLogin locally.

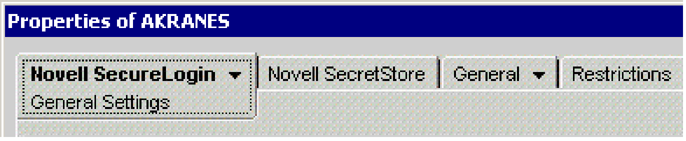
For information on these tasks see "Installing in Novell eDirectory Environments" in the *Nsure SecureLogin 3.51.2 Installation Guide*.

To access SecureLogin in ConsoleOne:

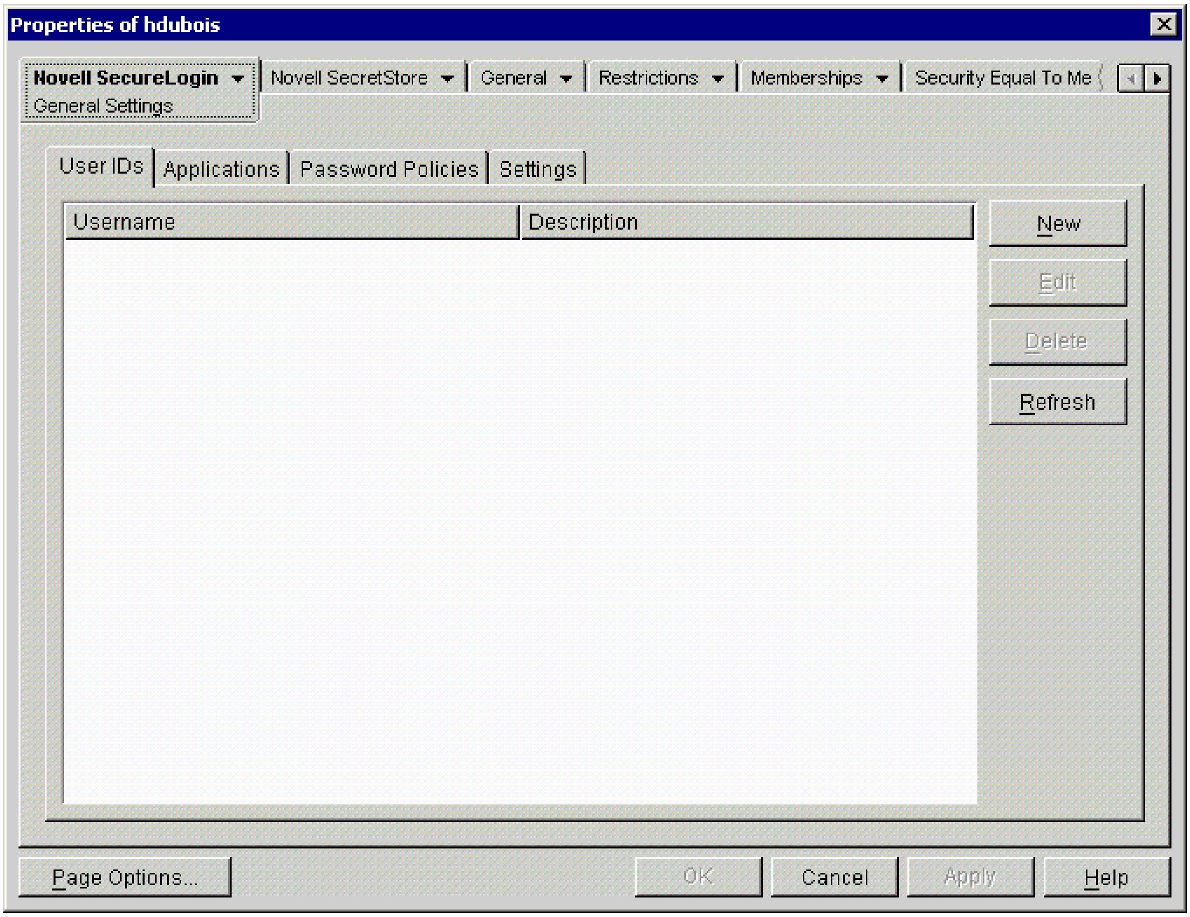
1. Run consoleone.exe.

   Typically, this file is found in the \novell\consoleone\1.2\bin directory on a local drive. Place a shortcut on your desktop, then run ConsoleOne from there.

2. Select a Container or User object, then click Properties.
3. Click Novell SecureLogin.



The following figure illustrates options on SecureLogin's main page in ConsoleOne. You can add user IDs, enable applications for single sign-on, create password policies, manage settings, and copy settings.



User IDs: Used to configure stored credentials that are linked to applications.

These credentials include usernames, passwords, or IP addresses. Because user IDs set at the container level apply to all users in the container, you can use this page to set up login access for a group of users where there is no requirement for individual user logins. See "Managing User IDs" on page 25.

Applications: Used to configure applications available for single sign-on.

This page displays applications that are enabled for single sign-on. You can manually add applications to the list or use the Add Applications Wizard. See "Managing Applications" on page 34.

Password Policies: Used to configure the settings and organizational rules for passwords.

See "Managing Password Policies" on page 43.

Settings: Used to configure users' SecureLogin environment, including the types of applications authorized for single sign-on.

See "Managing Administrative and User Settings" on page 52.

Copy Settings: Used to copy, export, and import settings, scripts, and user IDs across containers.

See "Copying, Exporting, and Importing SecureLogin Settings" on page 79.

Accessing SecureLogin from MMC

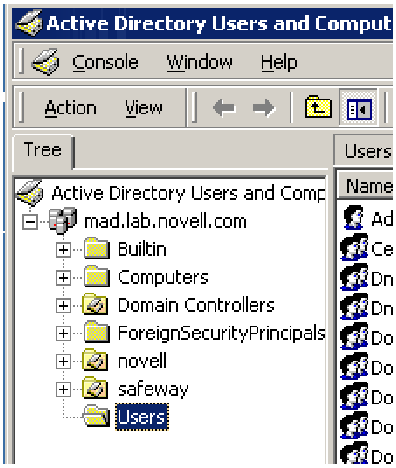
Before you can access MMC, you must complete the following tasks:

- Install the Microsoft Windows 2000 or 2003 Server family operating systems (including Active Directory) on at least one domain controller in your network.
- Complete administrative tasks (including extending the Active Directory schema).
- Install SecureLogin for Active Directory.
- Have SecureLogin running on the workstation.

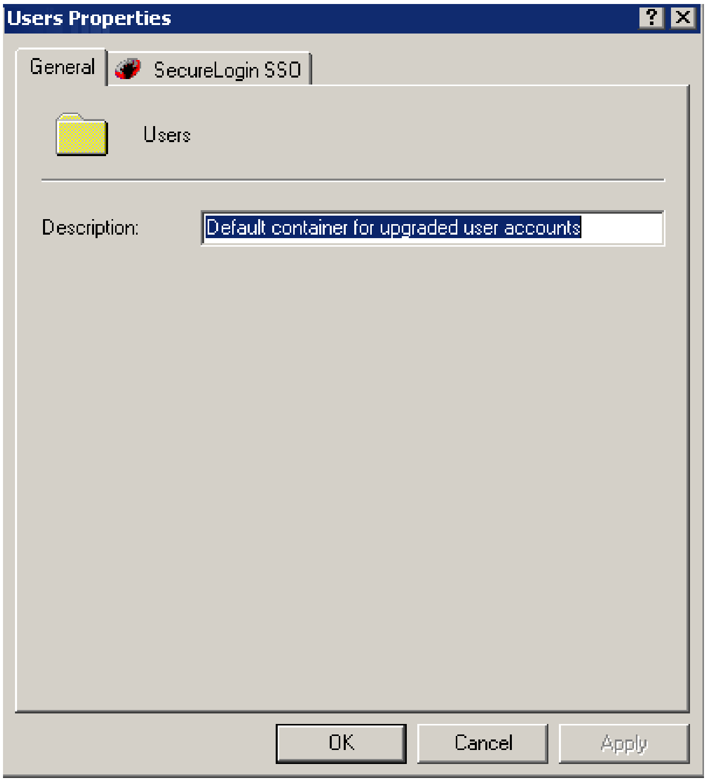
For information on these tasks, see "Installing in Active Directory Environments" in the *Nsure SecureLogin 3.51.2 Installation Guide*.

To access SecureLogin:

1. Click Start > Programs > Administrative Tools > Active Directory Users and Computers.
2. In the Active Directory Users and Computers pane, right-click an organizational unit (for example, Users).

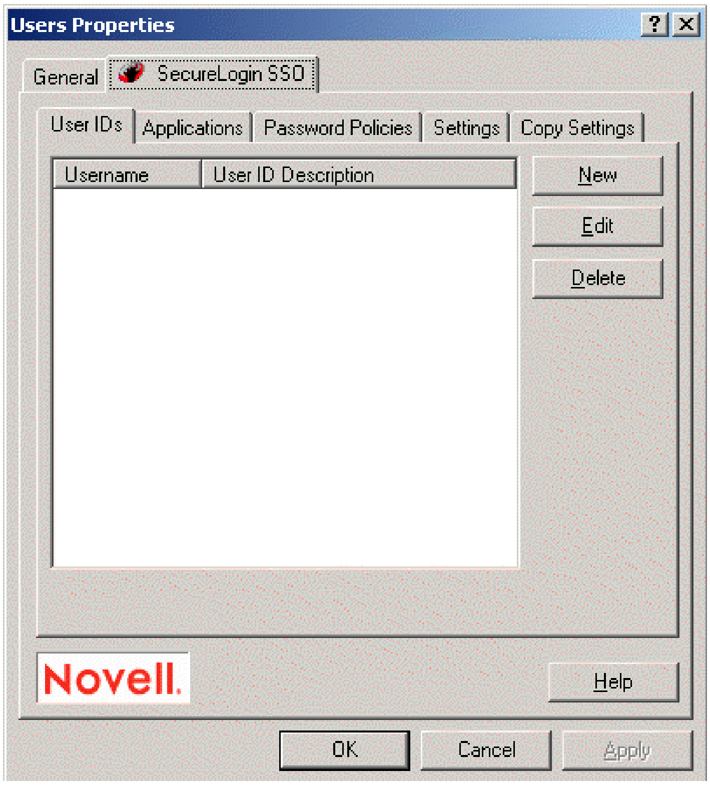


3. Click Properties, then click SecureLogin SSO.



Description: Default container for upgraded user accounts

As the following figure illustrates, options on SecureLogin's main page in MMC enable you to add user IDs, enable applications for single sign-on, create password policies, manage settings, and copy settings.



User IDs: Used to configure stored credentials that are linked to applications.

These credentials include usernames, passwords, or IP addresses. Because user IDs set at the container level apply to all users in the container, you can use this page to set up login access for a group of users where there is no requirement for individual user logins. See "Managing User IDs" on page 25.

Applications: Used to configure applications available for single sign-on.

This page displays applications that are enabled for single sign-on. You can manually add applications to the list or use the Add Applications Wizard. See "Managing Applications" on page 34.

Password Policies: Used to configure the settings and organizational rules for passwords.

See "Managing Password Policies" on page 43.

Settings: Used to configure users' SecureLogin environment, including the types of applications authorized for single sign-on.

See "Managing Administrative and User Settings" on page 52.

Copy Settings: Used to copy, export, and import settings, scripts, and user IDs across containers and domains.

See "Copying, Exporting, and Importing SecureLogin Settings" on page 79.

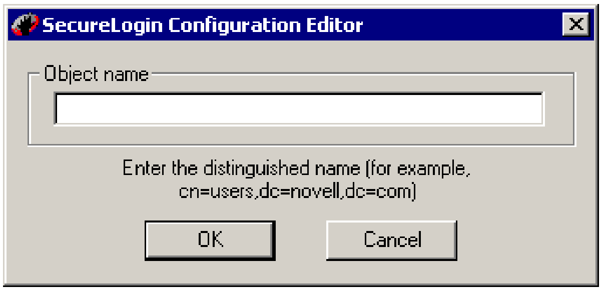
Accessing SecureLogin from SecureLogin Manager

SecureLogin Manager doesn't run on Windows 9.*x* workstations.

To access SecureLogin Manager:

1 Run slmanager.exe.

This file is in the \securelogin\tools directory.



Enter the distinguished name (for example, cn=users,dc=novell,dc=com)

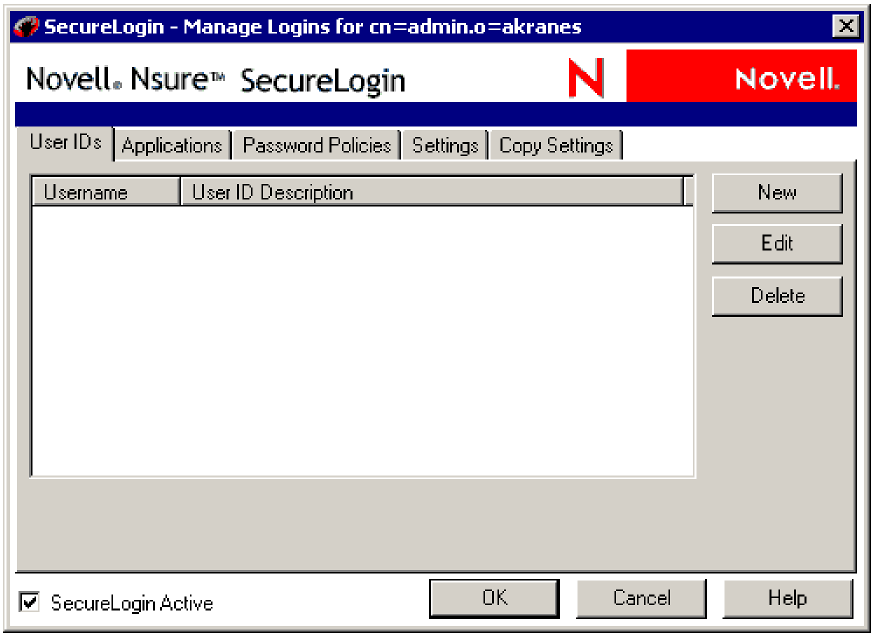
2 Log in as administrator.

In the Object Name text box, type a complete distinguished name. For LDAP and Active Directory, use LDAP conventions, as the figure in Step 1 illustrates.

For eDirectory, use eDirectory conventions. For example, type

```
cn=RDev.o=novell
```

The following figure illustrates SecureLogin Manager's main page:



☑ SecureLogin Active

Managing User IDs

After an application is enabled for single sign-on, SecureLogin prompts the user to enter login credentials in a SecureLogin dialog box. SecureLogin then stores these credentials, associating them with the relevant application script for use in subsequent logins. These credentials are displayed and managed in the User IDs page.

A user ID consists of whatever is required of a user to authenticate to a network or directory. For example, authentication to a Windows application might require a domain name, password, or PIN. Authentication to a Web application might require an IP address.

Credentials are linked to an application and can be stored at any object level. Credentials stored at the container or OU level apply to all users in that container or OU. For example, if everyone in the RDev department accesses an application on a specific domain, you can preset the domain in the User ID page. Users then don’t have to enter the domain manually. Also, you can change the domain name at any time without any affect to users.

Another example is a Web-based application that all users in an organization access by using the same username and password. If you set the password and username credentials for the application at the container or OU level, the username and password are preset for all users in that container or OU.

User IDs are especially useful when two or more applications can use the same credentials.

Scenario: Sharing a User ID. On the Applications page, you added GroupWise.exe, a Windows application. You also added gmail.digitalairlines.com, a Web application. At the ID page, you create a user ID named GroupWise. You link both applications to this user ID. Authorized users can now use single sign-on to access GroupWise® from a Windows environment (grpwise.exe) or a Web environment (http://gmail.digitalairlines.com).

If you change the password for one application, SecureLogin updates the password in one location. All applications that use that password automatically get the update.

You use the user ID feature to do the following:

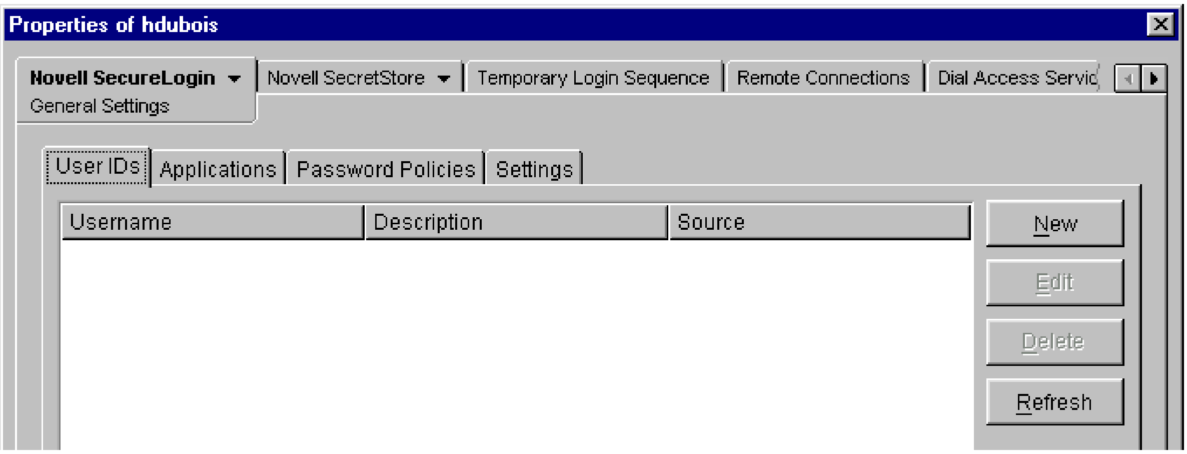
- View, add, edit, or delete user IDs.
- Link user IDs to additional applications.
- Define a user ID that several different applications can share.

You manage user IDs by using the SecureLogin snap-in to ConsoleOne, Active Directory Users and Computers in MMC, SecureLogin Manager, or the SecureLogin workstation client.

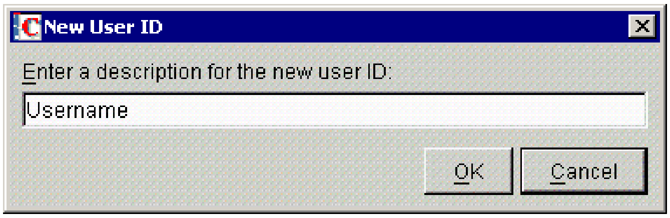
Creating User IDs

Adding a Description to the User ID Tab

1 Click User IDs > New.



2 Type a descriptive name (for example, DeskUp) in the New User ID dialog box, then click OK.


New User ID

Enter a description for the new user ID:

Username

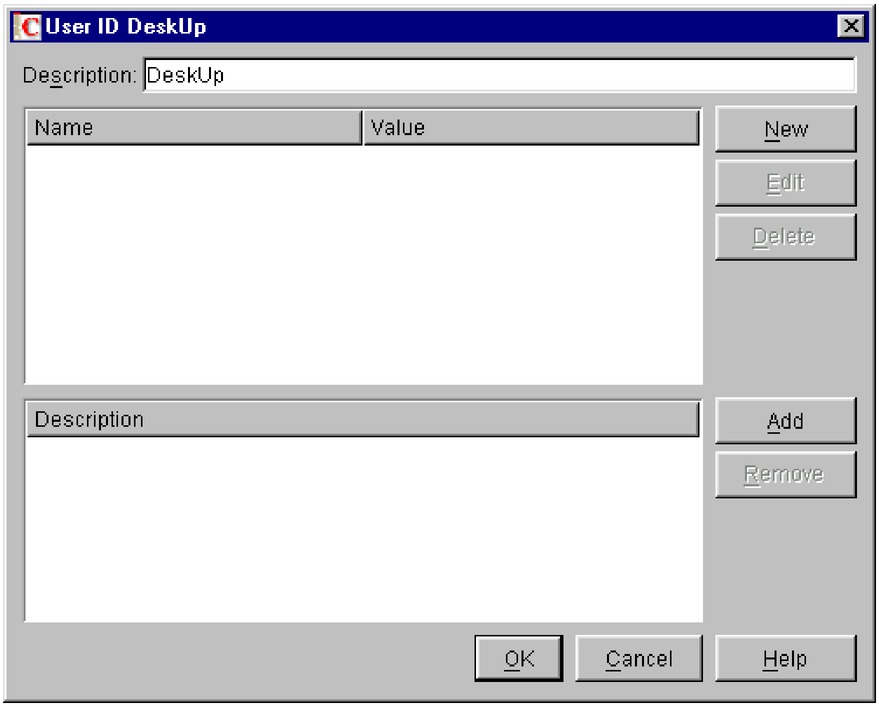
Adding a Username Variable and Value

A username variable displays the name that a user ID is associated with.

1 (Conditional) To add a username variable to an existing user ID, click the user ID, then click Edit.

For example, click DeskUp in the Description column. As the following figure illustrates, the User ID dialog box appears for the application. If you are adding a new user ID, this dialog box appears as soon as you have created the user ID.

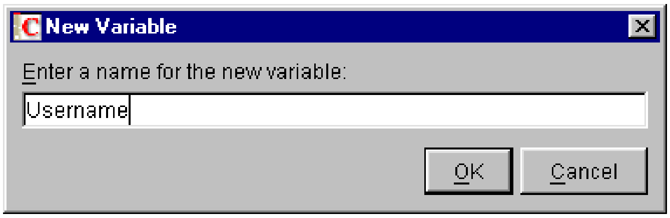
This dialog box is used to manage the variables (for example, username and password) associated with a login.



User ID DeskUp

Description: DeskUp

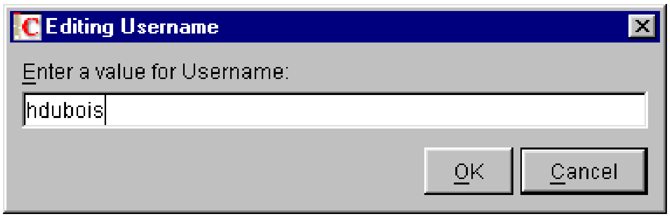
2 Click New, type a name (for example, Username) for the new variable, then click OK.



New Variable

Enter a name for the new variable: Username

3 Type a value (for example, hdubois) for the new variable, then click OK.



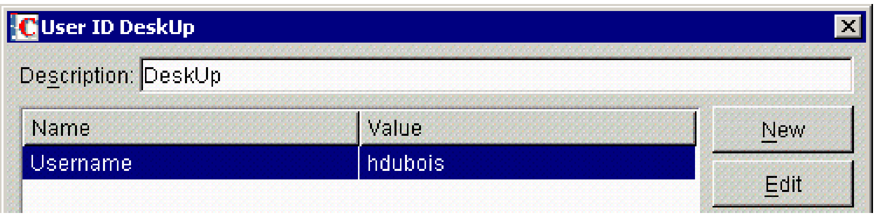
Editing Username

Enter a value for Username: hdubois

Adding a Password Variable and Value

After you enter a variable and value for a user ID, you return to the User ID *application name* dialog box. You can then add other variables and values if you want to.

1 Click New.

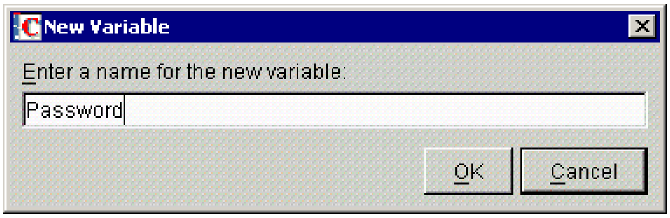


User ID DeskUp

Description: DeskUp

Name	Value
Username	hdubois

2 In the New Variable dialog box, type Password, then click OK.

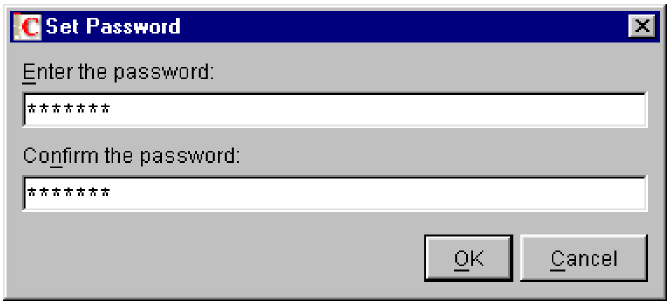


New Variable

Enter a name for the new variable:

Password

3 Type and confirm the new password, then click OK.



Set Password

Enter the password:

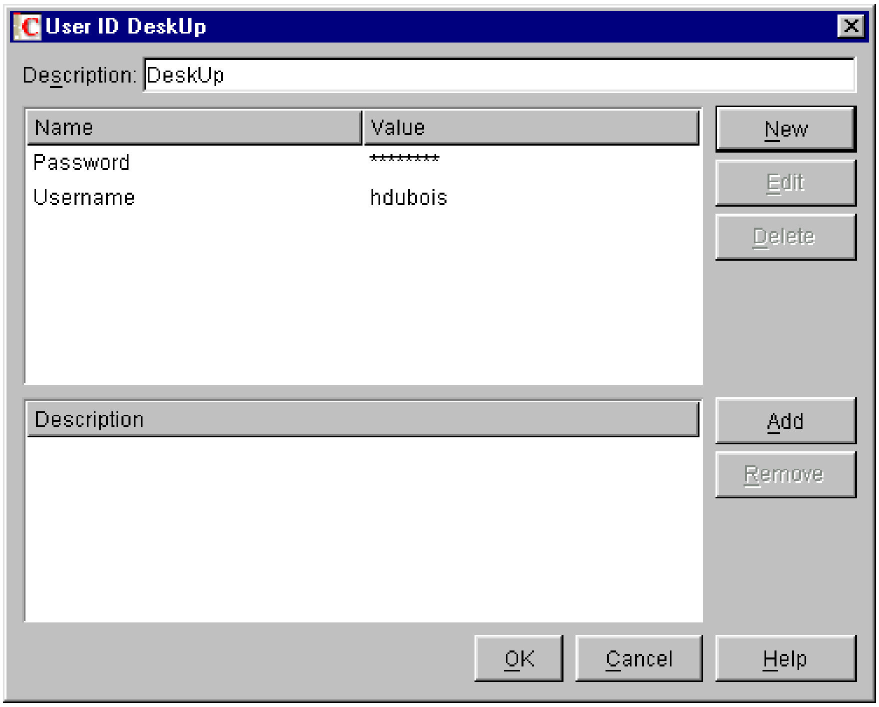
****

Confirm the password:

****

If you are using the properties of your own User object, the user ID values are saved to the local cache and a directory cache.

The following figure illustrates a completed user ID, with the Username and Password variables along with accompanying values for each:

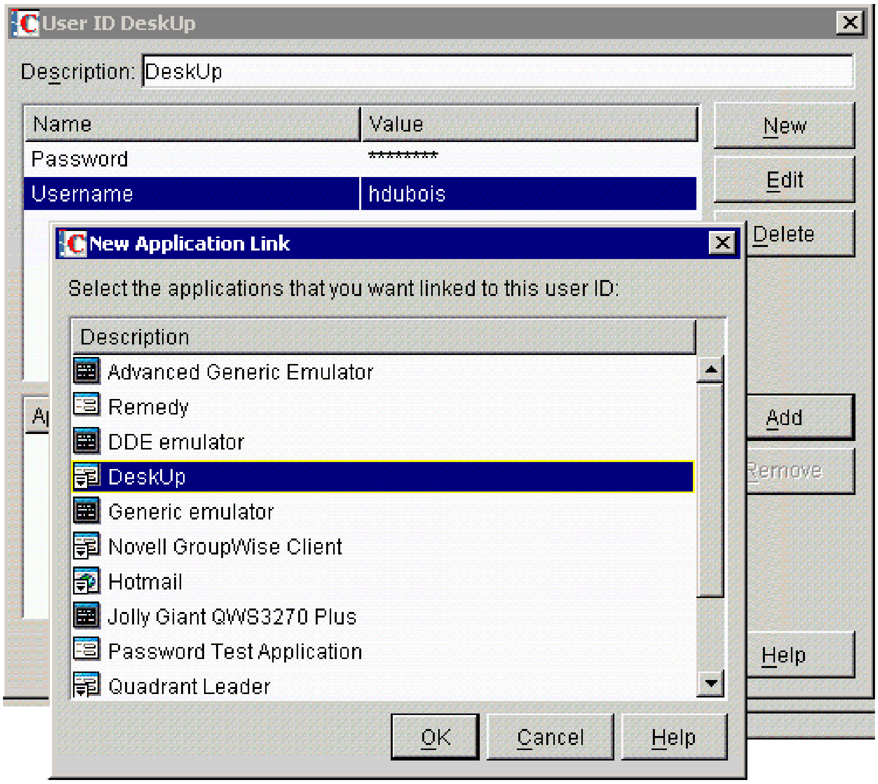


User ID DeskUp

Description: DeskUp

Name	Value
Password	********
Username	hdubois

4 (Optional) Link the user ID to an application by clicking Add, selecting the application, then clicking OK.



User ID DeskUp

Description: DeskUp

Name	Value
Password	********
Username	hdubois

New Application Link

Select the applications that you want linked to this user ID:

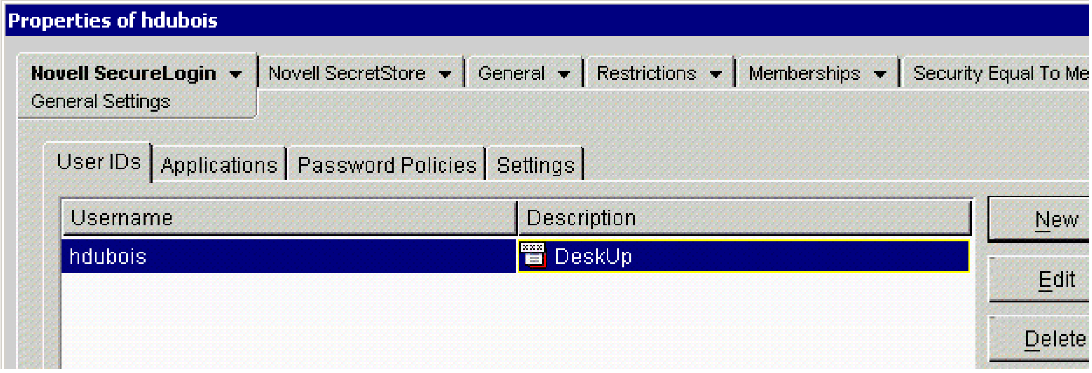
Description
Advanced Generic Emulator
Remedy
DDE emulator
DeskUp
Generic emulator
Novell GroupWise Client
Hotmail
Jolly Giant QWS3270 Plus
Password Test Application
Quadrant Leader

You can link a user ID to one or more applications. Applications that are linked with the same user ID share the same login data. If you change a password for an application, that change is stored in one place. All linked applications then use the updated data for single sign-on logins.

A down-arrow on the left side of the icon indicates that the ID is inherited.

5. Save the user ID by clicking OK, then save the data by clicking Apply or OK.

   The following figure illustrates the new user ID:



Username	Description
hdubois	DeskUp

Editing User IDs

You can change any variable, regardless of how it is named. Those variables that contain "password" in the name (or key) use the password change dialog box. Change all other variables by using the regular edit-variable dialog box.

Changing a Password

1. Click the user ID, then click Edit.
2. Click the Password line, then click Edit.
3. Enter and confirm the new password, then save changes.

Changing Other Variable Names

1. Click the user ID, then click Edit.
2. Click the variable (for example, Username) line, then click Edit.
3. Type a name, then click OK.
4. Save the changes.

Deleting User IDs

1. Click a user ID, then click Delete.

   You can't delete an inherited user ID or a default user ID. The default user ID is the first one that is associated with an application.

2. Save the data by clicking OK or Apply.

Setting Up Multiple IDs for an Application

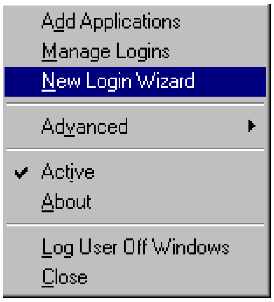
You can create additional logins to an application or server. SecureLogin manages multiple logins by providing a list when you launch the application.

Scenario: Multiple Identities. Occasionally, Henri must access deskup.exe as user Admin to change data. Usually, Henri accesses the application as user Henri to view data. Therefore, Henri's job responsibilities require that he have two identities for the application deskup.exe. Henri sets up an ID for each role. To log in to deskup.exe, Henri selects from a list of IDs, according to his role.

Using the New Login Wizard to Create IDs

To use SecureLogin on the desktop to set up multiple IDs for an application:

1 Right-click the SecureLogin icon on the task bar (system tray), then click New Login Wizard.



The Wizard is self-documenting. It provides information that helps you complete the remaining steps.

2 Select the application that requires a new login, then click Next.

3 Type a distinguishing description for the new login, then click Finish.

4 When you next run the application, select the new description, then provide login credentials.

Using Network Management Tools to Create IDs

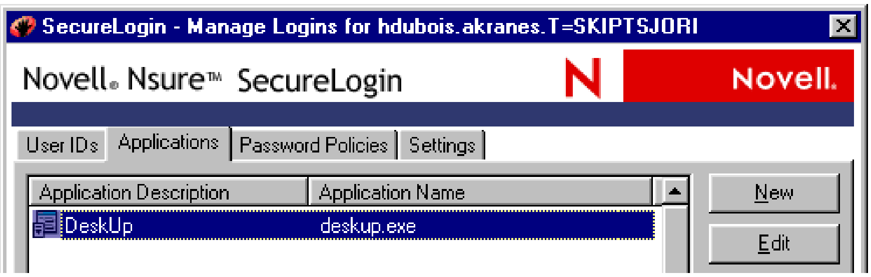
The following steps apply to ConsoleOne, MMC, or SecureLogin Manager:

1 (Conditional) Create a user ID for an application.

If a user ID already exists for the application that you need multiple IDs for, skip this step.

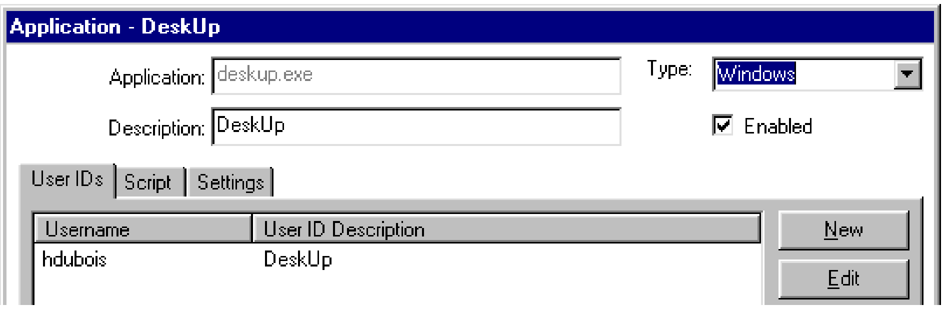
The application can be a Windows, Web, or other application. The application has a username and password.

2 Click Applications, select the application that you want to create the multiple user ID for, then click Edit.


SecureLogin - Manage Logins for hdubois.akranes.T=SKIPTSJORI
Novell. Nsure™ SecureLogin
Novell.
User IDs
Applications
Password Policies
Settings
New
Edit

Application Description	Application Name
DeskUp	deskup.exe

3 In the User IDs dialog box, click New.


Application - DeskUp

Application: deskup.exe

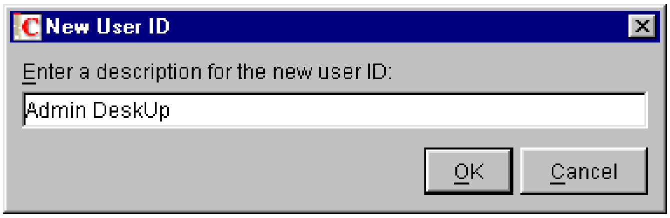
Type: Windows

Description: DeskUp

☑ Enabled

Username	User ID Description
hdubois	DeskUp

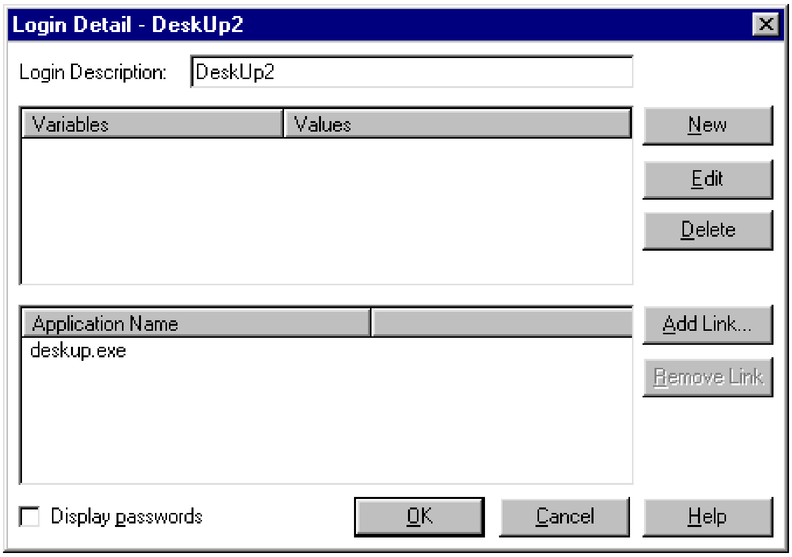
4 Type a description for the multiple-ID login that you are creating, then click OK.


New User ID

Enter a description for the new user ID:

Admin DeskUp

5 Select the new entry in the Description column, click Edit, create variables and values for the new user ID, then save changes.


Login Detail - DeskUp2

Login Description: DeskUp2

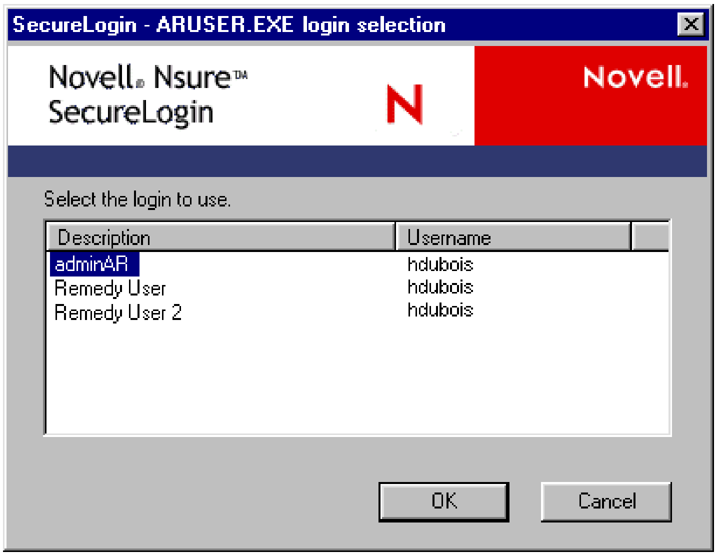
Variables	Values

Application Name	
deskup.exe	

☐ Display passwords

6 For subsequent logins to the application, select the user ID that you need.

As the following figure illustrates, a list displays each user ID that you have created. The default option is for the first login that was created.



SecureLogin - ARUSER.EXE login selection

Select the login to use.

Description	Username
adminAR	hdubois
Remedy User	hdubois
Remedy User 2	hdubois

Each user ID has a separate set of variables. The script for the login could use two variables (for example, a username and password) or more than two. Also, the variables might be named something other than Username and Password.

Managing Applications

When a user starts an application for the first time after it has been enabled for single sign-on, the script prompts the user for application credentials. SecureLogin encrypts and stores the credentials in the directory against the User object. During subsequent logins, the credentials are automatically passed to the application.

The Applications tab lists applications that have been enabled for single sign-on. You can enable applications by using the Applications page or the Add Applications Wizard.

Enabling Applications for Single Sign-On

This section provides information on the following:

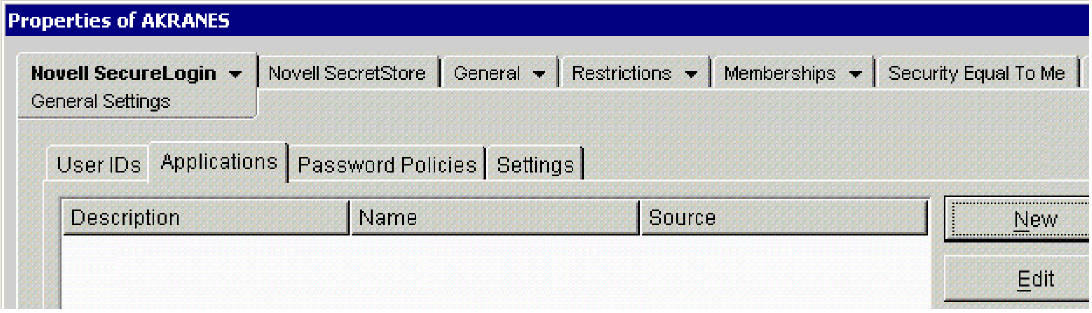
- "Enabling Applications with Prebuilt Scripts" on page 35
- "Enabling Applications that Don't Have Prebuilt Scripts" on page 37

Enabling Applications with Prebuilt Scripts

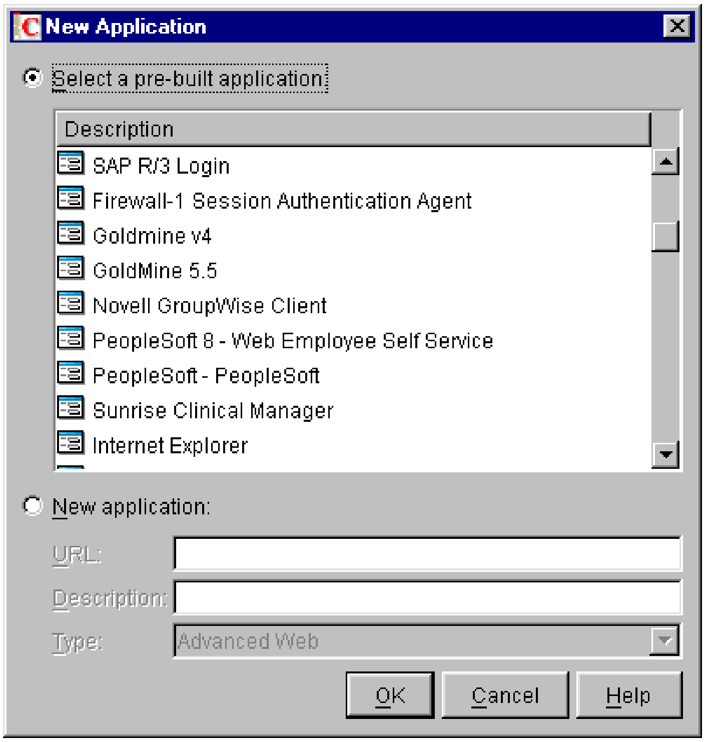
A prebuilt script already contains commands that SecureLogin requires for single sign-on. SecureLogin provides prebuilt scripts for many applications. The fastest way to determine whether a prebuilt script exists is to start the application and log in. If a prebuilt script exists, the SecureLogin single sign-on prompt displays.

To enable an application that has a prebuilt script:

1 In the Applications tab, click New.



By default, SecureLogin displays a list of applications that have prebuilt scripts:



● Select a pre-built application

- SAP R/3 Login
- Firewall-1 Session Authentication Agent
- Goldmine v4
- GoldMine 5.5
- Novell GroupWise Client
- PeopleSoft 8 - Web Employee Self Service
- PeopleSoft - PeopleSoft
- Sunrise Clinical Manager
- Internet Explorer

○ New application:

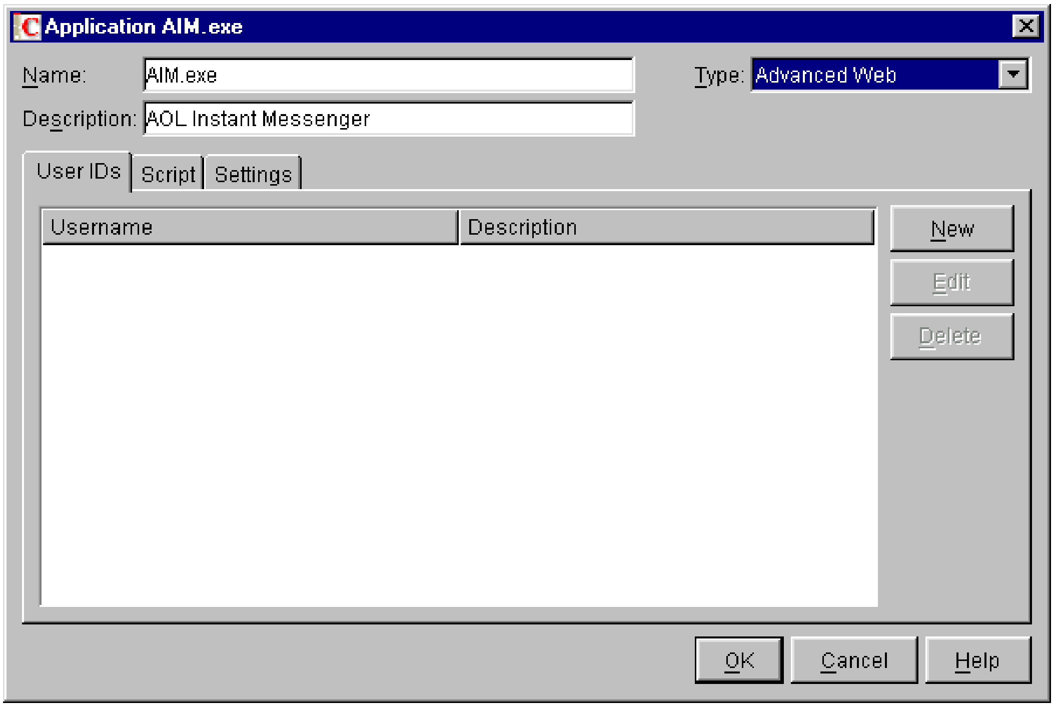
Type: Advanced Web

2 Click an application listed in the Description pane.

3 Add the application to the list by clicking OK.

4 (Conditional) For Web applications, change the application type to Web or Advanced Web.

The default type is Windows. If you don't change the type to Web or Advanced Web, the script won't work.



Application AIM.exe

Name: AIM.exe

Type: Advanced Web

Description: AOL Instant Messenger

When you select New Application to add a Web application in SecureLogin 3.51.2, you can select either the Web type or the new Advanced Web type.

The Web option remains in SecureLogin 3.51.2 so that customers who upgrade from previous versions of SecureLogin don't lose their existing Web scripts. In SecureLogin 3.51.2, the Web type can use the Advanced Web script commands the same as the new Advanced Web type can.

In earlier SecureLogin releases, Web pages were scripted as whole pages. Therefore, SecureLogin couldn't distinguish among frames within the Web page. The Advanced Web scripting feature allows you to script for a particular frame within a Web page.

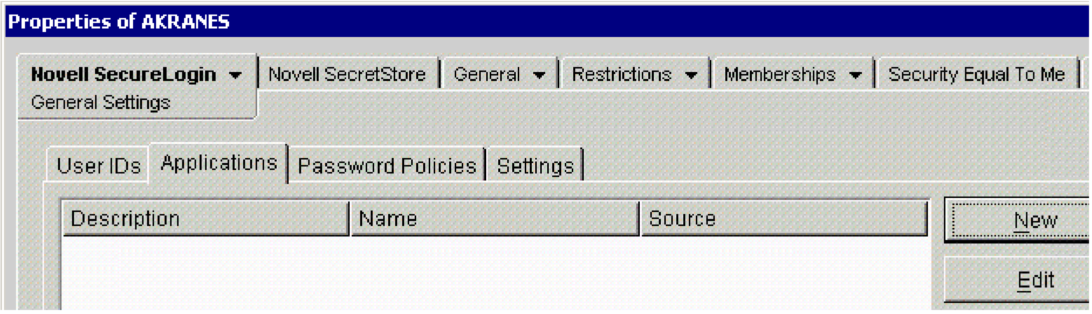
For information on Advanced Web Script commands that you can use (for example, Attribute) see "SecureLogin Commands" in the *Nsure SecureLogin 3.51.2 Scripting Guide*.

5 Save the application type by clicking OK, then enable the application for single sign-on by clicking Apply or OK.

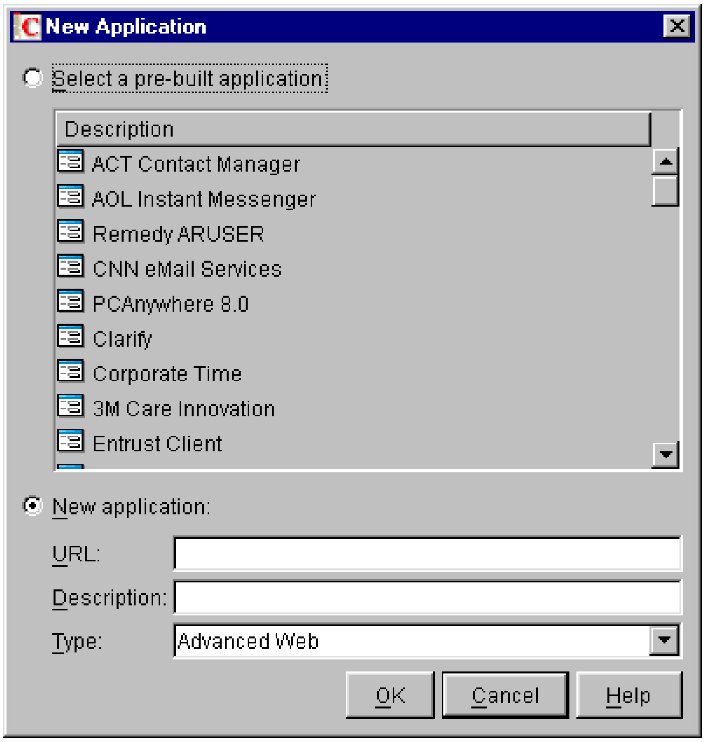
Enabling Applications that Don't Have Prebuilt Scripts

If SecureLogin doesn't provide a prebuilt script, you can create a script that enables the application for single sign-on.

1 In the Applications page, click New.



2 Select New Application.



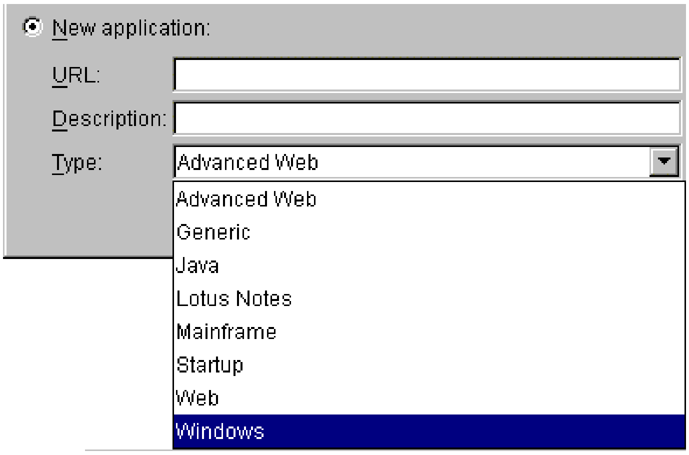
● New application:

URL:

Description:

Type: Advanced Web

3 Provide information in the Type field and text boxes.


● New application:

URL:

Description:

Type: Advanced Web

Type: In the Type drop-down list, select the application type (for example, Windows or Advanced Web).

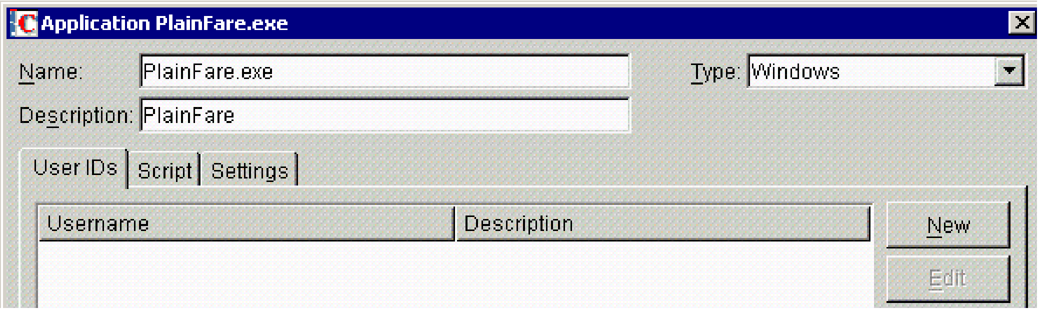
Executable Name/Name: For a Windows application, type the executable filename (for example, PlainFare.exe) in the Executable Name or Name text box.

URL: For a Web or Advanced Web application, type the URL where the application is found (for example, http://www.hotmail.com).

Description: In the Description text box, type a descriptive name for the application (for example, PlainFare).

4 Click OK.

5 Add a user ID for the application.



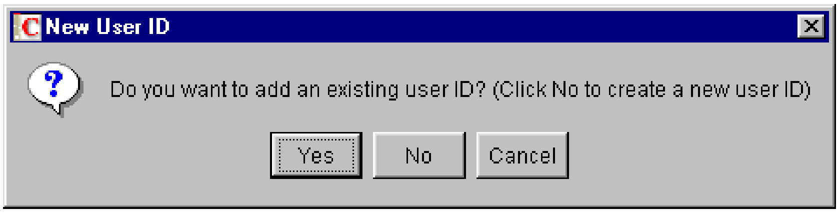
Name: PlainFare.exe

Type: Windows

Description: PlainFare

The User IDs page displays the user IDs linked to or associated with this application. In this example, no user ID has been linked to PlainFare.exe. To add a user ID, select the User ID page, then click New.

If a user ID exists, you can use it or create a new one.

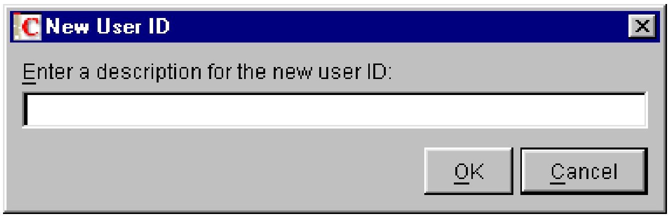


Do you want to add an existing user ID? (Click No to create a new user ID)

(If you use the SecureLogin desktop client to add a user ID, the dialog box varies.)

To use an existing user ID, click Yes. In the New User ID Link dialog box, select the user IDs that you want linked to this application, then click OK.

To create a new user ID, click No, type a description for the new user ID, then click New.



Enter a description for the new user ID:

After the User ID dialog box displays, add login variables (credentials). See "Creating User IDs" on page 26.

To edit a user ID, on the Applications page, click the application, click Edit, add a User ID, type a script, then click OK. For new user IDs, the Edit dialog box automatically opens.

6 Save the data by clicking Apply or OK.

Using the Generic Script Type

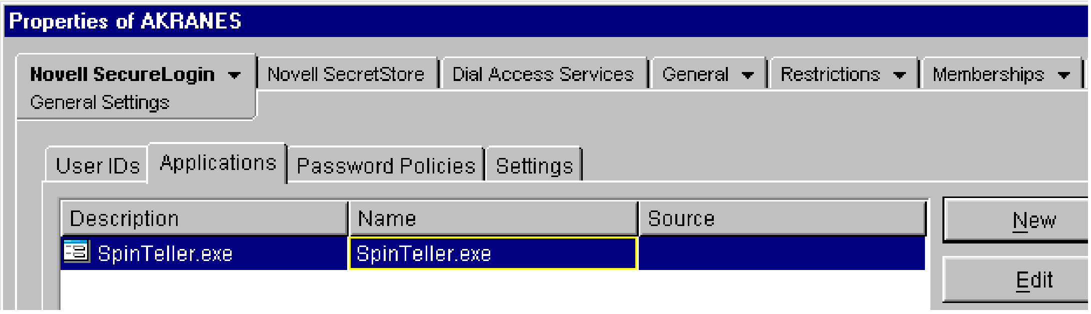
The Generic script type is for generic scripts. Generic scripts can be common to many scripts. Instead of copying and pasting the script, you can keep the script in a generic platform and include it in all scripts.

For example, you can use a standard block of script to prompt a user for a variable. By using the Include command and subcommands in various scripts, you can call this generic script.

Editing Scripts

When you add an application, SecureLogin either uses a prebuilt script that you select or creates a script for the application. You can view, edit, or modify the script.

1 Click Applications.

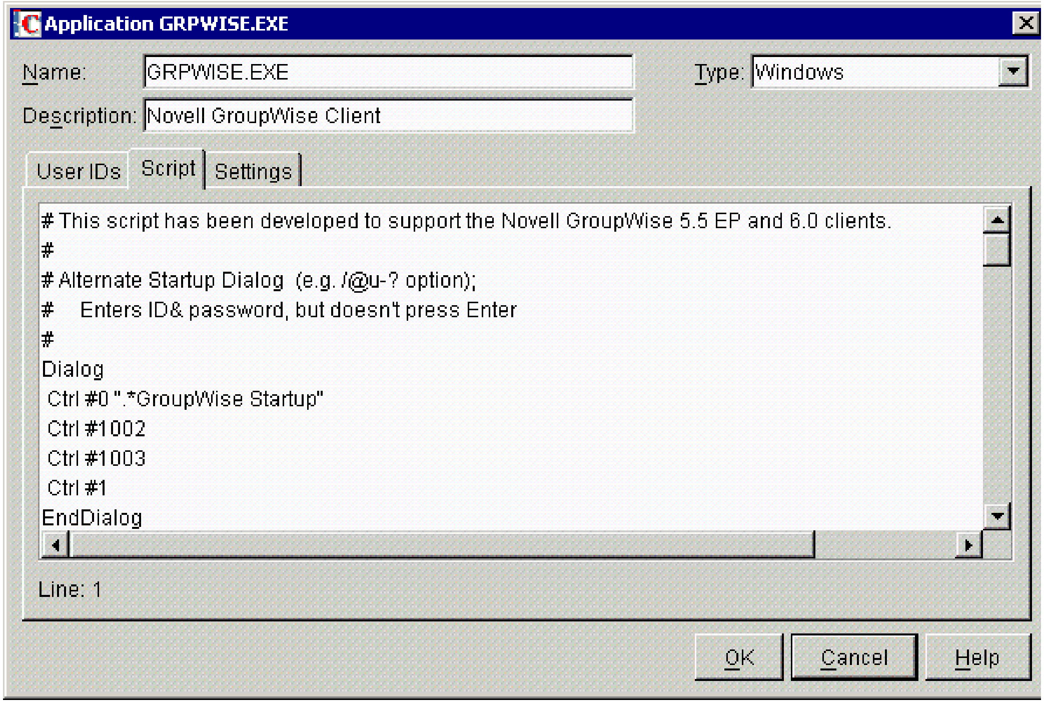


Properties of AKRANES

Description	Name	Source
SpinTeller.exe	SpinTeller.exe	

2 Click the application, then click Edit.

3 Click Script.



Name: GRPWISE.EXE

Type: Windows

Description: Novell GroupWise Client

```
# This script has been developed to support the Novell GroupWise 5.5 EP and 6.0 clients.
#
# Alternate Startup Dialog  (e.g. /@u-? option);
#     Enters ID& password, but doesn't press Enter
#
Dialog
 Ctrl #0 ".*GroupWise Startup"
 Ctrl #1002
 Ctrl #1003
 Ctrl #1
EndDialog
```

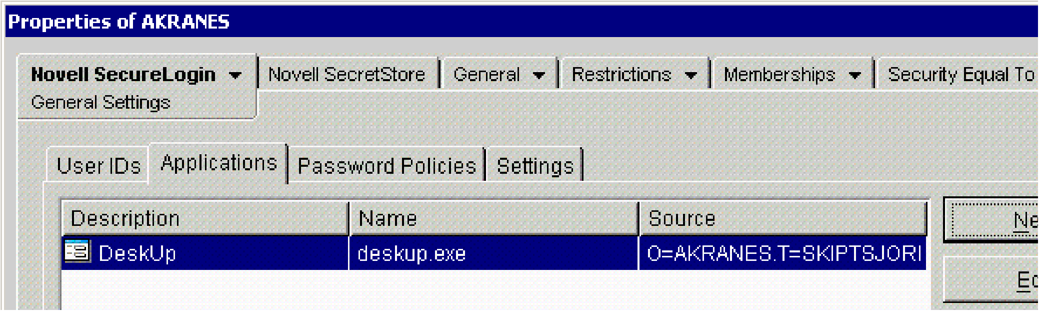
Line: 1

4 Edit the script, then click OK.

For information on scripts, see the *Nsure SecureLogin 3.51.2 Scripting Guide*.

Modifying Settings for Applications

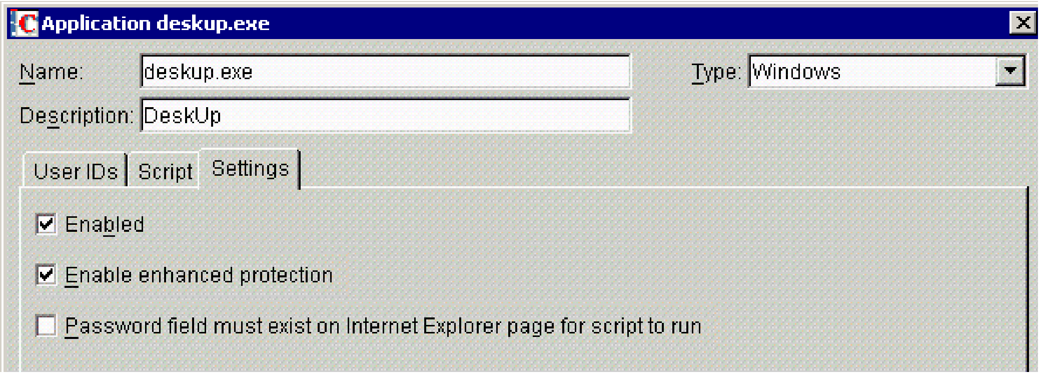
1 Click Applications.



Description	Name	Source
DeskUp	deskup.exe	O=AKRANES.T=SKIPTSJORI

A down-arrow on the left side of an icon indicates that the application is inherited.

2 Click the application name, click Edit, then click Settings.



Application deskup.exe

Name: deskup.exe

Type: Windows

Description: DeskUp

☑ Enabled

☑ Enable enhanced protection

□ Password field must exist on Internet Explorer page for script to run

3 Check the check boxes for the desired settings.

The following table provides information on the settings:

Preference	Description
Enabled	When the check box is checked, SecureLogin can use the user ID and script for this application and log the user in to the application.
Enable Enhanced Protection	Enhanced Protection is a feature in Novell SecretStore®. When the Enhanced Protection option is enabled for any secret in SecretStore, if an administrator changes or resets the user's eDirectory password, SecretStore enters a locked state. To unlock SecretStore, the user enters the previous eDirectory password (not the password that the administrator changed to). This feature protects users from a mischievous administrator who wants to discover confidential information. If the administrator changes the user's password, the login data that is enhanced protected will be locked.
Password Field Must Exist on Internet Explorer Page for Script to Run	Some Web pages have a general Login field but not an accompanying password field. If you uncheck the check box, the script runs for these pages as well as for pages requiring a password. If you check the check box, the script runs only on the pages that have a password field. You can write a Web script that has SecureLogin fill in forms that don't contain any passwords. Therefore, a password field isn't always necessary. This setting is for extra security or validation, to make sure that a password field exists on the page before the script runs.

Managing Password Policies

A password policy is a set of requirements or rules, such as the number of characters required for a password. To enforce security during logins, policies are applied to scripts.

The policy ensures that the values of the variables comply with specified rules governing their composition. Although this feature is called password policies, these policies can be used on any variables, not just password variables.

You can set password policies for the following:

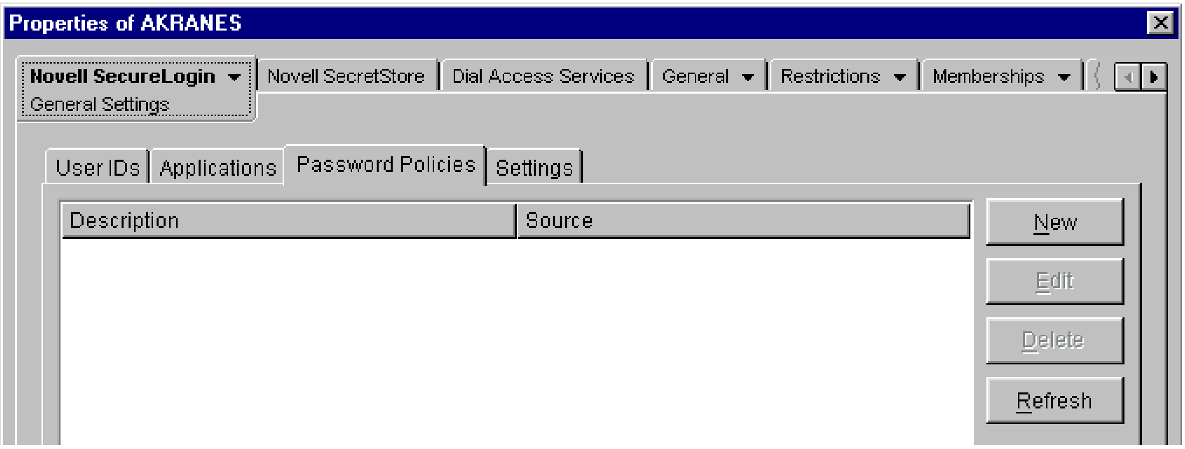
- A container or OU
- A User object
- An individual application

SecureLogin can generate random passwords. (See "ChangePassword" in the *Nsure SecureLogin 3.51.2 Scripting Guide*.) These passwords comply with password policies and significantly increase security. Typically, password rules are matched to the organizational policy for the application. However, SecureLogin can enforce stronger policies if they are required.

You can set a different password policy for each container or OU in the directory.

Creating or Editing a Password Policy

1 Click Password Policies.

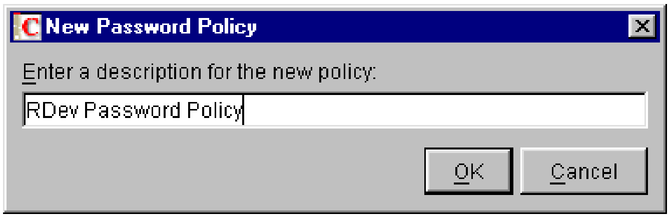


The Description column displays the name of the password policy. A down-arrow on the icon indicates that the policy is inherited.

The Source column displays the distinguished name of the object that contains the password policy (the container that the policy is inherited from).

SecureLogin enforces only new or more restrictive edited policies when a password is created or changed. SecureLogin doesn't check existing passwords to see whether they conform to new or edited policies.

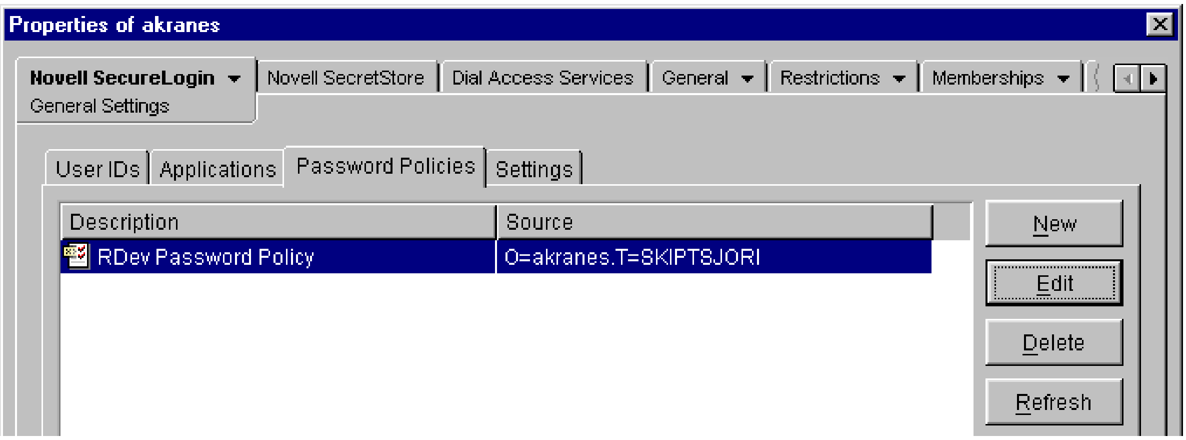
2 Click New, enter a descriptive name for the new policy, then click OK.



Enter a description for the new policy: RDev Password Policy

Use a unique name for all password policies, user IDs, and applications. A password policy can't have the same name as any other SecureLogin object.

3 (Conditional) If you are editing a policy, click the policy name, then click Edit.



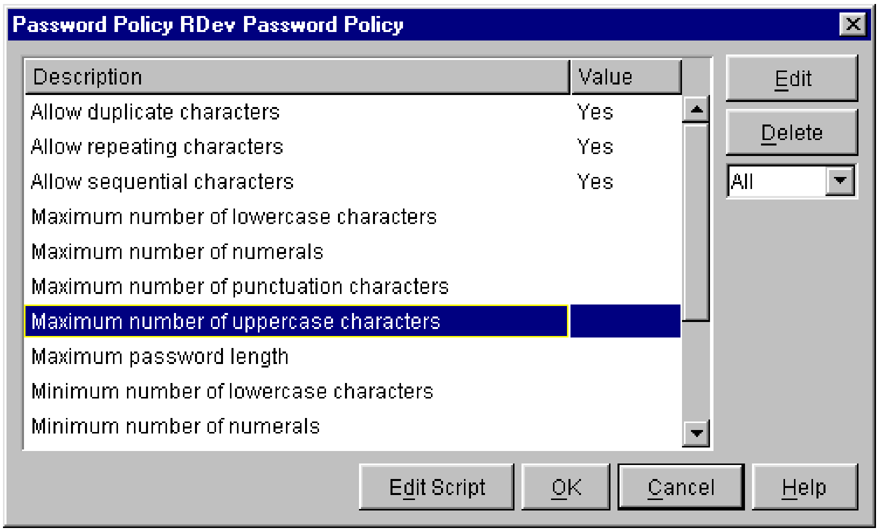
Properties of akranes

Novell SecureLogin General Settings | Novell SecretStore | Dial Access Services | General | Restrictions | Memberships

User IDs | Applications | Password Policies | Settings

Description	Source
RDev Password Policy	O=akranes.T=SKIPTSJORI

4 Edit the settings, then click OK.



Password Policy RDev Password Policy

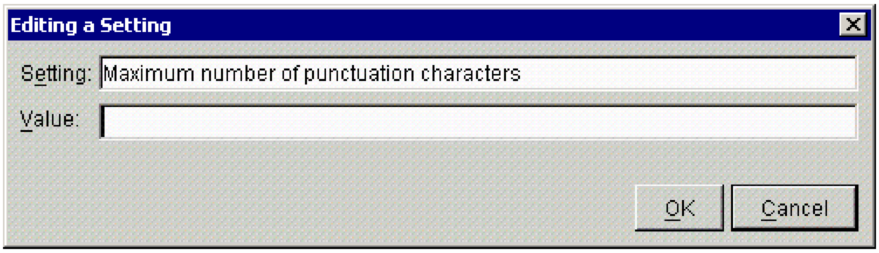
Description	Value
Allow duplicate characters	Yes
Allow repeating characters	Yes
Allow sequential characters	Yes
Maximum number of lowercase characters	
Maximum number of numerals	
Maximum number of punctuation characters	
Maximum number of uppercase characters	
Maximum password length	
Minimum number of lowercase characters	
Minimum number of numerals	

By default, several basic settings are displayed. To display all settings (basic and advanced), select All from the drop-down list below the Delete button.

You can edit more than one setting before clicking OK.

Not all settings are mandatory. You can set as few or as many policy restrictions as are necessary to meet security requirements.

To modify a setting, select it, click Edit, then type or select a value in the Value edit box.



Setting: Maximum number of punctuation characters

Value:

If you change a value for a setting, the new value appears in the Value column and in the modified script for the password policy. To see the changes to the script, click Edit Script.

For example, if you set the value of Maximum Number of Numeric Characters to 3, the script (available through Edit Script) displays MAXNUMERALS 3.

By default, the settings are case sensitive. For example, “a” is a different character from “A.” Even if repeating characters aren’t allowed, the password AaBC is still accepted.

The following table lists default values for basic settings:

Setting	Value	Details
Maximum number of uppercase characters	whole number	minimum zero, no upper limit
Maximum password length	whole number	minimum zero, no upper limit
Minimum number of uppercase characters	whole number	minimum zero, no upper limit
Minimum password length	whole number	minimum zero, no upper limit
Password must begin with an uppercase character	Yes/No	Default is No

The following table lists default values for advanced settings:

Setting	Value	Details
Allow duplicate characters	Yes/No No, case insensitive	The No option doesn’t prohibit uppercase or lowercase use of the same character. ABCA contains a duplicate character, but ABCD doesn’t.
Allow repeating characters	Yes/No No, case insensitive	The No option isn’t case sensitive. Therefore, it doesn’t prohibit uppercase or lowercase of the same character. AABC contains a repeating character, but ABCA doesn’t.
Allow sequential characters	Yes/No No, case insensitive	The No option isn’t case sensitive. ABCD and 1234 contain sequential characters, as do BDAC and 4321.
Maximum number of lowercase characters	whole number	minimum zero, no upper limit

Setting	Value	Details
Maximum number of numerals	whole number	minimum zero, no upper limit
Maximum number of punctuation characters	whole number	minimum zero, no upper limit
Minimum number of lowercase characters	whole number	minimum zero, no upper limit
Minimum number of numerals	whole number	minimum zero, no upper limit
Minimum number of punctuation characters	whole number	minimum zero, no upper limit. See "Allowable Punctuation Characters" on page 47.
Password must not contain any of these characters	keyboard characters	case sensitive

If you set a minimum and maximum option to the same number, the password contains that number of letters. If the minimum number is higher than the maximum number, you receive an error.

Changes are saved to the script for the policy. To view changes you have made to the script, click Edit Script. Later, you can easily edit these changes by again using the Edit Script feature.

5 Save the settings by clicking Apply.

Allowable Punctuation Characters

The following characters satisfy the punctuation setting:

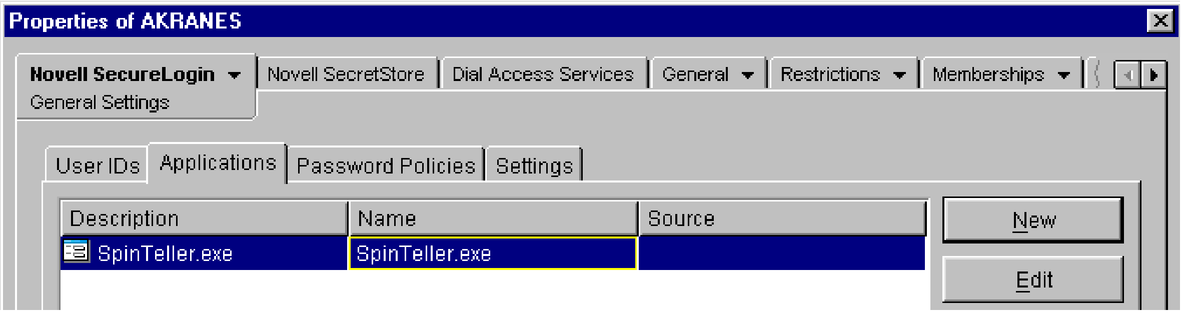
Character	Character Name
~	Tilde or swung dash
!	Exclamation mark
@	At
#	Hash or pound
$	Dollar
%	Percent
^	Caret
&	Ampersand
*	Asterisk
	Space
( )	Parentheses
_	Underscore
+	Plus
|	Delimiter or delimiter bar

Character	Character Name
-	Hyphen
=	Equals
\	Backward slash or backward diagonal
{ }	Braces or curly brackets
[ ]	Brackets
:	Colon
;	Semicolon
“	Quotation mark
'	Single quotation mark
<	Greater than
>	Less than
?	Question mark
/	Slash, diagonal, or slant
,	Comma
.	Period or full stop
`	Grave or accent grave mark

Using Password Policies in Scripts

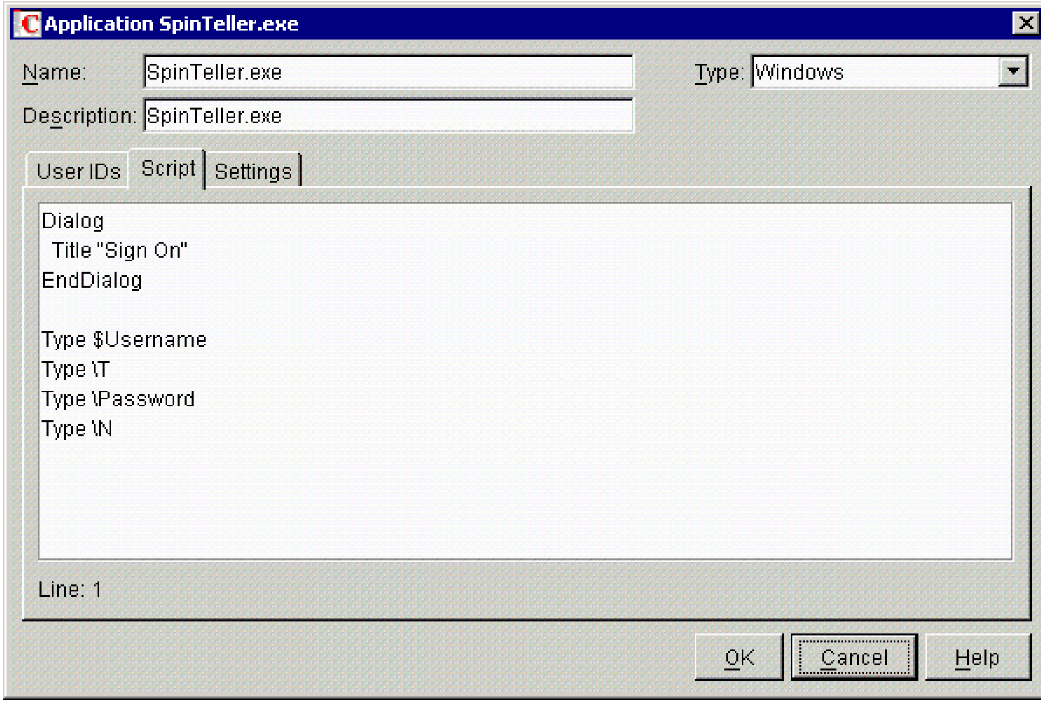
Within a script, you can use a password policy to restrict a variable to the assigned security settings.

1 Click Applications.



Description	Name	Source
SpinTeller.exe	SpinTeller.exe	

2 Click the required application, then click Edit.



```
Dialog
 Title "Sign On"
EndDialog

Type $Username
Type \T
Type \Password
Type \N
```

3 Add the following line to the top of the script:

`RestrictVariable` *`variable name password policy`*

For example, for SpinTeller.exe shown in Step 2, add

```
RestrictVariable $Password PasswordPolicy2
```

To restrict multiple variables to a particular password policy, add multiple RestrictVariable commands.

The *variable name* parameter can be a normal variable (for example, $Password), or a runtime variable (for example, ?temp). This flexibility can be useful if you change a password by using a runtime variable and then set a normal variable to the value of the runtime variable.

Adding the RestrictVariable command ensures that a variable complies with the policy. The value entered is rejected if it doesn't comply with the policy set for that variable. The RestrictVariable command applies the policy specified regardless of whether the variable is being added or edited through SecureLogin administration tools or through a script that is running.

If the value being changed by a user is not accepted, a message informs the user as to why the value was rejected.

If the value is being set through the ChangePassword command being run in automatic (random) mode, the value generated will comply with the policy.

In some cases, a policy might be created where no acceptable values exist. When this occurs, an error is displayed when the ChangePassword command tries to generate a password.

If you use the SecureLogin SET command to set values, they will not be forced to comply with password policies.

For more information, see "RestrictVariable" in the *Nsure SecureLogin 3.51.2 Scripting Guide*.

Example Password Policy Scripts

Example 1

```
MAXPASSWORDLENGTH 8
MINPASSWORDLENGTH 8
MAXPUNCTUATION 0
MINPUNCTUATION 0
MAXUPPERCASE 8
MINUPPERCASE 0
MAXLOWERCASE 8
MINLOWERCASE 0
MAXNUMERALS 8
MINNUMERALS 0
```

This password policy indicates that the password must be exactly 8 characters long and contain no punctuation characters.

The password asdf4jB8 is acceptable.

The password aasdf5$n is unacceptable because it contains a punctuation character.

Example 2

```
MAXPASSWORDLENGTH 12
MINPASSWORDLENGTH 6
MAXPUNCTUATION 8
MINPUNCTUATION 0
MAXUPPERCASE 8
MINUPPERCASE 0
MAXLOWERCASE 8
MINLOWERCASE 0
MAXNUMERALS 8
MINNUMERALS 0
NODUPLICATECHARACTERS CASEINSENSITIVE
POSITIONCHARACTER NUMERAL 3,4,5
```

This password policy indicates that the password must be between 6 and 12 characters long. It can contain no more than 8 of any character type (uppercase, lowercase, numeral, or punctuation). No character can appear more than once in the policy, regardless of case. A numeral must appear in at least one of positions 3, 4, or 5.

The password f54v9)_Q is acceptable.

The password f5v)_QF7 is unacceptable because it has no numeral in positions 3, 4 or 5, and the letter F occurs in positions 1 and 7.

Example 3

```
MAXPASSWORDLENGTH 16
MINPASSWORDLENGTH 6
MAXPUNCTUATION 8
MINPUNCTUATION 0
MAXUPPERCASE 16
MINUPPERCASE 1
MAXLOWERCASE 16
MINLOWERCASE 0
MAXNUMERALS 16
MINNUMERALS 0
BEGINWITHUPPERCASE
DISALLOWEDCHARACTERS @&
```

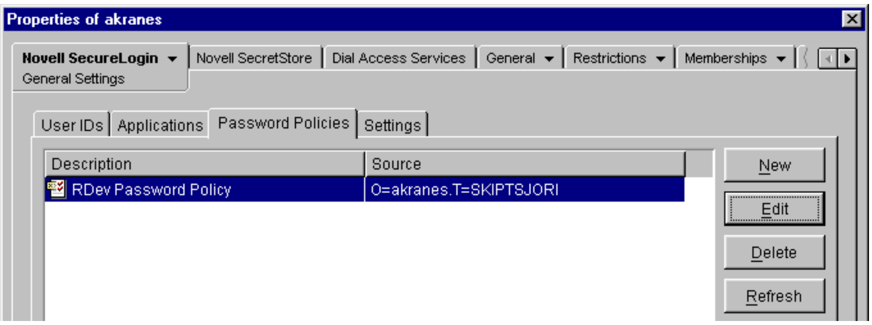
This password policy indicates that the password must be between 6 and 16 characters long. It must contain at least one uppercase character. It can contain no more than 8 punctuation characters. It must begin with an uppercase character, and it can't contain either the @ character or the & character.

The password R48iv"? is acceptable.

The password R48?- is unacceptable because it is less than 6 characters long.

Deleting a Password Policy

1 Select the Password Policies page.



Description	Source
RDev Password Policy	O=akranes.T=SKIPTSJORI

2 Select the policy that you want to delete, click Delete, then click OK.

In the Active Directory snap-in and SecureLogin on the desktop, you must also click Yes in the confirmation dialog box.

Distributing Password Policies

You can configure password policies at the container, OU, or User object level. Policies set at the container or OU level apply to all associated User objects or user accounts. Policies set at the User object or user account level override all higher-level policies.

For ease of maintenance in multiple-user environments, we recommend that you maintain password policies at the container or OU level.

Setting the Default Domain Policy in Active Directory

In Active Directory environments, at the domain level, make sure that the Default Domain policy allows all authenticated users to have Read rights to All Properties.

1 Expand Active Directory Users and Computers, right-click the domain name, then click Properties.

2 Click Group Policy > Properties, then click Security.

3 Click Advanced.

4 Click Authenticated Users Special, then click View/Edit.

5 Under the Allow column, check the Read All Properties check box, then click OK.

Managing Administrative and User Settings

This section provides information on the following:

- "Understanding the Configuration Hierarchy" on page 52
- "Viewing SecureLogin Settings" on page 52
- "Configuring SecureLogin Settings" on page 55

Understanding the Configuration Hierarchy

You can apply SecureLogin settings to a Container object, a User object, or a workstation.

- Container object

  Settings applied to a Container object affect all users and objects in and below that Container object.

- User object

  Settings applied to a User object supersede the settings applied to a Container object or to a workstation.

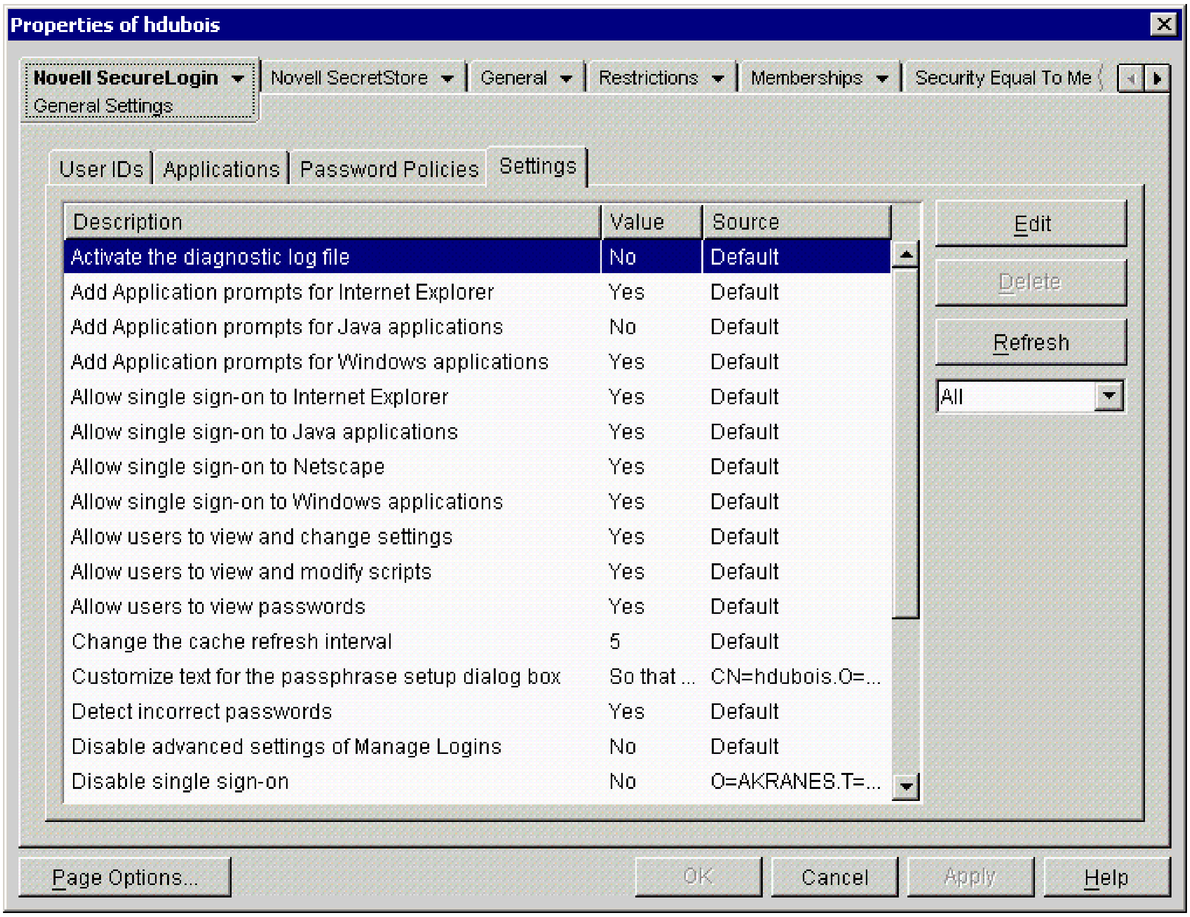
- Workstation

  You can give users the ability to apply settings to a workstation. However, any settings applied to a User object supersede settings applied to a workstation.

Viewing SecureLogin Settings

You can view SecureLogin settings by using SecureLogin on the desktop, ConsoleOne, Microsoft Management Console in Active Directory environments, or SecureLogin Manager.

1 Click Settings.



Description	Value	Source
Activate the diagnostic log file	No	Default
Add Application prompts for Internet Explorer	Yes	Default
Add Application prompts for Java applications	No	Default
Add Application prompts for Windows applications	Yes	Default
Allow single sign-on to Internet Explorer	Yes	Default
Allow single sign-on to Java applications	Yes	Default
Allow single sign-on to Netscape	Yes	Default
Allow single sign-on to Windows applications	Yes	Default
Allow users to view and change settings	Yes	Default
Allow users to view and modify scripts	Yes	Default
Allow users to view passwords	Yes	Default
Change the cache refresh interval	5	Default
Customize text for the passphrase setup dialog box	So that ...	CN=hdubois.O=...
Detect incorrect passwords	Yes	Default
Disable advanced settings of Manage Logins	No	Default
Disable single sign-on	No	O=AKRANES.T=...

The Description column (Setting Description in MMC and on the desktop) explains a setting's purpose or action.

The Value column lists the default or changed value.

The Source column (Inherited From in MMC and on the desktop) displays the origin of the setting's value. The origin can be one of the following:

- A default value
- Manually configured at the User object level
- An inherited value

2 Scroll to the desired setting.

The following table provides information on the settings. If you are running in standalone mode, not all settings are displayed.

Configuration Option	Description
Activate the Diagnostic Log File	Logs the details of use to the hard drive. Because this preference is used for debugging and troubleshooting, the default is set to No. If you need to investigate a SecureLogin issue on the workstation, set the value to Yes. **NOTE:** If you set this setting to Yes, expect a continuous increase in memory usage, similar to a memory leak.

Configuration Option	Description
Add Application Prompts for - Internet Explorer (and Netscape) - Java Applications - Windows Applications	Provides a prompt to enable an application for single sign-on, if a script exists for the application. To prevent a prompt, change the value to No. If you disable the prompt, users can enable (for single sign-on) only those applications that you configure at the container or OU level.
Allow Single Sign-on to - Internet Explorer - Java Applications - Netscape - Windows Applications	Enables single sign-on to the application type. To prevent users from being able to single sign-on to these applications, set the value to No. In contrast to disabling the SecureLogin prompts, disallowing single sign-on access disables any single sign-on for the application type.
Allow Users to View and Change Settings	Enables users to customize their SecureLogin environment by using the Settings tab to change settings on their workstations. To prevent users from customizing, change the value to No.
Allow Users to View and Modify Scripts	Enables users to view and edit scripts, which are SecureLogin's instructions as to what to do concerning the application. When the value is set to Yes, users can use the New and Edit buttons on the Applications page. To prevent users from viewing and modifying scripts, set the value to No.
Allow Users to View Passwords	Enables users to check the Display Passwords check box and view passwords that they use to log in to applications. To prevent users (and anyone else) from viewing their SecureLogin passwords, change the value to No. The Yes setting is useful when a user’s SecureLogin configuration needs to be reset. (The Clear Object Data or Clear Cache buttons reset the configuration.) Clearing object data deletes all use information, including passwords and passphrases that need to be entered when the user restarts SecureLogin. Allowing the user to view passwords enables the user to view and record passwords before object data (cache) is cleared.
Change the Cache Refresh Interval	Controls the number of minutes that SecureLogin waits before checking the container or OU cache for updates. The default is 5 minutes. Depending on your network and number of users, a recommended value is 240 minutes.
Customize Text for the Passphrase Setup Dialog Box	Enables you to personalize the text that appears in the Passphrase Setup dialog box that users encounter when they first use SecureLogin. Although you can type 8 lines with 64 characters on each line, limit your text to 415 characters. Otherwise, the text boxes hide the remaining text.
Detect Incorrect Passwords	We recommend that you set this value to No. The response to an incorrect password is included in the SecureLogin application connector (script).
Disable the Advanced Settings of Manage Logins	The Advanced option that is available from the SecureLogin task bar icon enables users to change SecureLogin settings, change their passphrases, and refresh the local cache. To prevent users from using this functionality, set the value to Yes. The Settings tab is then unavailable through either the Advanced option on the task bar icon or Manage Logins.

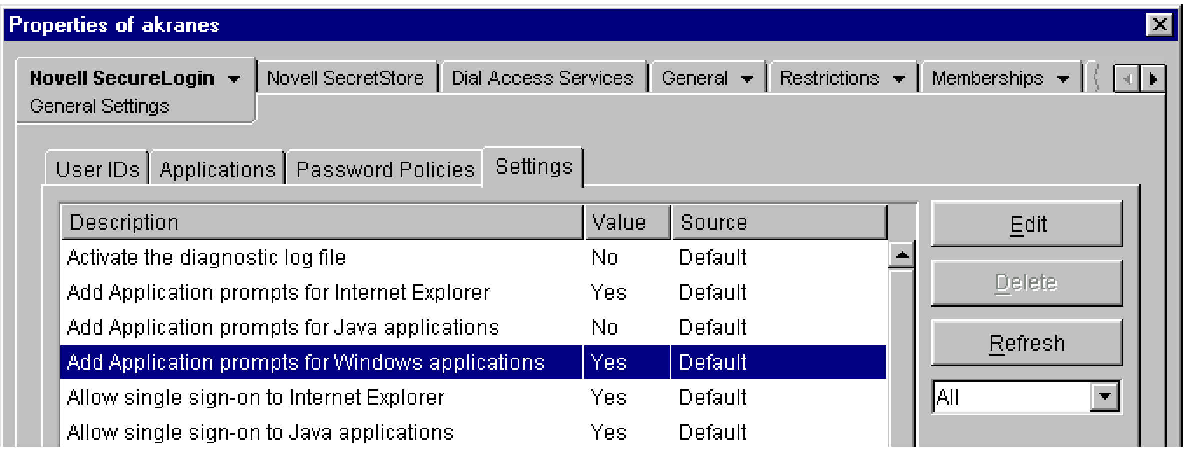
Configuration Option	Description
Disable Single Sign-On	By default, all users can single sign-on to Windows, Web, and terminal emulator applications. To prevent a user from using single sign-on, select the User object and change the value to Yes. In the snap-in to MMC, a Yes setting might cause the message "_wremove preference" to appear. If the message appears, click OK. You can ignore this message. It doesn't affect SecureLogin functionality.
Display the System Tray Icon	Whether the icon is displayed depends on the organization's security policies and preferences. To prevent users from displaying and accessing the system tray (task bar) icon, change the value to No.
Enable the File Cache	Enables SecureLogin to create and use cache files on the workstation. The cache file stores all user settings, including those inherited from higher-level containers and OUs. Settings are normally stored in a directory on the server. However, if the server is unavailable, or if you are using a laptop, the cache on the workstation is used. The cache is password protected and encrypted.
Enable the New Login Wizard on the System Tray Icon	Enables users to create multiple SecureLogin logins for the same application or server. To disable this feature, change the value to No.
Password Protect the System Tray Icon	Requires users to provide their network passwords before they can access options on the system tray SecureLogin icon. To require a password, change the value to Yes.
Prevent Users from Entering a Passphrase Question	By default, users can enter their own passphrase question, and then provide an answer. To require users to use a passphrase question that the administrator provides, set the value to Yes.
Stop Walking Here	Enables or disables inheritance settings from higher-level containers or OUs. Higher levels might have implemented a different version of SecureLogin. If inheritance from higher levels is required, set the value to No (default).
Use a Passphrase Policy	By default, SecureLogin doesn't require a passphrase policy. To require a passphrase policy, change the value to Yes, then edit and save the policy.

To access the Settings tab for Active Directory:

1 Select a Container or User object from the Active Directory Users and Computers in MMC, then select Properties.

2 Select the Settings tab from the SecureLogin SSO tab of the properties dialog box.

Configuring SecureLogin Settings



Description	Value	Source
Activate the diagnostic log file	No	Default
Add Application prompts for Internet Explorer	Yes	Default
Add Application prompts for Java applications	No	Default
Add Application prompts for Windows applications	Yes	Default
Allow single sign-on to Internet Explorer	Yes	Default
Allow single sign-on to Java applications	Yes	Default

The Settings page enables you to control SecureLogin functionality. Users are able to view a subset of these settings. Depending on the values you set, users can change the subset of settings on their workstations. Local settings (subset) override user settings that you make.

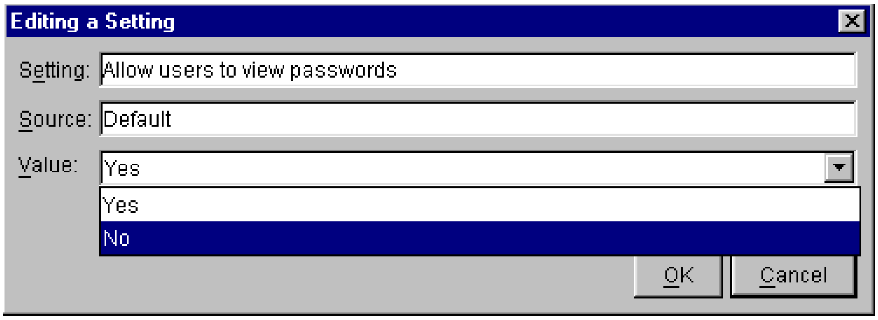
You can't delete a setting. When you click Delete in SecureLogin or the snap-in to MMC, the setting changes to the default value.

Also, if SecureLogin can't enforce a policy, SecureLogin changes the specified value to a valid approximation. For example, if you set the minimum password length greater than the maximum password length, SecureLogin can't enforce that setting.

1 Click Settings.

2 Click a setting, click Edit, change the value by using the drop-down list, then click OK.

   The following figure illustrates the Editing a Setting dialog box in ConsoleOne:



Setting: Allow users to view passwords

Source: Default

Value: Yes

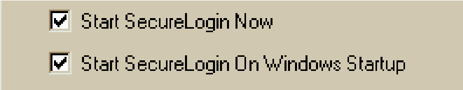
   To customize text for the passphrase setup dialog box, type the text. The customized text replaces the default text.

3 Save changes by clicking OK or Apply.

   Inherited fields in the SecureLogin Settings page don't apply until the corresponding settings are saved. To save inherited settings, click OK, close SecureLogin, then re-open SecureLogin.

Displaying the System Tray (Task Bar) Icon

When SecureLogin is installed, a Post-Install screen displays the following options:



☑ Start SecureLogin Now

☑ Start SecureLogin On Windows Startup

If the Start SecureLogin on Windows Startup check box, SecureLogin places the SecureLogin icon on the task bar whenever the workstation is started.

To prevent users from displaying and accessing the task bar icon:

1. Using administrative tools, right-click the Container or User object, then click Properties > Novell SecureLogin > General Settings > Settings.
2. Select Display the System Tray Icon, then click Edit.
3. Using the drop-down list, change the value to No.
4. Save the changes by clicking OK twice.

If you turn off the SecureLogin icon on the task bar (workstation) and then use another tool to change the data, the changes won't take effect until the workstation is restarted.

Disabling the Local Cache

To use login data when you work offline, you can store login data in encrypted files on your workstation. By default, these cache files are located in the \documents and settings*profile*\application data\securelogin\cache directory.

To disable the cache by using SecureLogin:

1. Right-click the SecureLogin icon on the task bar, select Advanced, then select Change Settings.
2. Select Settings > Enable Cache File.
3. Click Edit, set the value to No, then click OK twice.

To disable the cache by using administrative tools:

1. Right-click the Container or User object, then click Properties > Novell SecureLogin > General Settings > Settings.
2. Select Enable File Cache, click Edit, then set the value to No.
3. Save the changes by clicking OK twice.

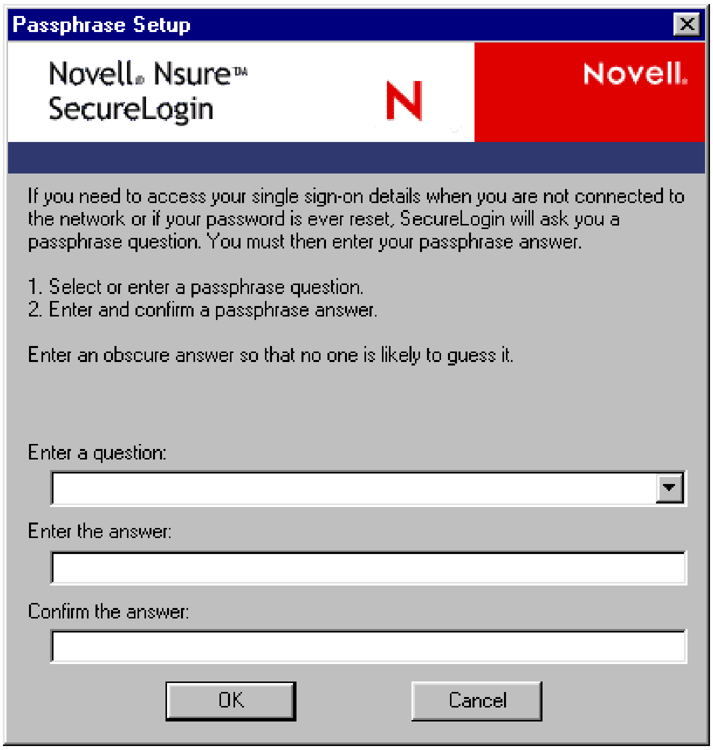
Managing Passphrases

This section provides information on the following:

- "How SecureLogin Uses Passphrases" on page 58
- "Providing Passphrase Questions" on page 59
- "Disabling User-Set Passphrase Questions" on page 60

How SecureLogin Uses Passphrases

When users first log in after SecureLogin is installed, they are prompted to enter a passphrase.



If you need to access your single sign-on details when you are not connected to the network or if your password is ever reset, SecureLogin will ask you a passphrase question. You must then enter your passphrase answer.

1. Select or enter a passphrase question.
2. Enter and confirm a passphrase answer.

Enter an obscure answer so that no one is likely to guess it.

Enter a question:

Enter the answer:

Confirm the answer:

A passphrase consists of a passphrase question and a passphrase answer. The passphrase is used to verify and authenticate the user. The passphrase ensures that only the authorized user has access to that user's single-sign-on applications.

In standalone environments, a password is used instead of a passphrase. This password is required each time the user starts the workstation or SecureLogin for authentication.

NOTE: You can't manage passphrase security in standalone mode.

The passphrase should not be confused with the normal login. A passphrase is used to protect the user's single sign-on credential information.

For example, in a directory environment, a rogue administrator can potentially log in to the network as the user by resetting the network password. Whenever SecureLogin recognizes that tampering or an administrative password change has been performed on the user's account, SecureLogin prompts for the passphrase. Without knowing the passphrase, the rogue administrator can't access the user's applications that are enabled for single sign-on.

The passphrase question and answer help you access your login data in the following situations:

- You are working remotely or offline.
- The network is down or isn't accessible.
- You forget your directory password and have it reset for you.
- Your credential store was locked when an administrator inappropriately reset your directory password.

NOTE: For a passphrase to display properly on multi-byte platforms (for example, Japanese and Chinese), users must use single-byte characters when entering a passphrase.

If you use Novell SecretStore, a specially-designated SecretStore Administrator might unlock your directory-based data stores on your behalf. For more information, see “Setting Up a SecretStore Administrator” in the *Novell SecretStore 3.3.3 Administration Guide* (http://www.novell.com/documentation/secretstore33/index.html).

Providing Passphrase Questions

You can provide preset passphrase questions for users to respond to, enable users to enter their own passphrase question, or do both.

By default, users can enter their own passphrase questions.

Passphrase questions can have up to 255 characters.

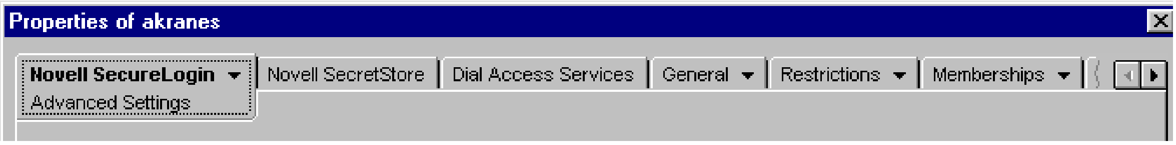
IMPORTANT: If a user forgets the passphrase answer, that user’s object data must be deleted and the passphrase reset. This action means that the user loses all the SecureLogin data, including application login credentials. Therefore, because the passphrase question is infrequently asked, the passphrase answer should be one that the user can easily remember, but one that others can’t easily guess.

Using ConsoleOne to Provide Questions

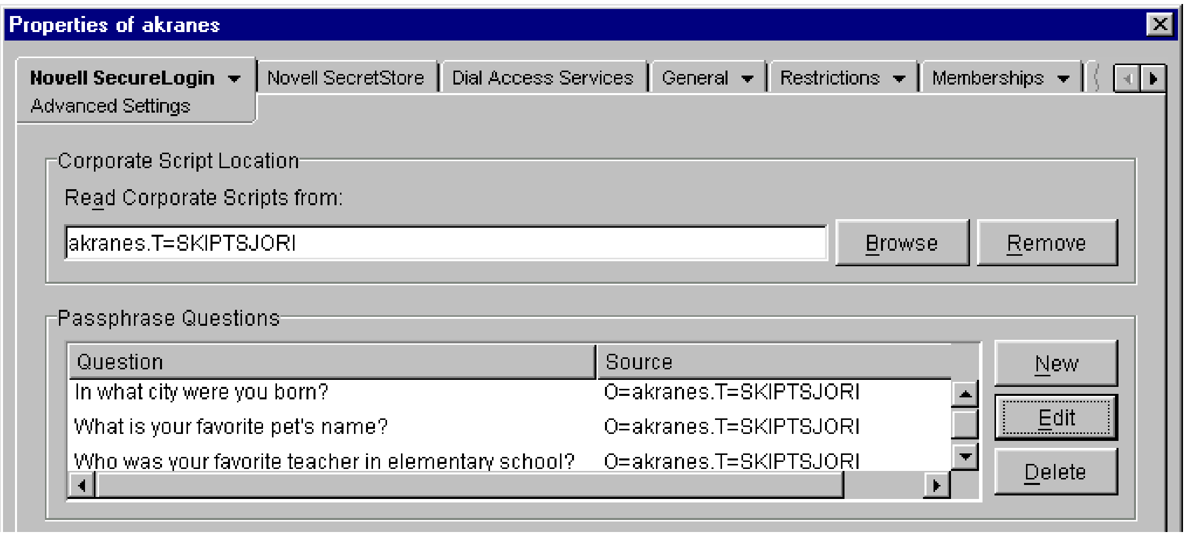
1. Right-click a Container object, then click Properties.

   You can provide passphrase questions for User objects, if a user has used SecureLogin and set a passphrase question.

2. Click Novell SecureLogin, then select Advanced Settings.



3. In the Passphrase Questions dialog box, click New.



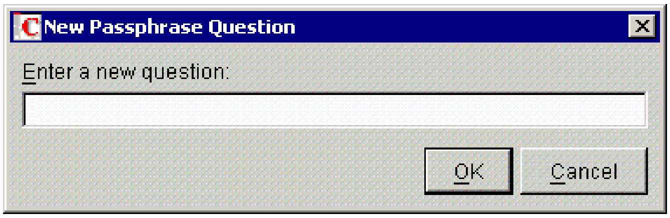
Corporate Script Location

Read Corporate Scripts from: akranes.T=SKIPTSJORI

Passphrase Questions

Question	Source
In what city were you born?	O=akranes.T=SKIPTSJORI
What is your favorite pet's name?	O=akranes.T=SKIPTSJORI
Who was your favorite teacher in elementary school?	O=akranes.T=SKIPTSJORI

4. Type a question, then click OK.



To edit a passphrase question, select it, click Edit, make changes, then click OK.

5 Click Apply.

Using MMC to Provide Questions

1 Select Start > Administrative Tools > Active Directory Users and Computers.

2 Right-click the relevant container or OU (for example, Users).

3 Select Properties > SecureLogin SSO > Settings.

4 Click Advanced Settings, then click New.

5 Type a passphrase question in the Enter a Passphrase Question edit box.

6 Click OK.

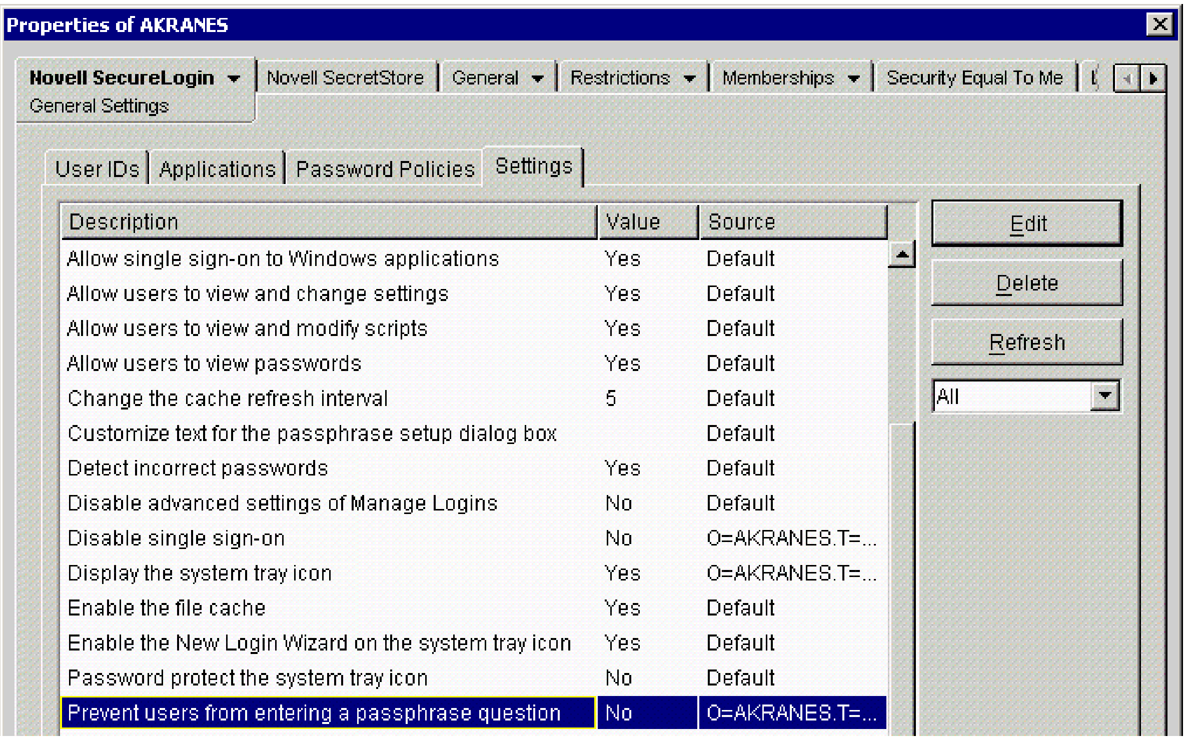
The passphrase question displays to all users associated with the container or OU.

Disabling User-Set Passphrase Questions

You can disallow user-set questions and require users to select a preset question.

Using ConsoleOne to Disable Questions

1 Select Novell SecureLogin > General Settings, then click Settings.



Description	Value	Source
Allow single sign-on to Windows applications	Yes	Default
Allow users to view and change settings	Yes	Default
Allow users to view and modify scripts	Yes	Default
Allow users to view passwords	Yes	Default
Change the cache refresh interval	5	Default
Customize text for the passphrase setup dialog box		Default
Detect incorrect passwords	Yes	Default
Disable advanced settings of Manage Logins	No	Default
Disable single sign-on	No	O=AKRANES.T=...
Display the system tray icon	Yes	O=AKRANES.T=...
Enable the file cache	Yes	Default
Enable the New Login Wizard on the system tray icon	Yes	Default
Password protect the system tray icon	No	Default
Prevent users from entering a passphrase question	No	O=AKRANES.T=...

2 Click Prevent Users from Entering a Passphrase Question, click Edit, select Yes from the drop-down list, click OK, then click Apply.

Using MMC to Disable Questions

1 On the Settings tab, click Advanced Settings.

2 Deselect Allow Users to Enter a Passphrase Question.

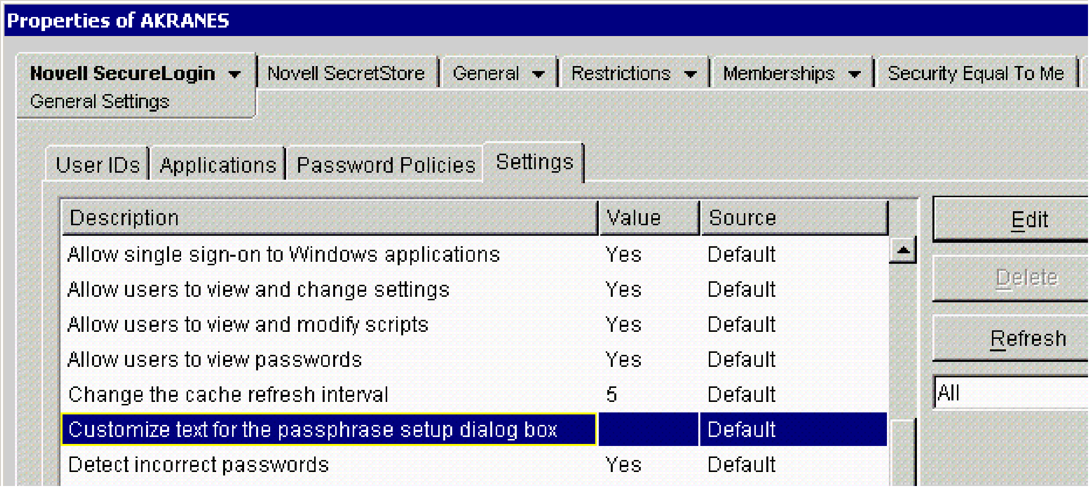
3 Click OK.

Customizing Instructions for Passphrases

When users first log in after installing SecureLogin, SecureLogin prompts them to select a passphrase question and type an answer. See “How SecureLogin Uses Passphrases” on page 58. You can edit that text and provide customized instructions for your organization.

Using ConsoleOne to Customize Instructions

1 Click Settings.

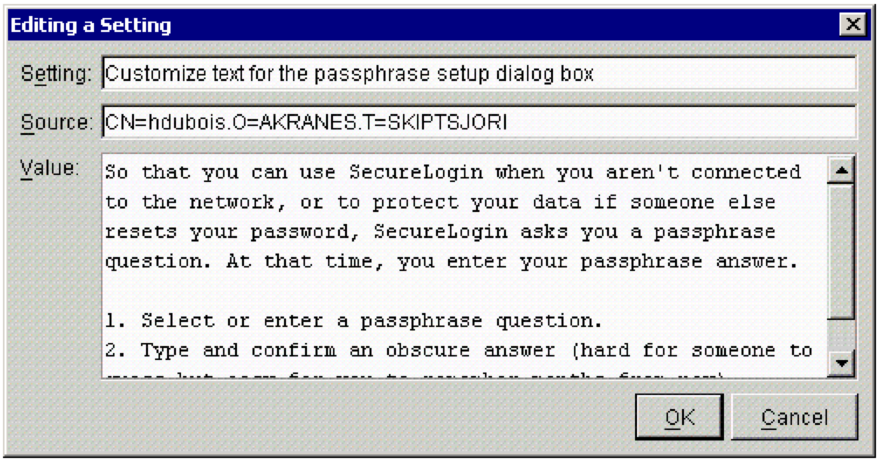


Description	Value	Source
Allow single sign-on to Windows applications	Yes	Default
Allow users to view and change settings	Yes	Default
Allow users to view and modify scripts	Yes	Default
Allow users to view passwords	Yes	Default
Change the cache refresh interval	5	Default
Customize text for the passphrase setup dialog box		Default
Detect incorrect passwords	Yes	Default

2 Select Customize Text for the Passphrase Setup Dialog Box, then click Edit.

NOTE: Because the primary data store is unavailable in standalone mode, many SecureLogin management features are not available in that mode.

3 Type text in the Value pane, then click OK.



Setting: Customize text for the passphrase setup dialog box

Source: CN=hdubois.O=AKRANES.T=SKIPTSJORI

Value:

```
So that you can use SecureLogin when you aren't connected
to the network, or to protect your data if someone else
resets your password, SecureLogin asks you a passphrase
question. At that time, you enter your passphrase answer.

1. Select or enter a passphrase question.
2. Type and confirm an obscure answer (hard for someone to
```

4 Click Apply.

5 Test the text by logging in as a new test user.

Using MMC to Customize Instructions

1 On the Settings tab, click Advanced Settings.

2 Check Use a Customized Prompt to Change a Passphrase Question.

3 Type the text that you want users to read.

4 Click OK.

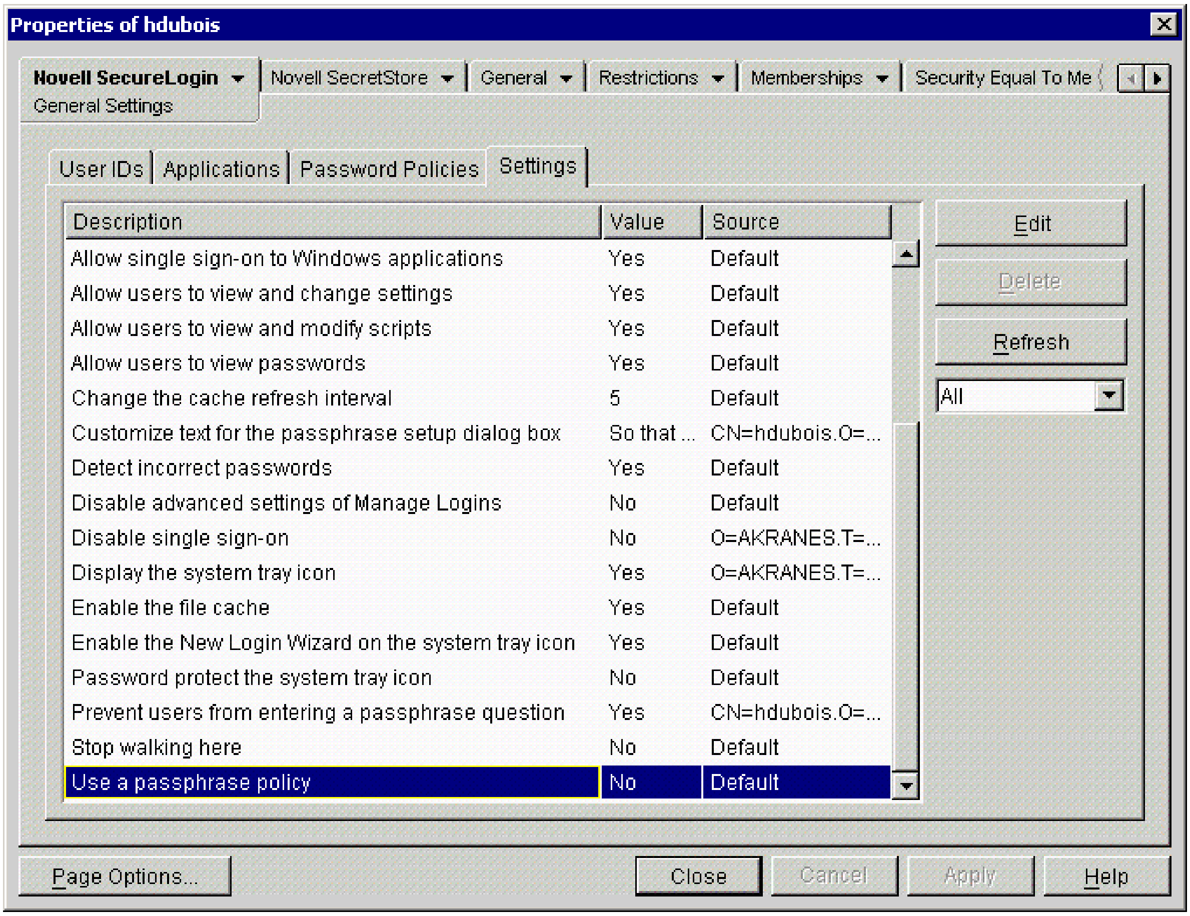
5 Test the text by logging in as a new test user.

Using a Passphrase Policy

By default, SecureLogin requires a passphrase answer that has at least six characters. To set additional requirements:

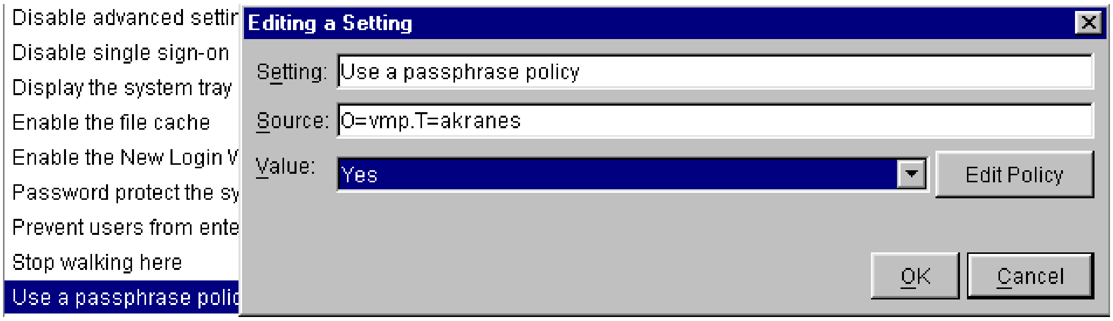
1 Click Settings.

2 Scroll to and select Use a Passphrase Policy.



Description	Value	Source
Allow single sign-on to Windows applications	Yes	Default
Allow users to view and change settings	Yes	Default
Allow users to view and modify scripts	Yes	Default
Allow users to view passwords	Yes	Default
Change the cache refresh interval	5	Default
Customize text for the passphrase setup dialog box	So that ...	CN=hdubois.O=...
Detect incorrect passwords	Yes	Default
Disable advanced settings of Manage Logins	No	Default
Disable single sign-on	No	O=AKRANES.T=...
Display the system tray icon	Yes	O=AKRANES.T=...
Enable the file cache	Yes	Default
Enable the New Login Wizard on the system tray icon	Yes	Default
Password protect the system tray icon	No	Default
Prevent users from entering a passphrase question	Yes	CN=hdubois.O=...
Stop walking here	No	Default
Use a passphrase policy	No	Default

3 In the Editing a Setting dialog box, require a passphrase policy by changing the value to Yes.



Setting: Use a passphrase policy

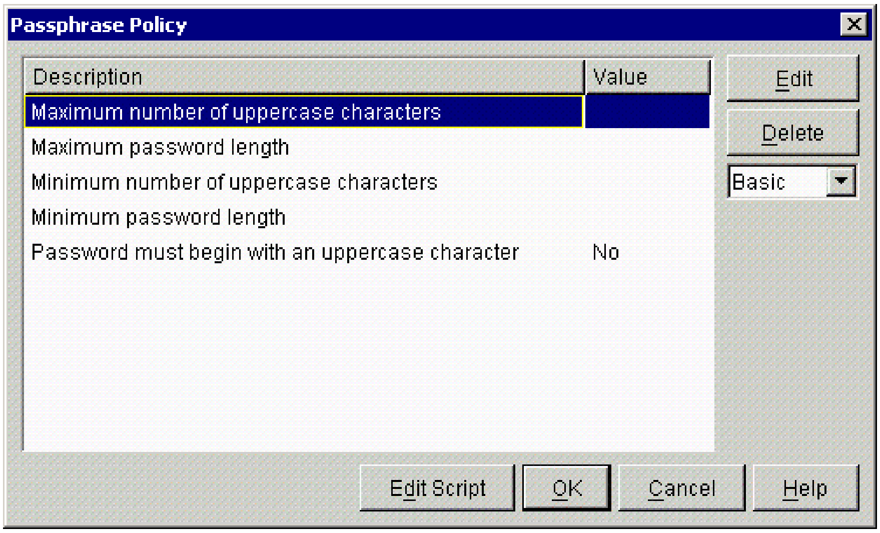
Source: O=vmp.T=akranes

Value: Yes

4 (Optional) To edit the passphrase policy, click Edit Policy.

4a Select a setting, then click Edit.

The following figure illustrates Basic passphrase policy settings that you can change:



Description	Value
Maximum number of uppercase characters	
Maximum password length	
Minimum number of uppercase characters	
Minimum password length	
Password must begin with an uppercase character	No

To view advanced settings, select Advanced from the drop-down list. To view Basic and Advanced settings, select All from the drop-down list.

4b In the Editing a Setting dialog box, change the value, then click OK twice.

The Advanced settings for passphrase policies are the same as for password policies. See the table of default values in "Creating or Editing a Password Policy" on page 43.

5 Save the setting by clicking OK twice.

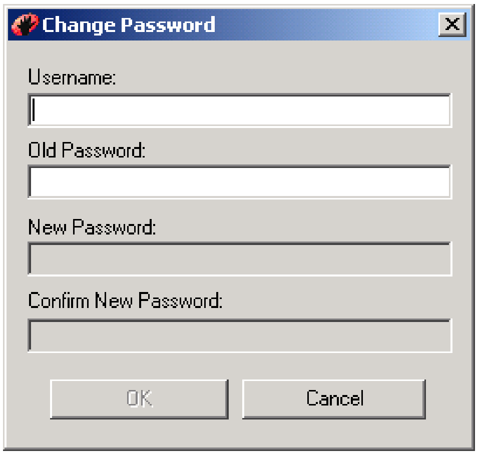
Managing Change-Password Events

Depending on your password rules, users might be required to change their passwords regularly. These passwords are stored on the application server. When passwords are changed on the application server, SecureLogin updates its password store. This is why SecureLogin handles password changes for all applications that are enabled for single sign-on.

To ensure that SecureLogin changes its stored passwords whenever users change their passwords, you need to update the application's script to include the Change Password routine.

1 Display the application's Change Password dialog box.

The Change Password dialog box must be displayed so that the Add Applications Wizard can identify the window. The following figure illustrates the Change Password dialog box for Password Test.



Change Password

Username:

Old Password:

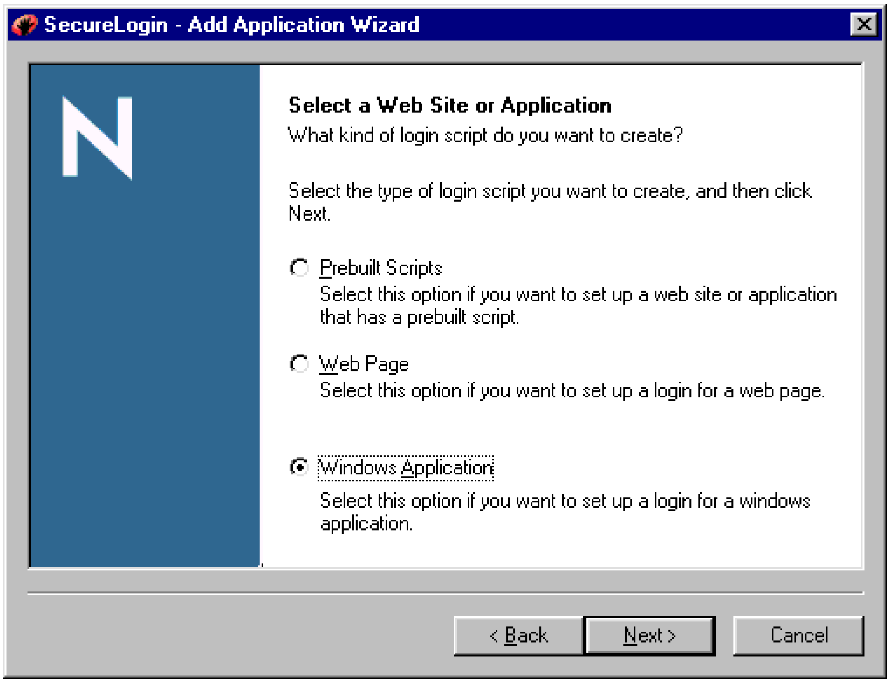
New Password:

Confirm New Password:

2 Right-click the SecureLogin icon on the task bar, select Add Applications, then click Next.

3 In the Welcome to SecureLogin dialog box, click Next.

4 Select Web Page or Windows Application, depending on your application, then click Next.



SecureLogin - Add Application Wizard

Select a Web Site or Application

What kind of login script do you want to create?

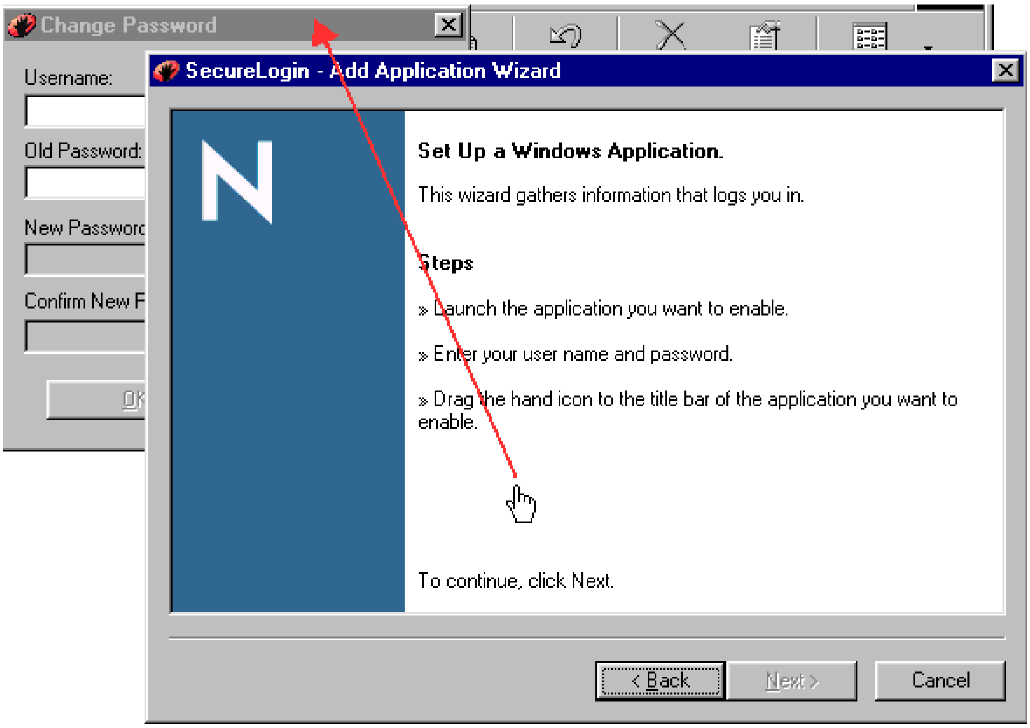
Select the type of login script you want to create, and then click Next.

○ Prebuilt Scripts
Select this option if you want to set up a web site or application that has a prebuilt script.

○ Web Page
Select this option if you want to set up a login for a web page.

● Windows Application
Select this option if you want to set up a login for a windows application.

5 Drag the hand icon from the Add Applications Wizard to the change-password window's title bar, then click Next.



SecureLogin - Add Application Wizard

Set Up a Windows Application.

This wizard gathers information that logs you in.

Steps

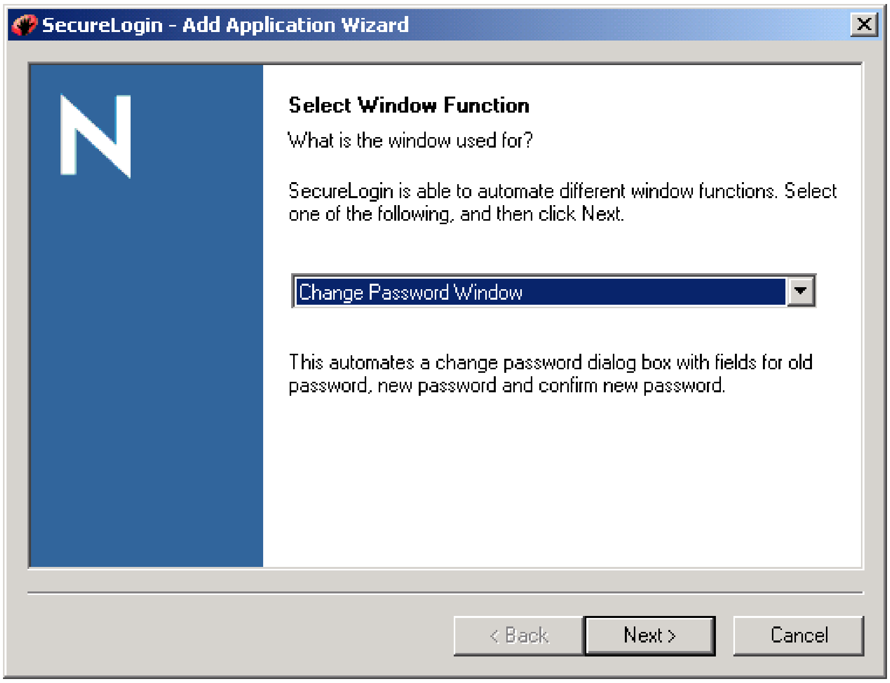
» Launch the application you want to enable.

» Enter your user name and password.

» Drag the hand icon to the title bar of the application you want to enable.

To continue, click Next.

6 Select Change Password Window from the drop-down list, then click Next.



SecureLogin - Add Application Wizard

Select Window Function

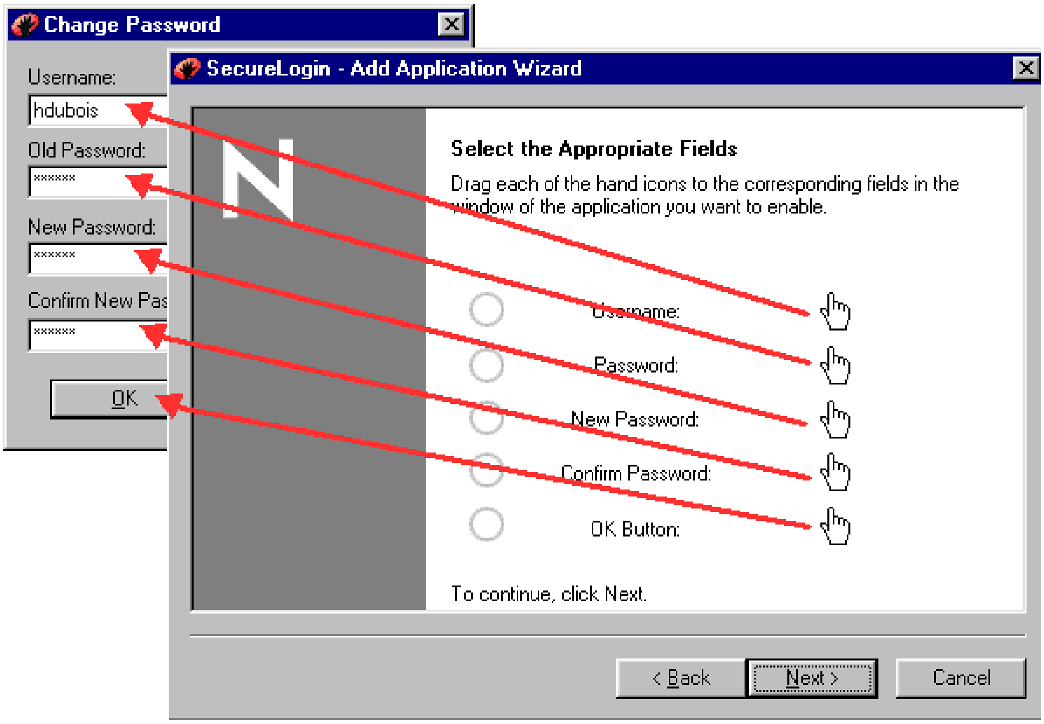
What is the window used for?

SecureLogin is able to automate different window functions. Select one of the following, and then click Next.

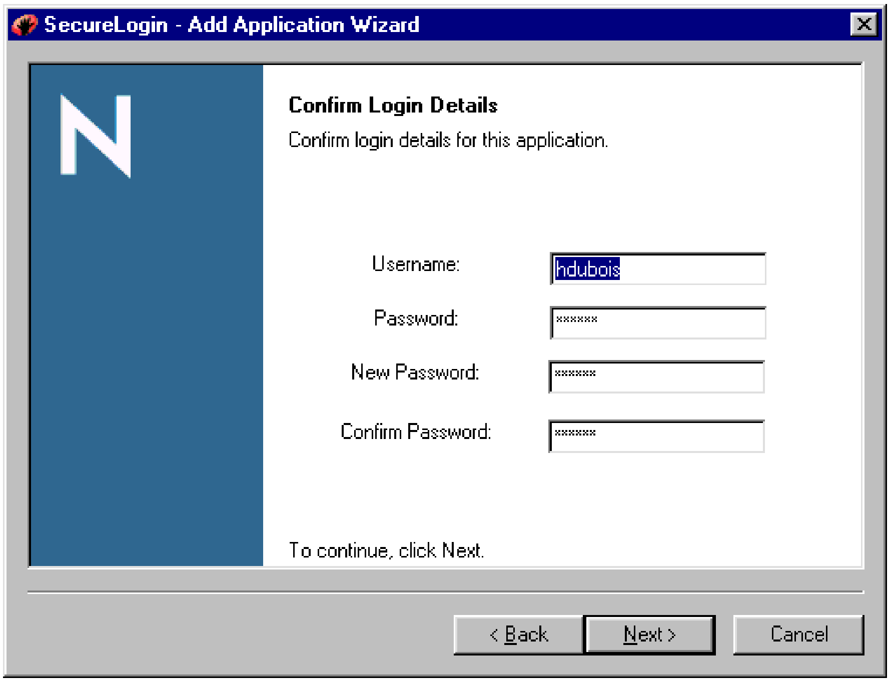
Change Password Window

This automates a change password dialog box with fields for old password, new password and confirm new password.

7 Type change-password information in the Change Password edit boxes, then drag the hand icons onto the corresponding Username, Old Password, New Password, Confirm New Password, and OK (Next, Login) fields in the Change Password dialog box.



8 In the Confirm Login Details dialog box, click Next.



SecureLogin - Add Application Wizard
Confirm Login Details
Confirm login details for this application.
To continue, click Next.
< Back
Next >
Cancel

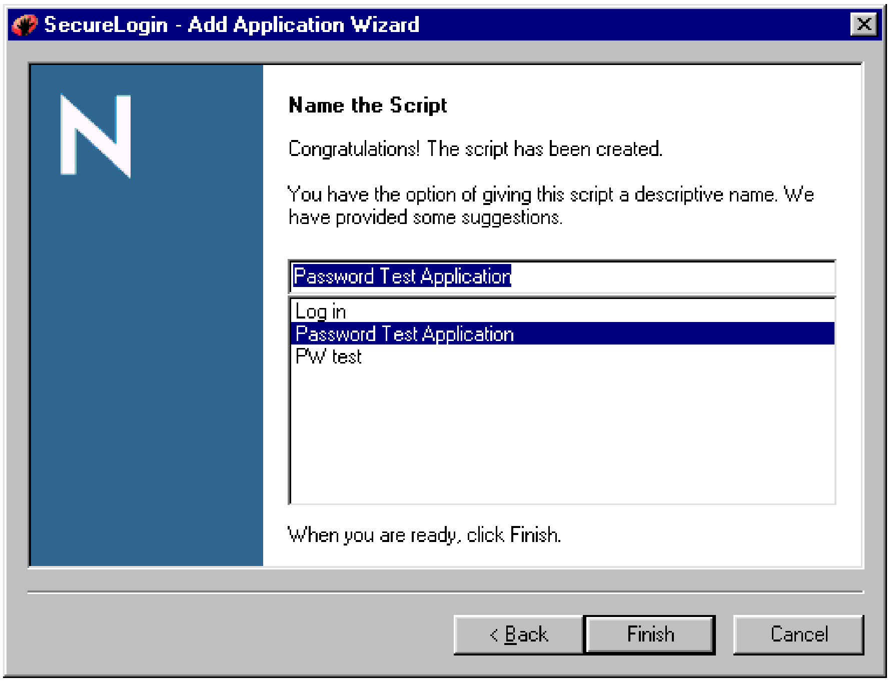
Username: hdubois

Password: ******

New Password: ******

Confirm Password: ******

9 In the Name the Script dialog box, select the name that already exists for the application.



SecureLogin - Add Application Wizard

Name the Script

Congratulations! The script has been created.

You have the option of giving this script a descriptive name. We have provided some suggestions.

Password Test Application

Log in
Password Test Application
PW test

When you are ready, click Finish.

10 Click Finish.

This process adds or updates the script's Change Password section. For information on the ChangePassword command, see "ChangePassword" in the *Nsure SecureLogin 3.51.2 Scripting Guide*.

11 To have the setting apply at the container level, copy the script from SecureLogin on the desktop to the application's script in the container.

Modifying Scripts to Respond to Messages

When you create a script for an application, it is important to respond to message boxes that appear. For example, the Password Test Application displays the following message boxes:

- Login Successful
- Change Password Successful
- Login Failure

To ensure that SecureLogin responds appropriately to the message boxes, you need to include each message box in the application's script.

This section provides information on the following:

- "Modifying "Password Changed" Message Boxes" on page 69
- "Modifying "Incorrect Password" Message Boxes" on page 71

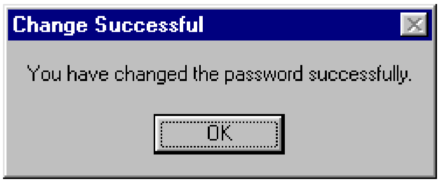
The information in this section uses Password Test Application as an example. However, the instructions apply to any Windows or Web application.

Modifying “Password Changed” Message Boxes

Many applications display a “password changed” message after the user changes a password. You can modify an application’s script so that SecureLogin does the following:

- Clears the application’s message.
- Updates credentials that SecureLogin has stored for the application.
- Displays your customized message.

1 Display the application’s “password changed” message.



Change Successful

You have changed the password successfully.

2 Right-click the SecureLogin icon on the task bar, then select Add Applications.

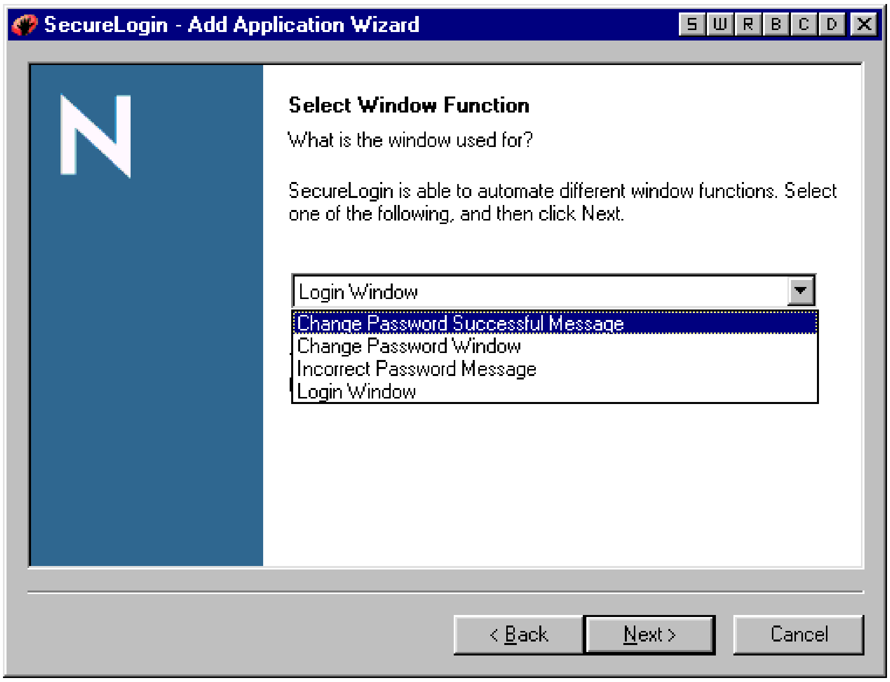
3 In the Welcome to SecureLogin dialog box, click Next.

4 Select Web Page or Windows Application (depending on your application), then click Next.

This example provides information on a Windows application.

5 In the Set Up a Windows Application dialog box, drag the hand icon to the application’s title bar (not to the error message box).

6 Select Change Password Successful Message, then click Next.



SecureLogin - Add Application Wizard

Select Window Function

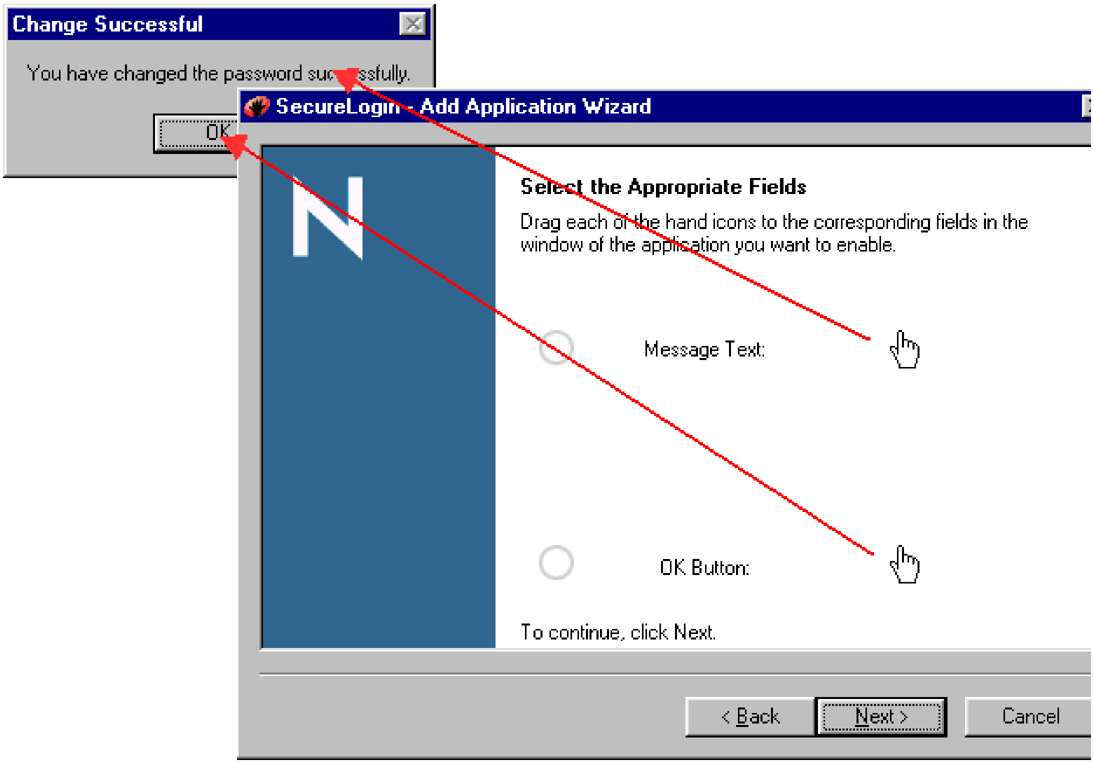
What is the window used for?

SecureLogin is able to automate different window functions. Select one of the following, and then click Next.

Login Window

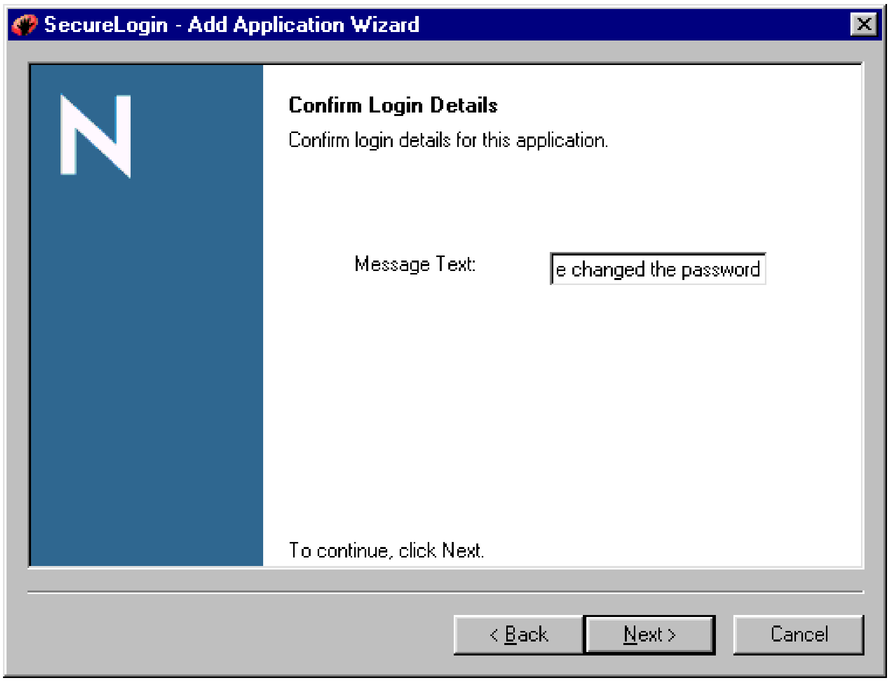
Change Password Successful Message
Change Password Window
Incorrect Password Message
Login Window

7 Drag the hand icons from the Wizard to the message text in the message box and to the OK button, then click Next.



Change Successful
You have changed the password successfully.
OK
SecureLogin - Add Application Wizard
Select the Appropriate Fields
Drag each of the hand icons to the corresponding fields in the window of the application you want to enable.
Message Text:
OK Button:
To continue, click Next.
< Back
Next >
Cancel

8 Modify the message by typing customized text in the Message Text edit box, then click Next.



SecureLogin - Add Application Wizard
Confirm Login Details
Confirm login details for this application.
To continue, click Next.
< Back
Next >
Cancel

Message Text: e changed the password

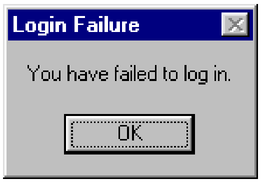
9 In the Name the Script dialog box, select the name that already exists for the application, then click Finish.

Modifying “Incorrect Password” Message Boxes

If an error occurs during login (for example, a credential is incorrect), SecureLogin displays an error message box. You can modify a script so that it responds to a login error message.

1 Display the application’s login error message.

The following figure illustrates the error message box in Password Test.exe.



Login Failure

You have failed to log in.

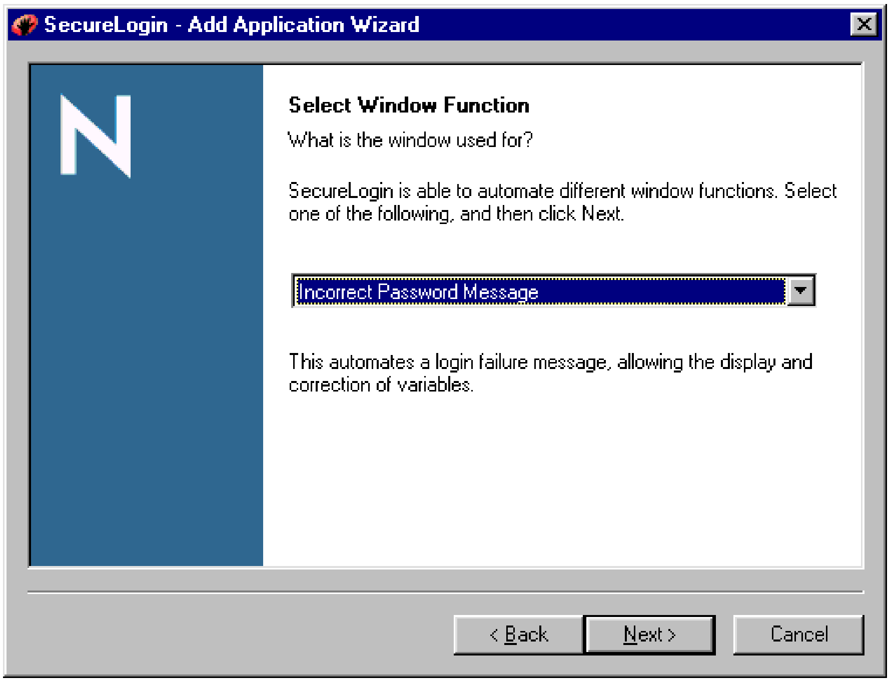
2 Right-click the SecureLogin icon on the task bar, then select Add Applications.

3 In the Welcome to SecureLogin dialog box, click Next.

4 Select Web Page or Windows Application (depending on your application), then click Next.

5 In the Set Up a Windows Application dialog box, drag the hand icon to the application’s title bar (not to the error message box).

6 Select Change Password Successful Message, then click Next.



SecureLogin - Add Application Wizard

Select Window Function

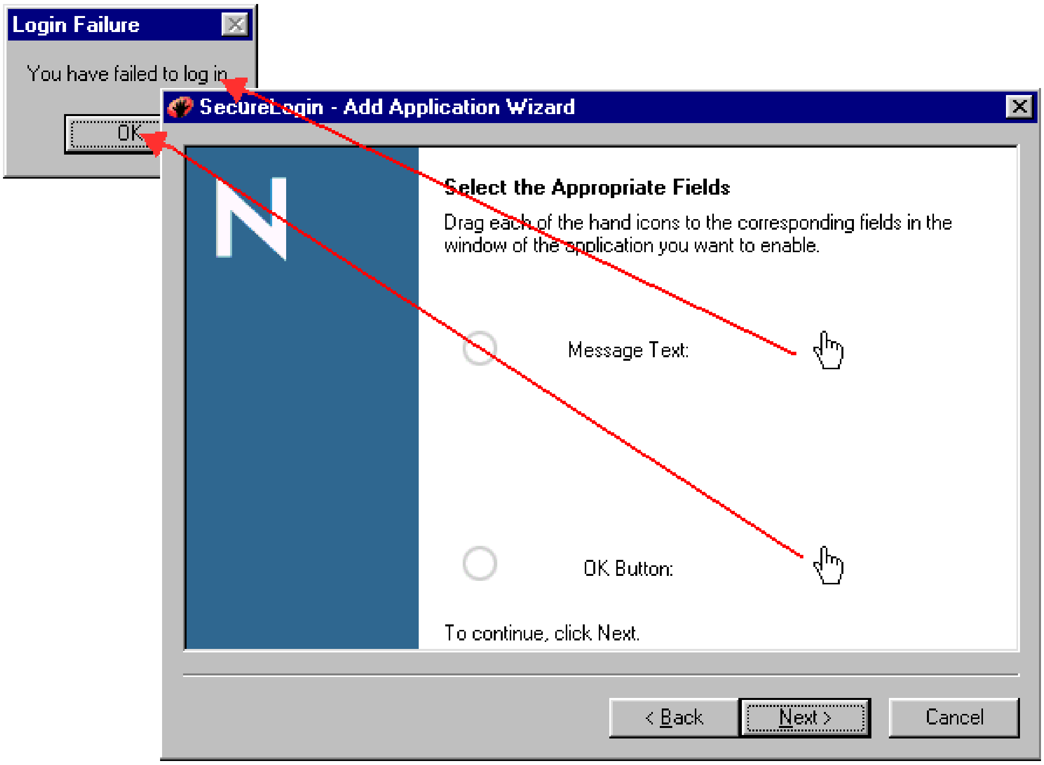
What is the window used for?

SecureLogin is able to automate different window functions. Select one of the following, and then click Next.

Incorrect Password Message

This automates a login failure message, allowing the display and correction of variables.

7 Drag the hand icons from the Wizard to the message text in the message box and to the OK button, then click Next.



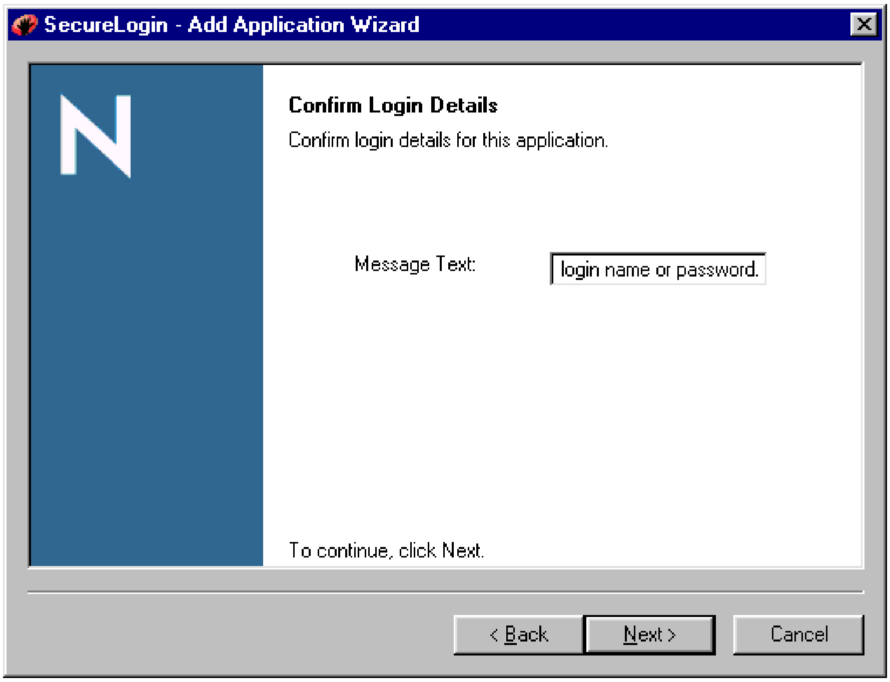
You have failed to log in.

Select the Appropriate Fields

Drag each of the hand icons to the corresponding fields in the window of the application you want to enable.

To continue, click Next.

8 Modify the message by typing customized text in the Message Text edit box, then click Next.



Confirm Login Details

Confirm login details for this application.

Message Text: login name or password.

To continue, click Next.

9 In the Name the Script dialog box, select the name that already exists for the application, then click Finish.

The next occurrence of an incorrect login displays a message box that has the changed text

An application might return one message for an incorrect username and a different message for an incorrect password. In such a case, handle both scenarios and display only the invalid credential by using the DisplayVariables command. See "DisplayVariables" in the *Nsure SecureLogin 3.51.2 Scripting Guide*.

Managing Corporate Scripts

Corporate scripts are normal scripts that are assigned to a Container object instead of to a User object. They reduce administrative tasks. You can create a container for corporate scripts, place a corporate script there, then point all users to that script. All users in or directed to that corporate script get their settings from that corporate script.

Corporate scripts differ from other scripts in two ways:

- The application is added in an Organization or Organizational Unit (OU) object instead of a User object.
- You use ConsoleOne, MMC, or SecureLogin Manager to add the application.
- User objects in the Organization or OU object, or objects lower in the directory tree, inherit settings from corporate scripts.

Windows Application, Web, Startup, and Terminal Launcher scripts can all be implemented as corporate scripts.

Where to Locate Corporate Scripts

In a corporate environment, all of the applications deployed to the users should match. You can ensure this by using Novell® ZENworks®. This means that the scripts for the applications will be identical. In a large tree, this could mean putting a copy of all of the scripts into each User container. You can copied these scripts, but only as a block. If you then need to update a single script you would have to copy all of the scripts to each container.

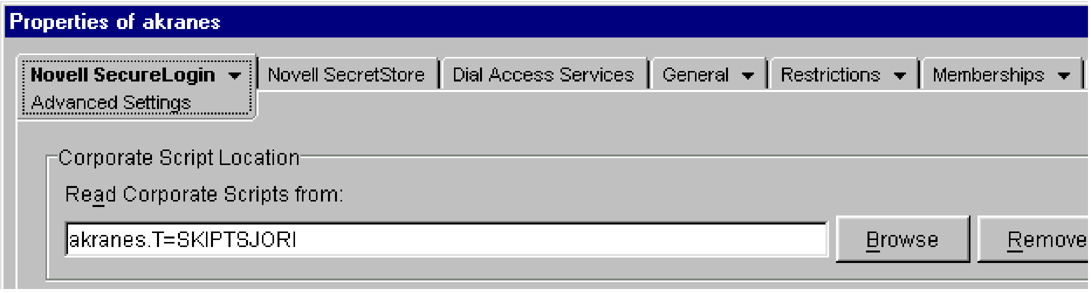
To eliminate this administrative overhead, you can point all of the users to a single corporate-scripts container. To make searching easy, you set this container relatively high in the tree, partition it, and replicate it to all user locations. Afterwards, when an application is introduced or modified, you need to add or modify only the script in one container. The script is then replicated out to all users.

Because they are automatically rolled out to all User objects held in the Container object, corporate scripts simplify implementing and administering SecureLogin single sign-on. By using this method, you don't have to configure applications for each individual user in your organization. All users read and use the same scripts.

Inheritance and Redirection

A corporate script is defined on a Container object. Objects within and below that container inherit the script.

After you create a corporate script, you can use the Read Corporate Scripts From edit box in ConsoleOne, MMC, or SecureLogin Manager to point to and use that script.



akranes.T=SKIPTSJORI

If you leave the Read Corporate Scripts From edit box empty, SecureLogin by default does the following:

- Reads the parent objects of the user (up to the object where you defined the Stop Walking Here setting as Yes).
- Applies these inherited settings to the user.

When you specify a context in this field, SecureLogin applies the settings of this context only and doesn't read any parent objects. The settings for the object are redirected from the context you specify in the Read Corporate Scripts From edit box to the object.

Scenario. The VMP company has 100 employees in the RDev department. VMP is a Container object, and RDev is a child Container object. Employees in the RDev department inherit settings from the VMP container.

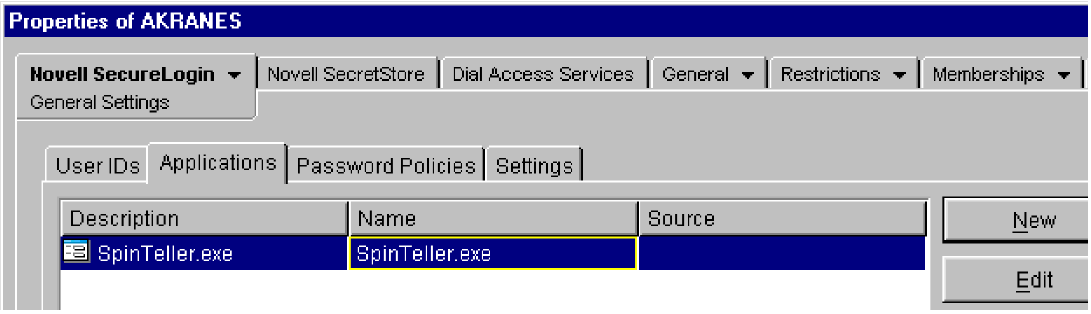
Ten employees in the RDev department require special SecureLogin settings for the AZ application. You create a new Container object (RDevAZapps) under the VMP container. You log in as admin, select the RDevAZapps Container object, then select Properties > Novell SecureLogin > General Settings. You create a script for the application that the 10 employees will use.

Next, you select one of the 10 users and access the Advanced Settings tab. You browse to and select the new RDevAZapp container, then click OK. That user now gets settings for the AZ application from the script in the RDevAZapps container. The settings have been redirected from the RDev container to the RDevAZapps container. You redirect all 10 users.

Inheritance of SecureLogin data stops at the container or OU. Redirected containers or OUs don’t inherit settings, enabled applications, or password rules that an Organizational Policy container or OU inherits from another container or OU.

Creating a Corporate Script: MMC or ConsoleOne

1. Log in as Admin or an Admin equivalent.
2. Navigate to the Container object where you want to create the corporate script.
3. Right-click the Container object, then click Properties.
4. Click Novell SecureLogin > General Settings > Applications > New.



Properties of AKRANES

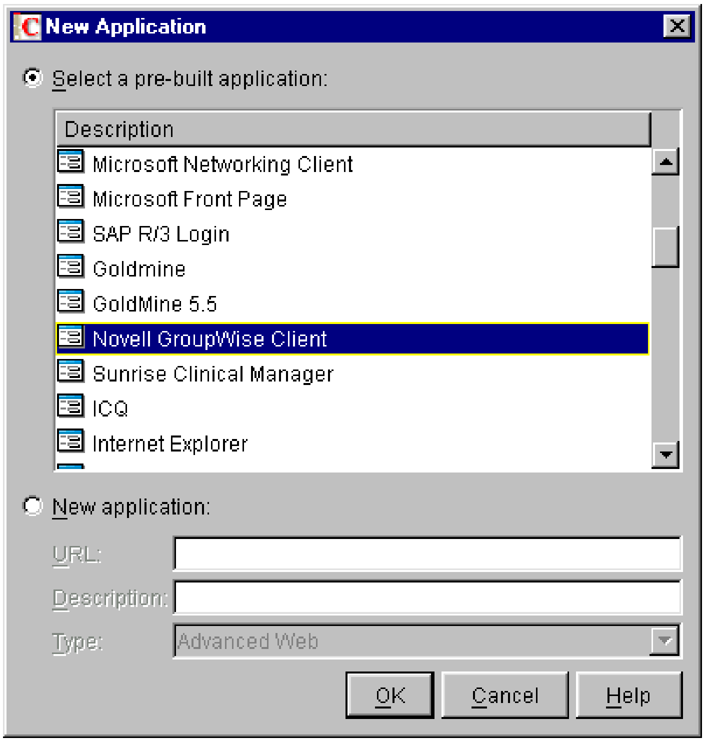
Description	Name	Source
SpinTeller.exe	SpinTeller.exe	

To use a prebuilt script, go to Step 5.

To create a new script for an application, without using a prebuilt script, go to Step 6.

5 (Optional) Add a prebuilt script to the application list.

5a Click Select a Prebuilt Application, scroll to and select the desired application, then click OK.



New Application

● Select a pre-built application:

Description
Microsoft Networking Client
Microsoft Front Page
SAP R/3 Login
Goldmine
GoldMine 5.5
Novell GroupWise Client
Sunrise Clinical Manager
ICQ
Internet Explorer

○ New application:

URL:

Description:

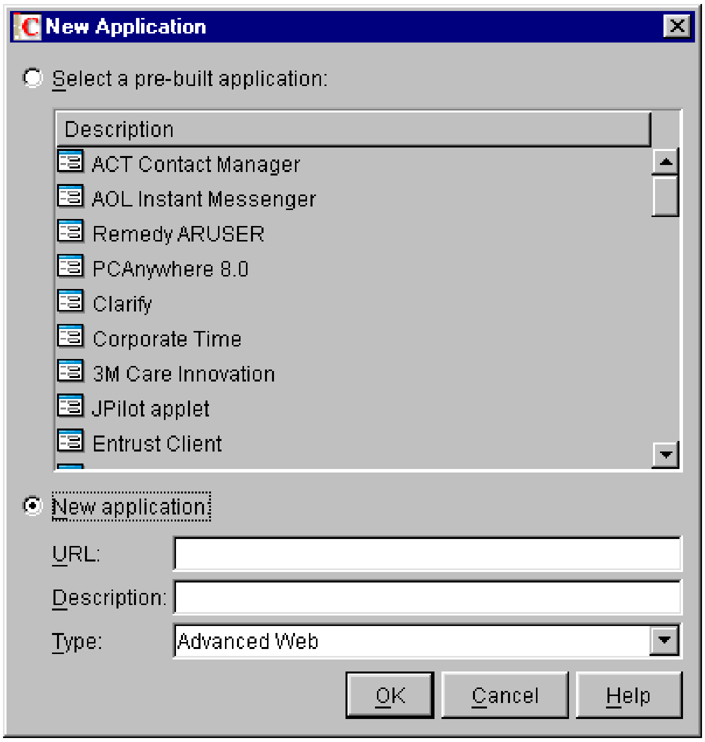
Type: Advanced Web

5b In the Applications [*application name*] dialog box, save the script by clicking OK.

After you click OK, you return to the Applications tab. Go to Step 7.

6 (Optional) Add an application that doesn't have a script.

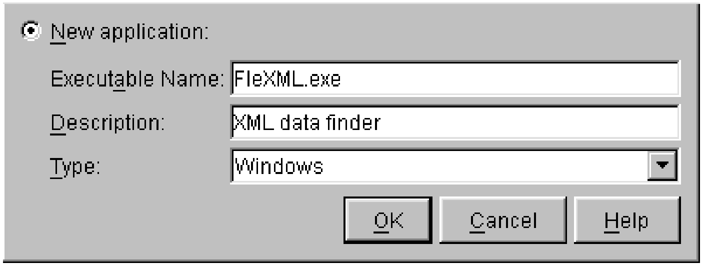
6a From the New Application dialog box, click New Application.



Type: Advanced Web

6b Type a name in the first text field.

For a Windows application, type the executable filename. For a Web application, type the URL. This name will display in the Description column on the Applications tab.



Executable Name: FIeXML.exe

Description: XML data finder

Type: Windows

6c Select a type (for example, Java, Startup, Windows) from the drop-down list, then click OK.

7 In the Applications tab, save the data by clicking Apply.

The next time the selected application is launched, users will be prompted to enter their credentials.Whenever the application is subsequently launched, SecureLogin enters the users' credentials, as though the login process has been eliminated.

8 Click the newly added application, click Edit, then click Script.

9 Add or edit a script.

For hands-on experience with basic scripting, work through the tutorial in the chapter, “Practicing Your Scripting Skills” in *Nsure SecureLogin 3.51.2 Scripting Guide*.

For script commands, with accompanying example scripts and explanations, see chapter, “SecureLogin Commands”in *Nsure SecureLogin 3.51.2 Scripting Guide*.

Creating a Corporate Script: SecureLogin Manager

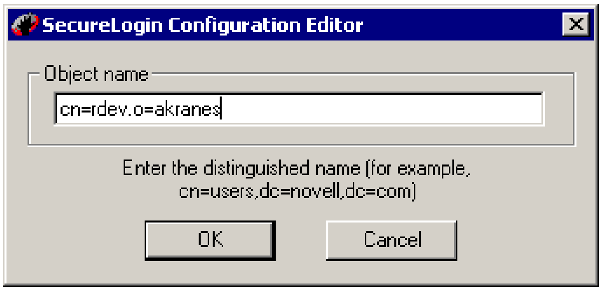
1 Log in to the workstation as Admin or equivalent.

2 Run SecureLogin.

3 Launch SecureLogin Manager.

Run slmanager.exe, found in the \securelogin\client\tools directory.

4 Type the distinguished name of the object where you want to create a corporate script.



cn=rdev.o=akranes

Enter the distinguished name (for example, cn=users,dc=novell,dc=com)

You logged in to the workstation as Admin or equivalent, then accessed SecureLogin as that user. SecureLogin Manager uses the rights of the authenticated user to create the corporate script for the context or object that you specify.

For AD and LDAP, use LDAP naming conventions (for example, cn=admin,cd=akranes). For eDirectory, use eDirectory conventions (for example, cn=admin.o=akranes).

5 Click OK.

Exempting an Object from a Corporate Script

Local scripts take precedence over corporate scripts. Occasionally, you might want a particular user to use a script other than the corporate script. To do this, create a local script for the application at the User object level.

If you have a corporate script for an application, and you have a user who should not have that application single sign-on enabled, create a blank local script for the application at the User object level.

You can also use this procedure to exempt a Container object from corporate scripts inherited from Container objects that are higher in the directory tree.

Using SecureLogin with Client Software

When you use SecureLogin with the following, additional functionality allows SecureLogin to leverage the user's information to authenticate to a directory:

- The Novell Client™ for Windows NT* or the Novell Client for Windows 9*x*
- The eDirectory option (selected during installation)
- The eDirectory with SecretStore option (selected during installation)
- The Microsoft Active Directory option (selected during installation)
- The LDAP option (selected during installation)

You can reference the ?*sysuser* and ?*syspassword* variables from within an application script, avoiding the need to store a copy of this data in the directory. Additionally, when the user is authenticating to SecureLogin while disconnected from the directory, the directory password can be used in place of the user's passphrase answer.‘

If you use SecureLogin with the Novell Modular Authentication Services™ (NMAS™) client, using the eDirectory password method, no additional installation or configuration is required. By default, the NMAS client hides the eDirectory password field in the Novell Client login dialog box in favor of a subsequent password prompt.

Deploying SecureLogin

The SecureLogin environment consists of user IDs, scripts that enable applications for single sign-on, password policies (rules), and SecureLogin settings. You can manage this environment individually (at the User object level), collectively (at the container or OU level), or both.

In a Microsoft Active Directory, SecureLogin cannot be configured from the highest level or root of the network directory. You need to configure each container or OU individually. To facilitate speedy deployment, SecureLogin provides two options for the distribution of the SecureLogin data across containers and organizational units:

- Copy Settings functionality (copy, export, or import settings)

  Copy Settings functionality exports and imports the SecureLogin environment in XML file format from one container or OU to another. We recommend that you test your SecureLogin configuration on a test User object and then copy the environment to the relevant container or OUs.

  Use the Copy Settings functionality if

  - You need to distribute configurations across a LAN or WAN.
  - You need to copy a SecureLogin environment from one object to another, for example from a User object to a container or OU.
  - The containers require the same or similar SecureLogin environment.

    It is faster to copy and apply the basic settings, and then modify the settings, than to configure each container or OU individually.
  - You need a backup of your user environment for disaster recovery.
- Redirect organizational policy

  Organizational policy functionality redirects one container or OU to another, essentially inheriting the container's or OU's SecureLogin environment.

  Scenario: Redirecting. In the DigitalAirlines Company, the directory tree includes the Development, Marketing, and Sales organizational units. The SecureLogin environment is required to be the same for the Sales and Marketing departments. However, the administrator doesn't want the User objects for each department in the same OU.

  Implementing SecureLogin's Organizational Policy functionality, the administrator selects Marketing to be the Corporate Policy OU. The Sales OU is then directed to obtain the SecureLogin environment from the Marketing OU. Any changes made to the Marketing SecureLogin environment are automatically inherited by Sales, significantly reducing administration.

  Use redirection if

- Multiple containers or OUs require the same SecureLogin environment.
- Inheritance from a higher level than the Organizational Policy container or OU is not required.
- Administrator User objects are manually configured.
- The container or OUs are on the same directory tree.

  We recommend that you not use redirection across a LAN or WAN.

Copying, Exporting, and Importing SecureLogin Settings

The Copy Settings feature enables you to copy SecureLogin settings (data) from one object in a directory tree to one or more objects in that tree. You can copy an object's settings to a container, OU, or User object. The objects can be in the same context or in a different context. You can't copy settings from one tree to another.

However, you can export or import settings from one tree to a target tree. After settings are exported or imported, you can then copy them from within the target tree.

Also, you can copy from one administrative tool (ConsoleOne, MMC, or SecureLogin Manager) and import into another tool.

The Copy feature saves settings internally (RAM) and copies to objects. The Export feature saves the settings externally to an XML file. You can then use the XML file repeatedly to import settings to objects.

Copy Settings doesn't copy, export, or import variables. Therefore, usernames and passwords are not copied, exported, or imported.

Copying SecureLogin Settings

To copy SecureLogin settings, use the following guidelines:

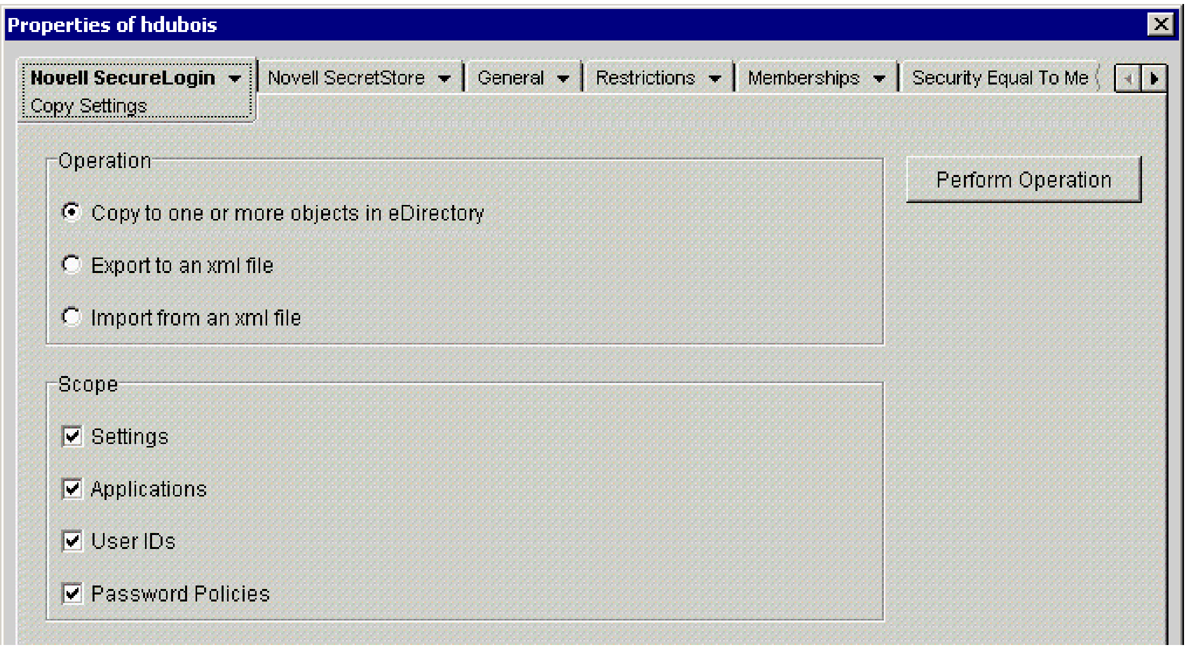
- Typically, copy from a User object to a User object and from a Container object to a Container object.
- Copy settings to an object in the same context, a parallel context, or a subordinate context. Don't copy settings from an object in a subordinate context to an object in a superior (higher in the tree) context.
- Copy items that have local settings. When inheritable settings are copied, they become local settings on the object that the settings are copied to. Such copied settings might have broken login-to-application links.
- Ensure that you don't overwrite Administrator settings when copying settings to a container or organizational unit. For example, if you set the option Allow Users to View and Change Settings to No, and then copy this as part of a SecureLogin environment to the container/OU including the Administrator user object, the Administrator won't be able to view or change SecureLogin settings. To prevent this from happening, always change the settings on Administrative accounts before restricting the associated container or OU settings.

To copy settings:

1 In ConsoleOne, right-click the object that has the settings that you want to copy, then click Properties.

  You can select an Organization, Organizational Unit, Locality, Country, or User object.

2 At the Novell SecureLogin tab, select Copy Settings.



Properties of hdubois

Operation

● Copy to one or more objects in eDirectory

○ Export to an xml file

○ Import from an xml file

Scope

☑ Settings

☑ Applications

☑ User IDs

☑ Password Policies

3 Select Copy to One or More Objects in eDirectory, then select all check boxes (in the Scope pane) for settings that you want to copy.

By default, all data are selected. To limit the scope, select check boxes for data that you don't want to copy, export, or import.

For example, if you only want to copy user IDs, select the other check boxes.

4 Click Perform Operation.

5 On the Select Objects page, select one or more objects that you want to copy the settings to.

You can browse to and select one or more objects from other contexts, but you can't select objects from other trees. You can select objects in one context and then browse to other contexts to select additional objects.

To select an object, click it, then click Select. Selected objects appear in the Selected Objects pane.

6 Click OK.

Exporting SecureLogin Settings

You can export settings from one tree and import them into the same tree or a different tree. The Export and Import options operate on the same settings as Copy Settings.

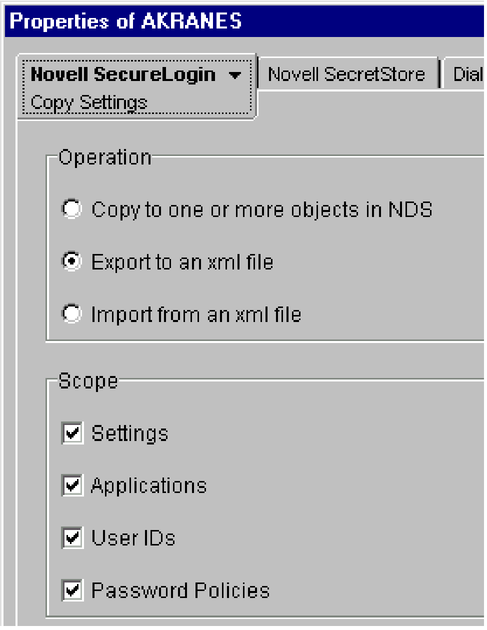
To export and import settings, you use XML files. The files have a corresponding XML schema file (nsldata.xsd).

The XML schema file specifies XML tags and type of data. The file controls how SecureLogin behaves.

To export SecureLogin Settings:

1 Right-click the object that has the settings that you want to export, then click Properties.

2 On the Novell SecureLogin page, click Copy Settings.



Properties of AKRANES

Operation

○ Copy to one or more objects in NDS

● Export to an xml file

○ Import from an xml file

Scope

☑ Settings

☑ Applications

☑ User IDs

☑ Password Policies

3 Click Export to an XML File, then select all check boxes (in the Scope pane) for settings that you want to export.

To limit the scope, deselect check boxes for settings that you don't want to export.

4 Click Perform Operation.

5 Save the settings to an XML file.

Navigate to the directory where you want to save the XML file, specify the filename, then click Save.

The settings are ready to import to another object.

You can edit exported XML files. The XML schema file is provided so that you can verify any modified XML file. However, an easier way to verify a modified file is to import it. The SecureLogin snap-in to ConsoleOne reports an error if the modified file has incorrect syntax or some other problem.

Importing SecureLogin Settings

1 Right-click the object that you want to import the settings to, then click Properties.

2 Select Copy Settings.

3 Select Import, then select all check boxes (in the Scope pane) for settings that you want to import.

To limit the scope, deselect check boxes for settings that you don't want to import.

4 Click Perform Operation.

5 Navigate to and select the XML file that contains the settings that you want to import, then click Open.

When you import settings from an XML file, SecureLogin validates the XML file against the XML schema. An invalid XML file is rejected.

You can only import settings to one object at a time. However, after importing you can then copy (within the target tree) settings that you imported.

Redirecting

Inheritance of SecureLogin data stops at the container or OU. Redirected containers or OUs don’t inherit settings, enabled applications, or password rules that a container or OU inherits from another container or OU.

The following process illustrates how to redirect a Sales OU to inherit the SecureLogin configuration from the Marketing OU by using Active Directory.

1. Select Start > Programs > Administrative Tools > Active Directory Users and Computers.
2. Right-click the Sales OU, then select Properties.
3. Select SecureLogin SSO, then click Advanced Settings.
4. In the Read Corporate Scripts and Settings From edit box, type the container or OU.

   Type the complete distinguished name, so that you uniquely identify the container or OU. For example, type

   ```
   CN=Users,CD=www,DC=server,DC=com
   ```

   To remove a name, click Remove.
5. Save the data and close the Advanced Settings page by clicking OK.
6. To verify inheritance and redirection, double-click the SecureLogin icon on the task bar, then select Applications.

   Prebuilt scripts and password policies that are available at the container or OU level display a checkmark on the icon in the Application Description column. These application scripts and password policies are created and maintained at the container or OU level. Therefore, they can’t be edited or deleted by using SecureLogin on the desktop.

   For additional information on redirection, see “Managing Corporate Scripts” on page 73.

Defining Applications That SecureLogin Detects

SecureLogin automatically detects most applications that require users to log in. You or the user can set the preferences to have SecureLogin detect or ignore Windows, Java, or Internet applications. However, you might want SecureLogin to detect or ignore a particular application without setting a preference that will be applied to all applications. You achieve this by creating an exclude.ini file on the workstation and defining the applications that you want SecureLogin to ignore or detect.

Applications to be included and excluded are listed in the same exclude.ini file.

SecureLogin is hard-coded to include or exclude the following applications:

captainhook.exe	notes.exe	setup.exe
combro~1.exe	nswebsso.exe	sllock.scr
slbroker.exe	nwadmn32.exe	slmanager.exe
loginw32.exe	nwadmn95.exe	slproto.exe

loginw95.exe	nwadmnnt.exe	slwinsso.exe
mmc.exe	nwtray.exe	tlaunch.exe
msdev.exe	protocomsystray.exe	wfica32.exe
nlnotes.exe	scrnlock.scr	

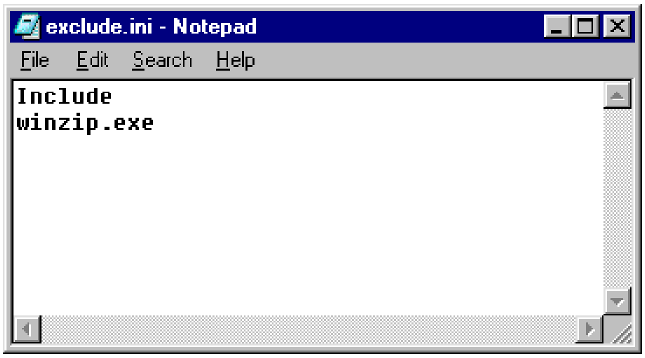
Detecting Specific Applications

You can use the Include command to specify applications that SecureLogin detects. The Include command has the following benefits:

- Increases performance
- Stops auto-detection of new applications
- Stops SecureLogin auto-detection of any applications not listed in the file
- Increases security

To specify applications:

1. Create a file in a text editor.
2. Type Include on the first line.



```
Include
winzip.exe
```

3. List the applications that you want SecureLogin to detect.

   When you use the Include command, list every application that SecureLogin needs to detect. Don’t enter more than one application on a line.

4. Save the file as exclude.ini in the SecureLogin installation directory.

   Typically, the directory is c:\Program Files\Novell\SecureLogin.

Ignoring Additional Applications

To use the exclude.ini file to prevent SecureLogin from detecting applications:

1. Using a text editor, create a file.
2. Type Exclude on the first line.

   You can’t simultaneously use Exclude and Include commands.

3. Type Nodefault next to the first application name.
4. List the executable names of applications that you want SecureLogin to ignore.

List all the applications except those that SecureLogin is to detect. Add one executable name per line. For example, to prevent SecureLogin from detecting weblog.exe, enter the following line in the exclude.ini file:

```
weblog.exe
```

5 Save the file as exclude.ini in the SecureLogin installation directory.

Typically, the directory is c:\Program Files\Novell\SecureLogin.

Setting Local Cache Expiration

If the offline cache has been enabled by the SecureLogin administrator, the offline cache downloads SecureLogin data from the network directory, encrypts the data, and stores it on the workstation. The cache contains SecureLogin configuration information, including password policies, user credentials, applications enabled for single sign-on, and settings. The cache enables SecureLogin to operate even when the workstation is disconnected from the network.

To ensure that users regularly update their caches, previous versions of SecureLogin set a mandatory expiration timeframe of seven days from last cache update. The current version of SecureLogin does not include a mandatory cache expiration. This change caters primarily to mobile users who are not always able to connect to their directory within seven days.

You can modify expiry dates on the user workstation by using the Registry Editor.

To set the local cache expiration period:

1 Click Start > Run.

2 In the Open edit box, type regedit, then click OK.

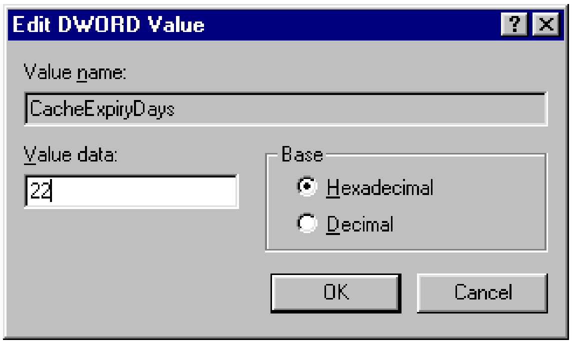
3 In the registry editor, select HKEY_LOCAL_MACHINE\software\Protocom\SecureLogin.

4 Right-click SecureLogin, then select New > DWORD Value.

5 Overtype New Value [#1] with CacheExpiryDays, the press Enter.

6 Double-click CacheExpiryDays.

7 In the Edit DWORD Value dialog box, enter the required number, then click OK.



CacheExpiryDays

22

● Hexadecimal
○ Decimal

The value data is the number of days. Don’t enter 0 (zero) because the cache would expire immediately upon refresh.

8 Quit the Registry Editor by selecting Exit from the Registry menu.

SecureLogin Attribute Provisioning Tool

The SecureLogin Attribute Provisioning Tool (SLAP tool) enables SecureLogin to leverage an organization's provisioning system. You can use the SLAP tool to import the following data, in XML format, from third-party applications into the SecureLogin user's datastore as well as export information (except for passwords and passphrases):

- User IDs
- User variables
- Application scripts
- Organizational settings
- Password policies
- User credential sets
- Passphrase questions and answers

The SLAP tool operates as a bidirectional translator between SecureLogin data in a directory and an XML file. The XML schema used is the same as the Copy Settings GUI importer/exporter. In addition to copying settings, the SLAP tool can extract usernames. The SLAP tool doesn't export sensitive data such as passwords and passphrases.

For example, an organization with 10,000 users in a SAP* system, implementing SecureLogin, can speed deployment significantly by automating the initial user login with the SLAP tool. Use the SLAP tool to extract the usernames and passwords into a text file that is subsequently loaded into SecureLogin. The SLAP tool removes the requirement for each user to enter credentials on first login to SecureLogin.

SLAP Tool Syntax

The SLAP tool syntax is

```
slaptool [-hlaspcPef] -r object_name_file | -o "object" [file ...]
```

Option	Description
-h	Displays a help message and exits. (All other options are ignored.)
-l	Excludes user IDs.
-v	Excludes variables. (Passwords aren't exported in the current version.)
-a	Excludes applications.
-s	Excludes settings.
-p	Excludes password policies.
-c	Excludes credsets.
-P	Excludes the passphrase. (Affects import only.)
-e	Performs an export rather than an import.
-r object_name_file	Specifies a file containing line-delimited object names on which to perform the operation.

Option	Description
-o object	Specifies a particular object on which to operate.
-f	Uses the cache file, rather than accessing a directory. (This option can't be used with -r or -o, and SecureLogin must be set to use Dummy mode. The user is selected interactively at runtime).
[file ...]	Specifies one or more .xml files to read data from (or, if exporting, to write data to). No file specification reads or writes data from or to stdin or stdout.

For example,

```
./slaptool.exe -o "CN=markus.O=novell.T=RDev" initial_setup.xml
```

In this example, slaptool.exe reads user IDs, applications, settings and password policies from the file initial_setup.xml and writes them out to the object CN=markus.O=novell.T=RDev.

SLAP Tool Example

The following example Perl script assumes usernames and passwords are stored in a text file named listofnames.txt. There is one space between each username and password pair per line.

An XML file that contains the data for import is required to run this script. Where the data is customized on a per username basis, the string to be substituted is replaced with *usernamegoeshere*.

```
open FILE,"listofnames.txt";
foreach (<FILE>) {
chomp;                  # Clean string
@lines = split(/\n/);   # Split up string
foreach $l (@lines) {
  @fields = split(/\s/);
  $name = $fields[0];
  $pass = $fields[1];
  open DATAFILE,"source.xml";
  open OUTFILE,">data.xml";
  foreach (<DATAFILE>) { # Write up a file specific to this user
    s/\*usernamegoeshere\*/$name/;
    s/\*passwordgoeshere\*/$pass/;
    # Any other variable susbstitution can be done here too...
    print OUTFILE "$_";
  }
    close DATAFILE;
    close OUTFILE;
    system "slaptool.exe -o \"CN=$name.O=myorg.T=OURCOMPANY\" data.xml";
      }
}
close FILE;
unlink 'data.xml';
```

Using an XML file called source.xml, run the script with the data to be imported. For example, import data that has been manually exported from a single user setup, but with the value for the username replaced with the string "*usernamegoeshere*".

The example script does not include error handling.

XML File Example

```
<?xml version="1.0"?>
<securelogin>
   <passphrasequestions>
      <question>Please enter a passphrase for SLAP testing.</question>
   </passphrasequestions>
   <passphrase>
      <activequestion>Please enter a passphrase for SLAP testing.</
activequestion>
      <answer>passphrase</answer>
   </passphrase>

   <logins>
      <login>
         <name>fnord</name>
         <symbol>
            <name>username</name>
            <value>bob</value>
         </symbol>
         <symbol>
            <name>Password</name>
            <value>test</value>
         </symbol>
      </login>
      <login>
         <name>notepad.exe</name>
         <symbol>
            <name>username</name>
            <value>asdf</value>
         </symbol>
         <symbol>
            <name>Password</name>
            <value>test</value>
         </symbol>
      </login>
      <login>
         <name>testlogin</name>
         <symbol>
            <name>username</name>
            <value>Novell</value>
         </symbol>
         <symbol>
            <name>Password</name>
            <value>test</value>
         </symbol>
      </login>
    </logins>
</securelogin>
```

Running Slaptool.exe

Run slaptool.exe from a command prompt.

If slaptool.exe doesn’t run from the securelogin\tools directory, you might need to copy the following files to the Program Files\Novell\SecureLogin directory, and run slaptool.exe from there:

- slaptool.exe
- libxml2.dll
- getopt.dll

3 Using Login Watcher

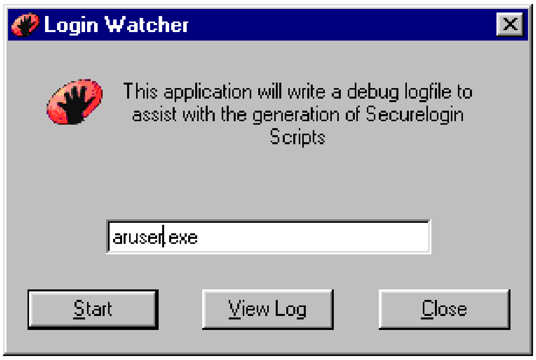
Login Watcher helps you enable applications to work with SecureLogin.

1 Close SecureLogin.

   SecureLogin might prompt you to close some applications before it can stop running.

2 Run loginwatch.exe, found in the \securelogin\tools directory.

3 Type the name of the application you want to watch (for example, aruser.exe.).



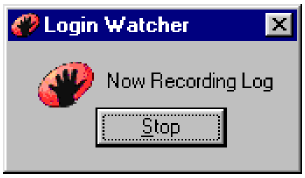
This application will write a debug logfile to assist with the generation of Securelogin Scripts

aruser.exe

   Include the filename extension.

4 Click Start.

   The following dialog box appears in the corner of the screen.



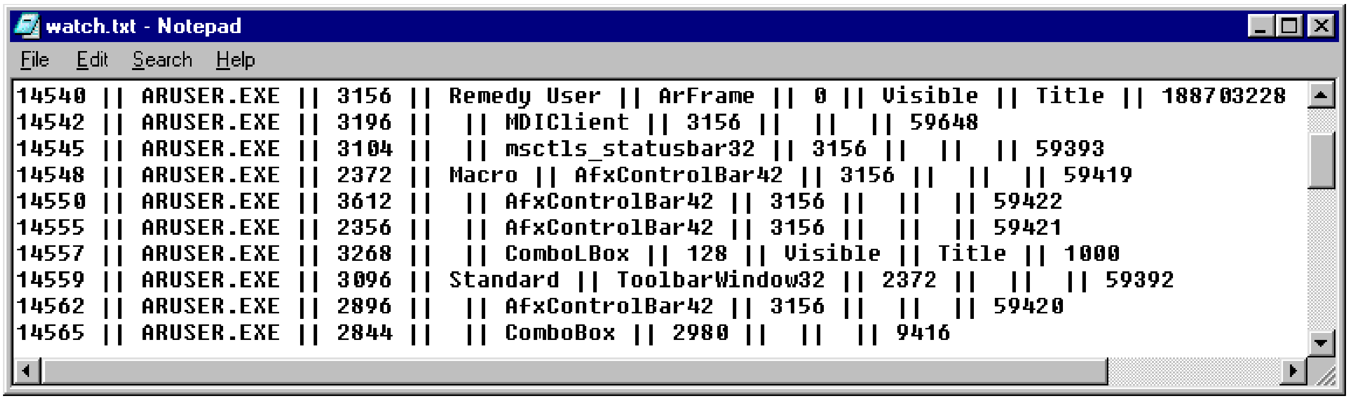
Now Recording Log

5 Run the application (for example, Remedy Aruser) that you want Login Watcher to watch.

   Login Watcher logs all details related to the dialog boxes that the program displays.

6 Click Stop on the Login Watcher dialog box.

7 Click View Log.



```
14540 || ARUSER.EXE || 3156 || Remedy User || ArFrame || 0 || Visible || Title || 188703228
14542 || ARUSER.EXE || 3196 ||  || MDIClient || 3156 ||  ||  || 59648
14545 || ARUSER.EXE || 3104 ||  || msctls_statusbar32 || 3156 ||  ||  || 59393
14548 || ARUSER.EXE || 2372 || Macro || AfxControlBar42 || 3156 ||  ||  || 59419
14550 || ARUSER.EXE || 3612 ||  || AfxControlBar42 || 3156 ||  ||  || 59422
14555 || ARUSER.EXE || 2356 ||  || AfxControlBar42 || 3156 ||  ||  || 59421
14557 || ARUSER.EXE || 3268 ||  || ComboLBox || 128 || Visible || Title || 1000
14559 || ARUSER.EXE || 3096 || Standard || ToolbarWindow32 || 2372 ||  ||  || 59392
14562 || ARUSER.EXE || 2896 ||  || AfxControlBar42 || 3156 ||  ||  || 59420
14565 || ARUSER.EXE || 2844 ||  || ComboBox || 2980 ||  ||  || 9416
```

The log is saved in c:\watch.txt.

Login Watcher records the information in the following format: time || ModuleName || window handle || window text || class name || parent || Visible flag || Title Flag || Control ID. The following table provides information on the format:

Format Item	Description
Time	The milliseconds elapsed since the recorder was started (for example, 14540)
Module Name	The name of the executable that created the window (for example, aruser.exe).
Window Handle	The unique identifier of that instance of the window (for example, 3156).
Window Text	The text of the window (for example, Remedy User). For edit boxes, the text is the contents. For buttons, the text is the label. For windows with titles, the text is the title.
Class Name	The name of the window class (for example, ARFrame).
Parent	The window handle of the parent window. Allows SecureLogin to cross-reference through the list and find the parent.
Visible Flag	Set on top-level windows that have the style Visible set.
Title Flag	Set on top-level windows that have the style Title set.
Control ID	The unique identifier of that control in the program (for example, the control to type a password). Login Watcher appends data to the existing watch.txt file.

4 Working with Terminal Emulators

This section provides information on the following:

- "Introduction to Terminal Launcher" on page 89
- "Enabling an Emulator Application for Single Sign-On" on page 89
- "Configuring Backup Sessions" on page 110
- "Determining Which Session File To Automatically Use" on page 111
- "Using Terminal Launcher With Non-HLLAPI-Compliant Emulators" on page 111

Introduction to Terminal Launcher

Terminal Launcher configures terminal emulator applications and enables them for single sign-on.

Terminal Launcher does the following:

- Acts as the translator between an emulator login sequence and a user's variables (for example, the username and password) stored in SecureLogin.
- Coordinates the information being entered onto a mainframe or Telnet screen.

Terminal Launcher can use High Level Language Application Programming Interface (HLLAPI) commands to interface with a wide range of mainframe emulators.

The SecureLogin scripting language enables you to enter a variety of keystrokes through Terminal Launcher to an emulator. For information on scripting and the commands used with Terminal Launcher, see the *Nsure SecureLogin 3.51.2 Scripting Guide*.

Terminal Launcher supports the following emulator types:

- HLLAPI
- DDE
- VBA
- Generic
- Advanced Generic

Standalone users or SecureLogin administrators can choose to start emulator applications in Terminal Launcher. However, users in most organizations are unlikely to have access to Terminal Launcher.

Enabling an Emulator Application for Single Sign-On

The main steps to enable an application include the following:

- “Creating a Terminal Emulation Session File” on page 90.
- “Creating a Script for the Emulator Application” on page 90
- “Configuring the Emulator” on page 92
- “Creating a Login for an Emulator” on page 106
- “Setting Up a Shortcut” on page 108

Creating a Terminal Emulation Session File

Before enabling any terminal emulator for single sign-on, you need to create a session file. This file includes the following:

- All the required settings for the server to connect to.
- Any other parameters required for deployment to users.

The session file can be saved locally or on the server. You configure SecureLogin to access the file in the specified location. When SecureLogin launches the emulator, SecureLogin executes this session file.

To create a session file:

1. Start the terminal emulator application.
2. Connect to the required host.
3. Modify the terminal emulator settings as required.
4. Save the session.

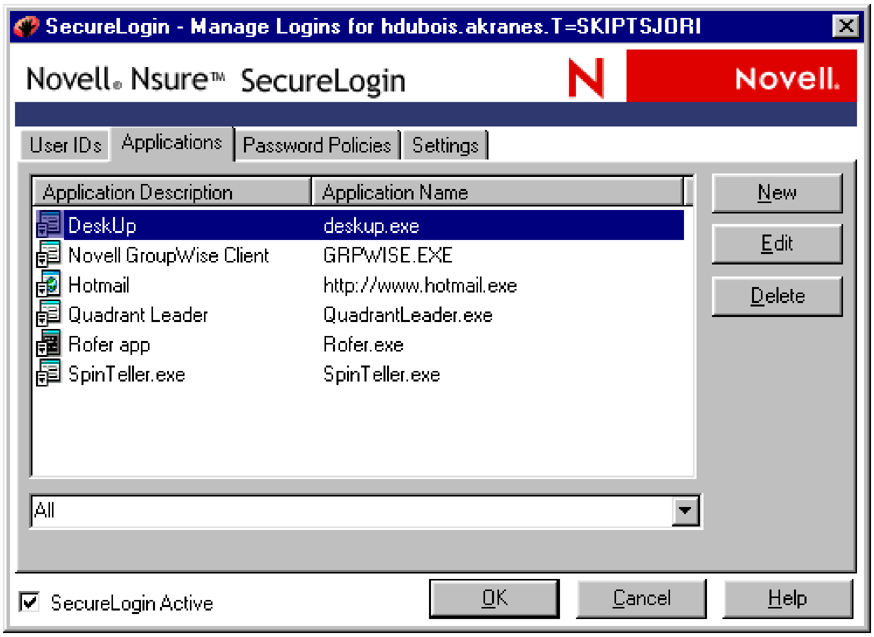
   By default, the session file is typically saved to the application’s installation directory.
5. From the Connection menu, select Disconnect.

   The session file remains loaded, but you have disconnected from the host.
6. From the File menu, select Save [*session name*].
7. Quit the terminal emulator application.

Creating a Script for the Emulator Application

The following example sets up SecureLogin Terminal Launcher to single sign-on to a session using Eicon* Aviva*.

1. Double-click the SecureLogin icon on the task bar, click Applications, then click New.



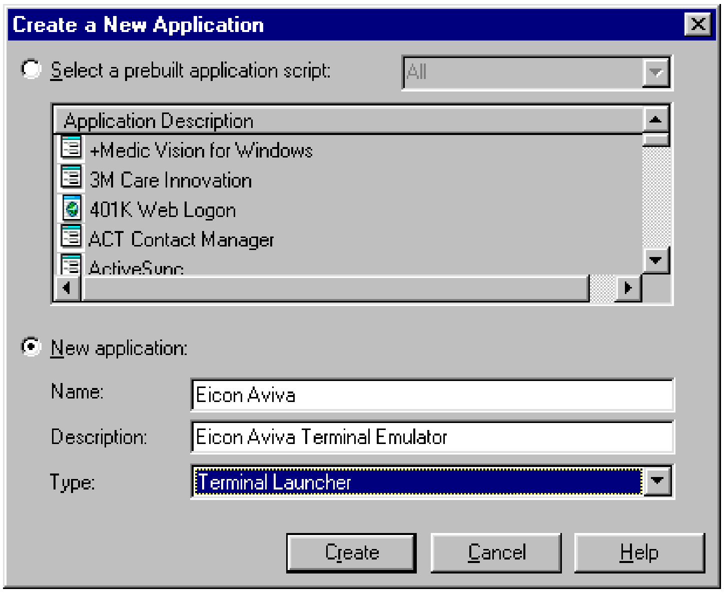
SecureLogin - Manage Logins for hdubois.akranes.T=SKIPTSJORI

Application Description	Application Name
DeskUp	deskup.exe
Novell GroupWise Client	GRPWISE.EXE
Hotmail	http://www.hotmail.exe
Quadrant Leader	QuadrantLeader.exe
Rofer app	Rofer.exe
SpinTeller.exe	SpinTeller.exe

All

☑ SecureLogin Active

2 Select New Application, type a name in the Name text box, type a description, select Terminal Launcher as the type, then click Create.



Create a New Application

○ Select a prebuilt application script: All

Application Description
+Medic Vision for Windows
3M Care Innovation
401K Web Logon
ACT Contact Manager
ActiveSync

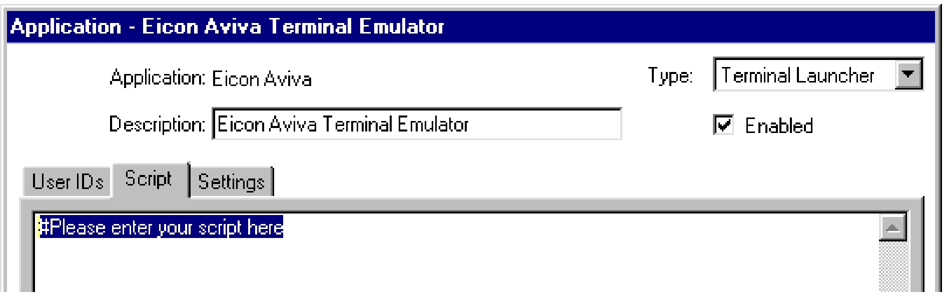
● New application:

Name: Eicon Aviva

Description: Eicon Aviva Terminal Emulator

Type: Terminal Launcher

3 Click Script.



Application: Eicon Aviva

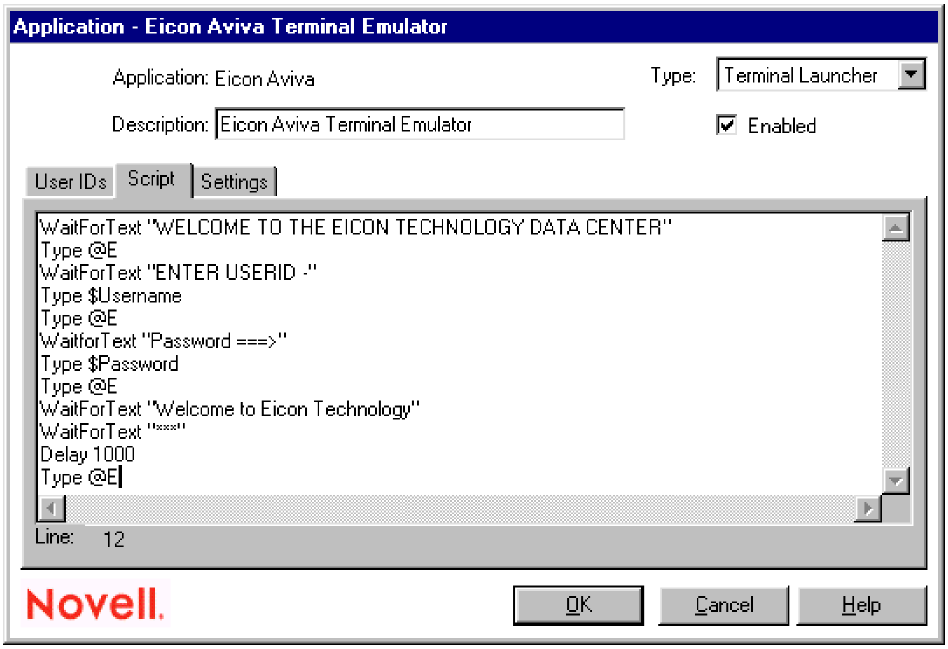
Type: Terminal Launcher

Description: Eicon Aviva Terminal Emulator

☑ Enabled

```
#Please enter your script here
```

4 Ensure that Enabled is checked, type a script, then click OK.



Application: Eicon Aviva

Type: Terminal Launcher

Description: Eicon Aviva Terminal Emulator

☑ Enabled

```
WaitForText "WELCOME TO THE EICON TECHNOLOGY DATA CENTER"
Type @E
WaitForText "ENTER USERID -"
Type $Username
Type @E
WaitforText "Password ===>"
Type $Password
Type @E
WaitForText "Welcome to Eicon Technology"
WaitForText "***"
Delay 1000
Type @E
```

Line: 12

Type screen syntax accurately in the script. Otherwise, the script won’t work. Whenever possible, copy and paste from the emulator screen into the script editor window.

To find out whether Terminal Launcher is working as expected, you might want to type only a MessageBox command.

For example, type

```
MessageBox "The emulator and Terminal Launcher are working as expected."
```

Then after confirmation, enter the complete script.

5 Save the data and close open windows by clicking OK.

Configuring the Emulator

This section provides information on the following:

- “Configuring WinHLLAPI, HLLAPI, or 16-Bit HLLAPI Emulators” on page 93
- “Configuring a DDE Emulator” on page 95
- “Configuring a VBA Emulator” on page 97
- “Configuring a Generic Emulator” on page 99

- “Configuring an Advanced Generic Emulator” on page 102

Configuring WinHLLAPI, HLLAPI, or 16-Bit HLLAPI Emulators

This section can help you configure WinHLLAPI, HLLAPI, or 16-bit HLLAPI emulators. If you select the wrong HLLAPI type, however, Terminal Launcher will fail. To find out the HLLAPI type, do one of the following:

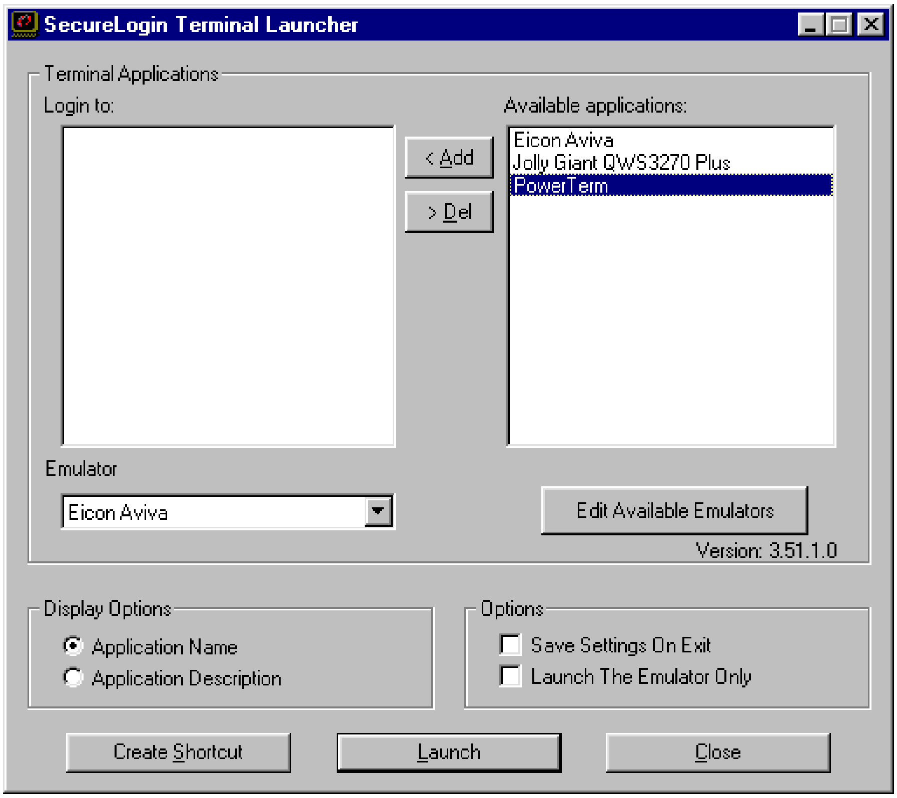
- Consult the documentation on the emulator to find out the following:
    - Whether the emulator supports HLLAPI
    - The type of HLLAPI that the emulator supports (WinHLLAPI, HLLAPI, or 16-bit HLLAPI)
- Check the .dll files by using Dependency Walker.

  NOTE: Dependency Walker won’t open 16-bit.dll files.
- Create a configuration for each of the three HLLAPI types.

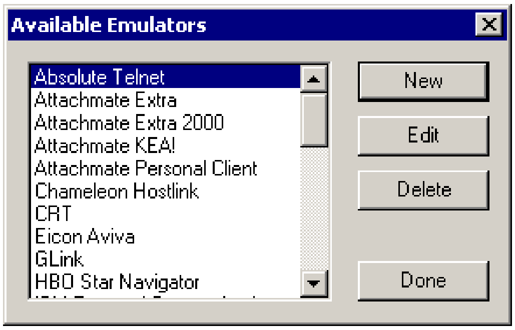
TIP: Most HLLAPI-based emulators require you to configure HLLAPI short session names (normally A-Z) and link them with the session files or the main application. Otherwise, SecureLogin won’ t be able to determine which HLLAPI session to send responses to, and it will appear that SecureLogin isn’t working. This will be the case even though everything within the SecureLogin configuration is correct.

1 Click Start > Programs > Novell SecureLogin > Terminal Launcher.

As the following figure illustrates, Terminal Launcher displays the application that you created the script for:



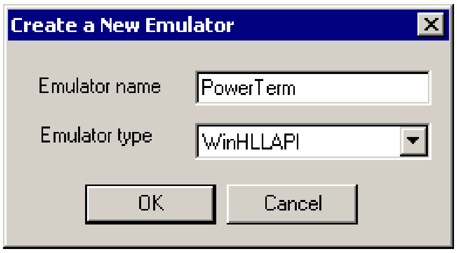
2 Click Edit Available Emulators > New.



Available Emulators

- Absolute Telnet
- Attachmate Extra
- Attachmate Extra 2000
- Attachmate KEA!
- Attachmate Personal Client
- Chameleon Hostlink
- CRT
- Eicon Aviva
- GLink
- HBO Star Navigator

3 Type a name for the emulator, select WinHLLAPI, HLLAPI, or HLLAPI16 as the emulator type, then click OK.

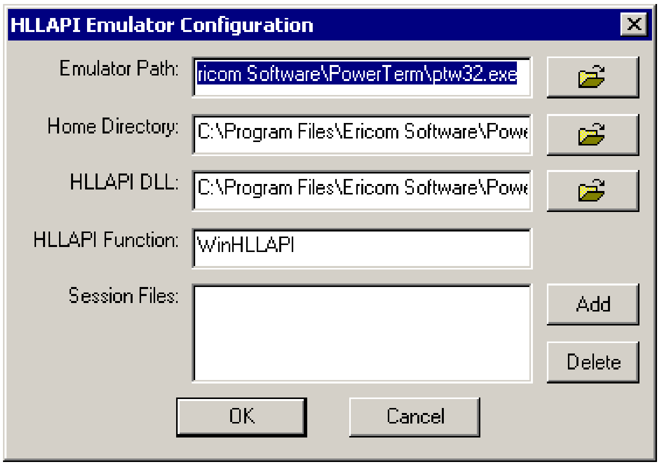


Create a New Emulator

Emulator name: PowerTerm

Emulator type: WinHLLAPI

4 Type values, then click OK.



HLLAPI Emulator Configuration

Emulator Path: ricom Software\PowerTerm\ptw32.exe

Home Directory: C:\Program Files\Ericom Software\Powe

HLLAPI DLL: C:\Program Files\Ericom Software\Powe

HLLAPI Function: WinHLLAPI

Session Files:

Field	**Description**
Emulator Path	The directory path and executable filename of the emulator. Either type the path or use the Browse button located to the right of the text box. You can type short (8.3 format) or long filenames. Enclose long filenames in quotes (for example, "c:\Program Files\emulator").
Home Directory	The directory path to files for this emulator.

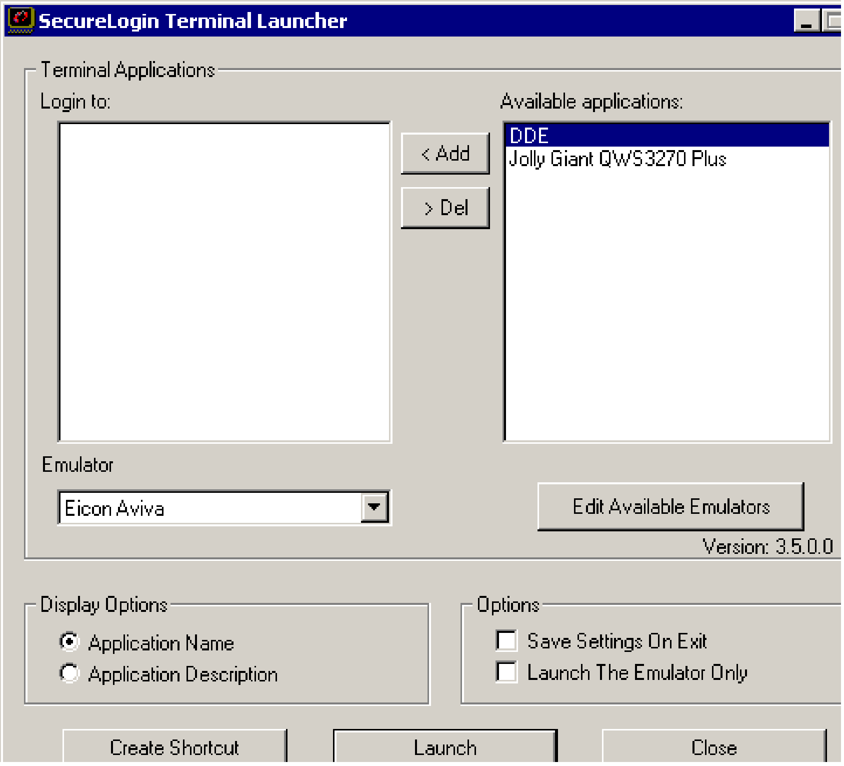
Field	Description
HLLAPI.DLL	The directory path to the .dll file for this emulator, along with the .dll filename. This file is in the Home directory. Typically, the filename contains "hllapi" in the name, but on occasion you need to refer to the documentation on the emulator. Validate the .dll file by using Dependency Walker (depends.exe), which is available from the Dependency Walker Web site (http://www.dependencywalker.com).
HLAPPI Function	The name of the HLLAPI function contained within the hllapi.dll file. Find or validate this information by using Dependency Walker. The function is case sensitive. Enter the function name exactly as you find it in Dependency Walker.
Session Files	The session files for the emulator. Type the path and session file name. Enclose long names within quotes (for example, "C:\Program Files\Sessions\Session1.xxx").

5 In the Available Emulators dialog box, click Done.

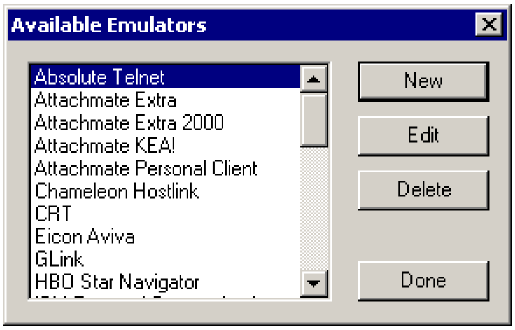
Configuring a DDE Emulator

1 Click Start > Programs > Novell SecureLogin > Terminal Launcher.

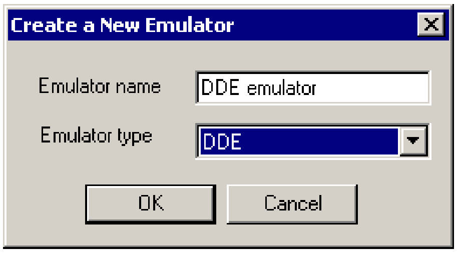
As the following figure illustrates, Terminal Launcher displays the application that you created the script for:



2 Click Edit Available Emulators > New.



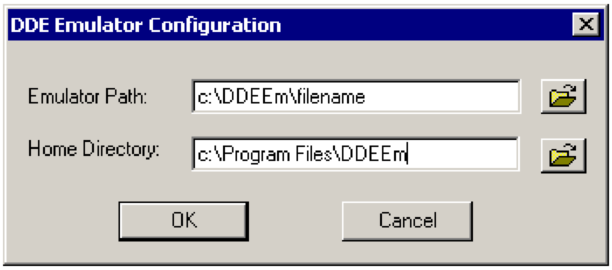
3 Type a name for the emulator, select DDE as the emulator type, then click OK.



Emulator name: DDE emulator

Emulator type: DDE

4 Type values, then click OK.



Emulator Path: c:\DDEEm\filename

Home Directory: c:\Program Files\DDEEm

Field	**Description**
Emulator Path	The directory path and executable filename of the emulator. Either type the path or use the Browse button located to the right of the text box. You can type short (8.3 format) or long filenames. Enclose long filenames in quotes (for example, "c:\Program Files\emulator").
Home Directory	The directory path to where the executable is located.

5 In the Available Emulators dialog box, click Done.

Configuring a VBA Emulator

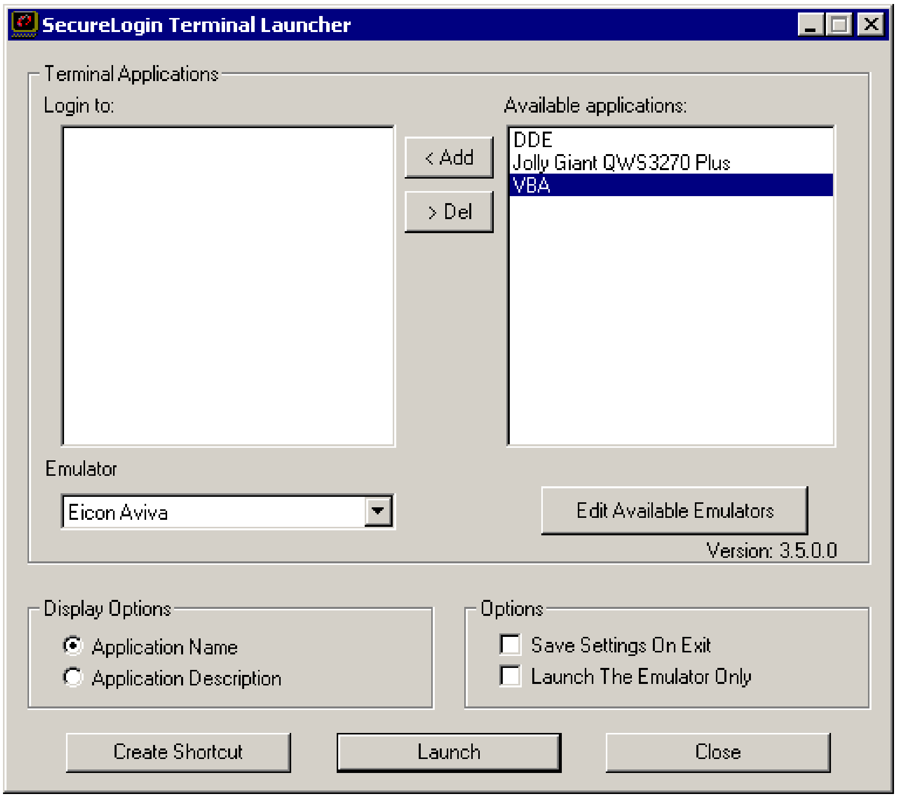
VBA emulators support the Visual Basic* scripting language. In most cases, it is possible to write a macro for the emulator. The macro prompts SecureLogin to enter credentials.

Configuring VBA emulators to work with Terminal Launcher is a specialized field and is specific to each emulator.

VBA emulators can often be configured as Generic emulators. However, generic configuration offers limited functionality.

1 Click Start > Programs > Novell SecureLogin > Terminal Launcher.

As the following figure illustrates, Terminal Launcher displays the application that you created the script for:



SecureLogin Terminal Launcher

Terminal Applications

Login to:

Available applications:

DDE
Jolly Giant QWS3270 Plus
VBA

Emulator: Eicon Aviva

Version: 3.5.0.0

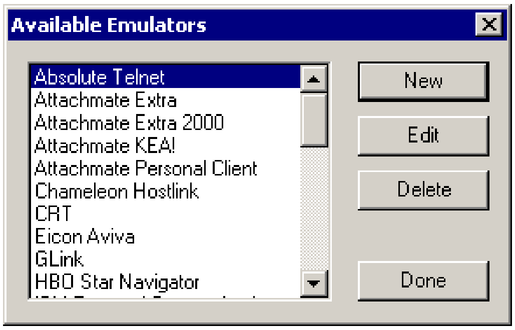
Display Options

● Application Name
○ Application Description

Options

□ Save Settings On Exit
□ Launch The Emulator Only

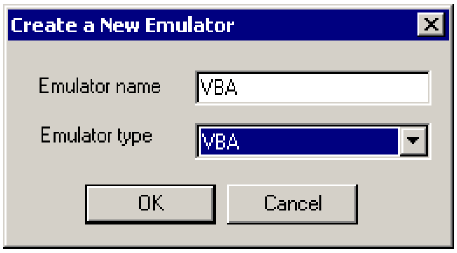
2 Click Edit Available Emulators > New.



Available Emulators

Absolute Telnet
Attachmate Extra
Attachmate Extra 2000
Attachmate KEA!
Attachmate Personal Client
Chameleon Hostlink
CRT
Eicon Aviva
GLink
HBO Star Navigator

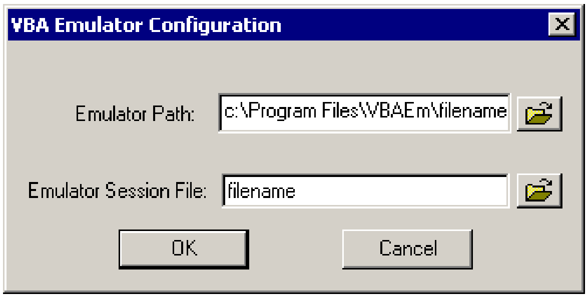
3 Type a name for the emulator, select VBA as the emulator type, then click OK


Create a New Emulator

Emulator name: VBA

Emulator type: VBA

4 Type values, then click OK.


VBA Emulator Configuration

Emulator Path: c:\Program Files\VBAEm\filename

Emulator Session File: filename

Field	Description
Emulator Path	The directory path and executable filename of the emulator. Either type the path or use the Browse button located to the right of the text box. You can type short (8.3 format) or long filenames. Enclose long filenames in quotes (for example, "c:\Program Files\emulator").
Emulator Session	The session file for the emulator. Type the path and session file name. Enclose the path and filename within quotes (for example, "C:\Program Files\Sessions\Session1.xxx").

5 In the Available Emulators dialog box, click Done.

Configuring a Generic Emulator

The Generic Emulator option enables you to configure SecureLogin's Terminal Launcher to interface with emulators that do not provide HLLAPI, VBA, or DDE support. Terminal Launcher interfaces with generic emulators though the Windows Clipboard by copying and pasting.

Because an emulator doesn't have to be programmed to allow external programs to interface with it, almost any emulator can be configured as a generic emulator.

Normal generic emulators have Select All, Copy, and Paste functions. These functions are most often found in the Edit menu, which is at the top of the emulator screen. However, buttons or keyboard shortcuts might be available.

Terminal Launcher uses these functions to interface with the emulator. Upon running a WaitForText command in a script, Terminal Launcher repeatedly simulates the selection of Select All, then Copy, which places the content of the emulator's screen on the Windows Clipboard. Terminal Launcher then searches the content of the Clipboard for the text it is waiting for.

If the text is not found, Terminal Launcher repeats the procedure, which usually takes about half a second.

Also, the emulator screen flickers while the WaitForText command is being executed. This is normal. See "BeginSplashScreen / EndSplashScreen" in the *Nsure SecureLogin 3.51.2 Scripting Guide*.

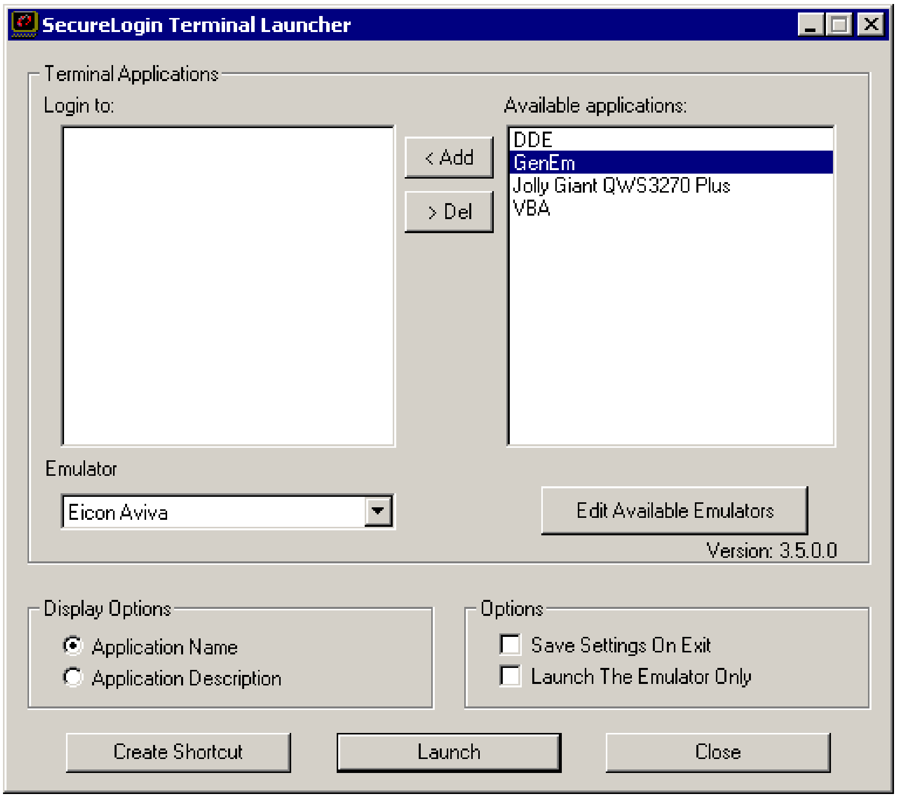
If Terminal Launcher finds the text it is looking for, Terminal Launcher goes to the next line of the script, which is most often a Type command. The Type command enters a username or password. To enter the text into the emulator, you can configure Terminal Launcher to type the text in, or to use the Clipboard.

When using the Clipboard, Terminal Launcher copies the text (for example, a username) to the Clipboard and then simulates the selection of the Paste function of the emulator. This procedure copies the text to the screen of the emulator. When using the direct typing method, Terminal Launcher simulates pressing the applicable keys on the keyboard.

The process is then repeated for the password, and the user's login to the mainframe session is complete.

1 Click Start > Programs > Novell SecureLogin > Terminal Launcher.

As the following figure illustrates, Terminal Launcher displays the application that you created the script for:



SecureLogin Terminal Launcher

Terminal Applications

Login to:

Available applications:

DDE
GenEm
Jolly Giant QWS3270 Plus
VBA

Emulator: Eicon Aviva

Version: 3.5.0.0

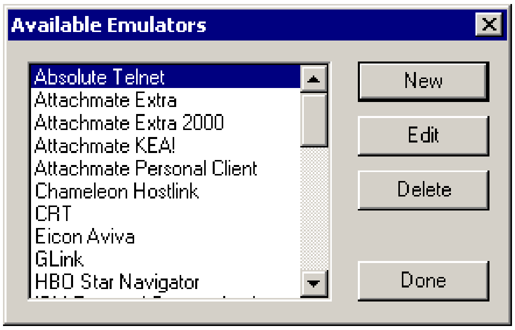
Display Options

● Application Name
○ Application Description

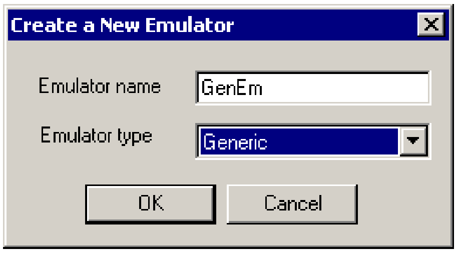
Options

□ Save Settings On Exit
□ Launch The Emulator Only

2 Click Edit Available Emulators > New.



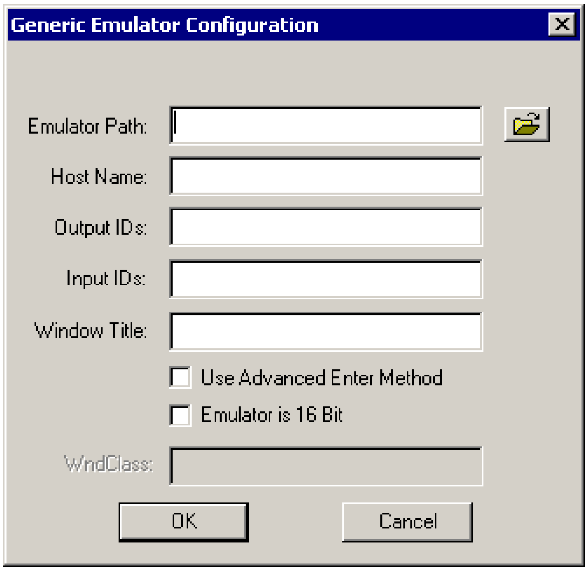
3 Type a name for the emulator, select Generic as the emulator type, then click OK.



Emulator name: GenEm

Emulator type: Generic

4 Type values, then click OK.



□ Use Advanced Enter Method

□ Emulator is 16 Bit

Field	Description
Emulator Path	The directory path and executable filename of the emulator. Either type the path or use the Browse button located to the right of the text box. You can type short (8.3 format) or long filenames. Enclose long filenames in quotes (for example, "c:\Program Files\emulator").

Field	Description
Host Name	The IP address, host name, or emulator session file you want Terminal Launcher to connect to or load. Occasionally, emulators require command line switches before they accept connection commands at startup. If so, include the switches in the Host Name text box. **Scenario for Including a Command Line Switch:** Henri is configuring a generic emulator. The emulator requires the /h switch so that the emulator can accept an IP address at startup. Henri types /h 192.168.130.222 in the Host Name text box.
Output IDs	The Control ID for the Copy function of the emulator. For information on finding Output IDs, see Appendix D, "Finding Control IDs and Offsets of an Emulator," on page 135. Some emulators allow a keyboard simulation alternative (for example, CTRL+C) instead.
Input IDs	The Control ID for the Paste function of the emulator. For information on finding Input IDs, see Appendix D, "Finding Control IDs and Offsets of an Emulator," on page 135. Some emulators allow a keyboard simulation alternative (for example, CTRL+V) instead.
Window Title	Assists Terminal Launcher in detecting the emulator window. If no Window Title is specified, Terminal Launcher might not detect the emulator opening. To find the Window Title, use Window Finder. Run Window Finder, then right-click and drag the SecureLogin icon to the title bar of the emulator. The required value will be shown as the second-from-last entry (Window Text) in Window Finder. Some emulators hide the real Window Title. There is no rule to describe which text you should enter into the Terminal Launcher configuration. (It depends on how the emulator hides it.) First, try the configuration without a Window Title specified. Next, try the text that is actually displayed in the title bar of the emulator. Finally, try the real Window Title.
Use Advanced Enter Method	Enables you to use the Advanced Enter method. This method is necessary for Lawson and StarNavigator emulators. Advanced Enter sends the \n character sequence to the emulator for the Type @E command.

5 In the Available Emulators dialog box, click Done.

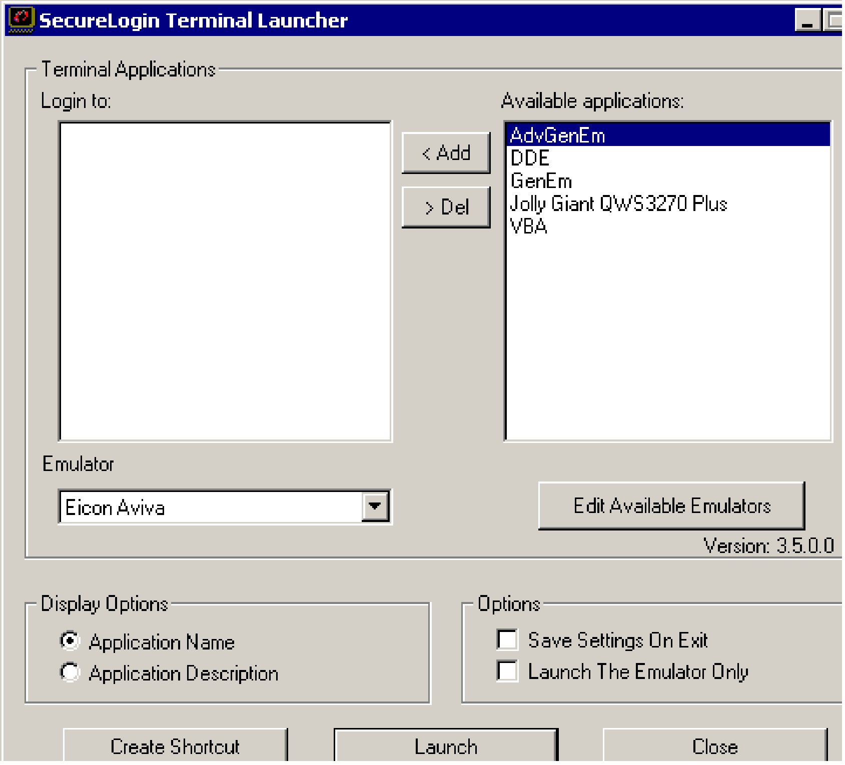
Configuring an Advanced Generic Emulator

Advanced generic emulators have Copy and Paste functions, but do not have a Select All function.

For advanced generic emulators, Terminal Launcher follows the same process as for generic emulators, except for one difference. Instead of simulating the selection of Select All, Terminal Launcher clicks and drags the mouse cursor over the emulator screen. This procedure selects all the text that the emulator is displaying.

1 Click Start > Programs > Novell SecureLogin > Terminal Launcher.

As the following figure illustrates, Terminal Launcher displays the application that you created the script for:



SecureLogin Terminal Launcher

Terminal Applications

Login to:

Available applications:
- AdvGenEm
- DDE
- GenEm
- Jolly Giant QWS3270 Plus
- VBA

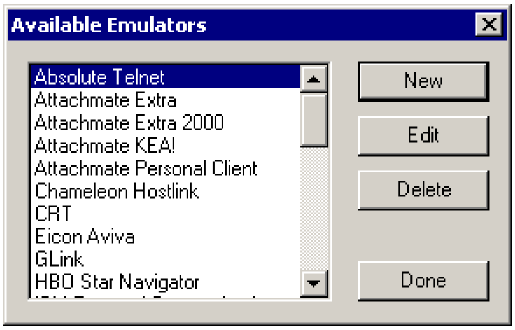
Emulator: Eicon Aviva

Version: 3.5.0.0

Display Options
- ● Application Name
- ○ Application Description

Options
- □ Save Settings On Exit
- □ Launch The Emulator Only

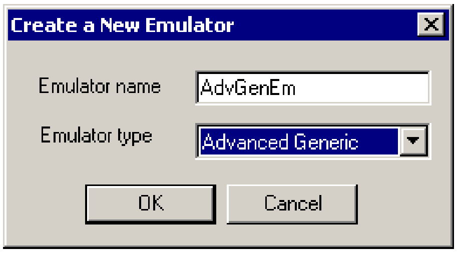
2 Click Edit Available Emulators > New.



Available Emulators

- Absolute Telnet
- Attachmate Extra
- Attachmate Extra 2000
- Attachmate KEA!
- Attachmate Personal Client
- Chameleon Hostlink
- CRT
- Eicon Aviva
- GLink
- HBO Star Navigator

3 Type a name for the emulator, select Advanced Generic as the emulator type, then click OK.

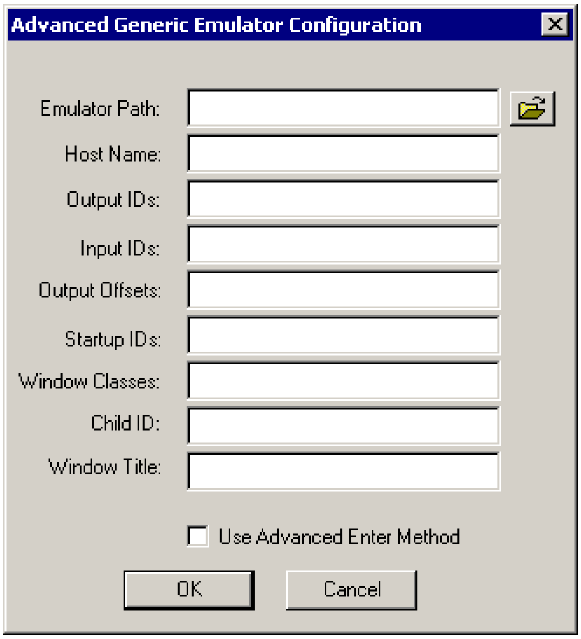


Create a New Emulator

Emulator name: AdvGenEm

Emulator type: Advanced Generic

4 Type values, then click OK.



Field	Description
Emulator Path	The directory path and executable filename of the emulator. Either type the path or use the Browse button located to the right of the text box. You can type short (8.3 format) or long filenames. Enclose long filenames in quotes (for example, "c:\Program Files\emulator").
Host Name	The IP address, host name, or emulator session file you want Terminal Launcher to connect to or load. Occasionally, emulators require command line switches before they accept connection commands at startup. If so, include the switches in the Host Name text box. **Scenario for Including a Command Line Switch:** An emulator requires the /h switch so that the emulator can accept an IP address at startup. Henri types /h 192.168.130.222 in the Host Name text box.
Output IDs	The Control ID for the Copy function of the emulator. Some emulators allow a keyboard simulation alternative (for example, CTRL+C) instead. For information on finding Output IDs, see Appendix D, “Finding Control IDs and Offsets of an Emulator,” on page 135.
Input IDs	The Control ID for the Paste function of the emulator. Some emulators allow a keyboard simulation alternative (for example, CTRL+V) instead. For information on finding Input IDs, see Appendix D, “Finding Control IDs and Offsets of an Emulator,” on page 135.

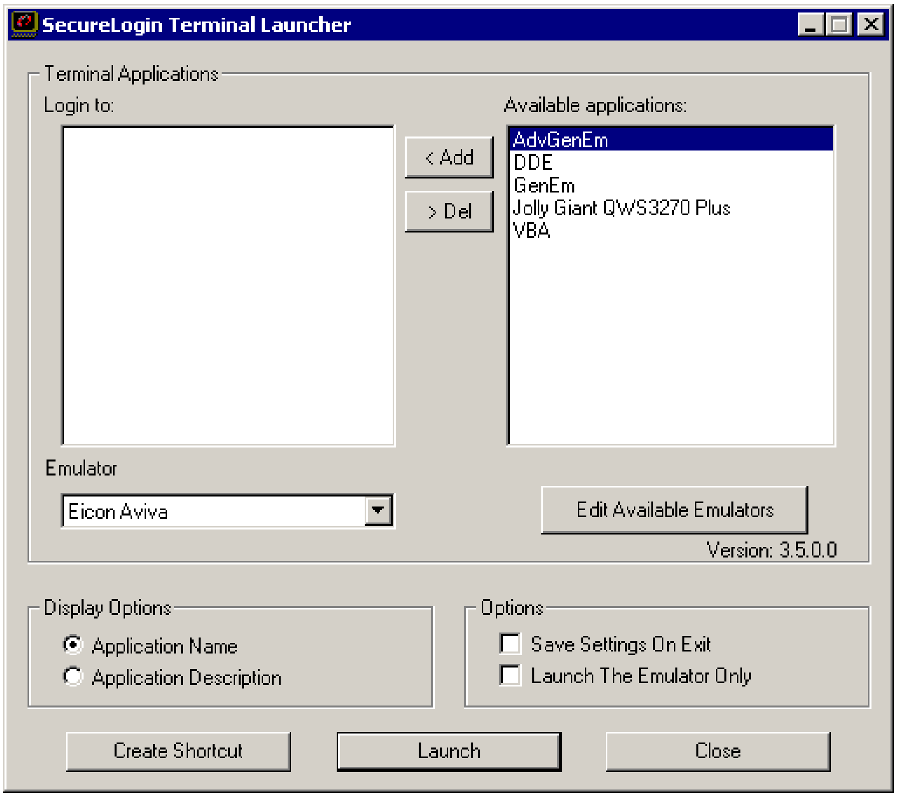
Field	Description
Output Offsets	For Terminal Launcher to select the text on the screen without a Select All function, Terminal Launcher needs to use the mouse to copy from the screen. Select all the text by clicking and dragging the cursor over the entire emulator screen. For Terminal Launcher to do this correctly, you need to specify how much space to allow for the toolbar and other bars when Terminal Launcher starts to drag. The Output Offset is the specified number, which tells Terminal Launcher where to start the click-and-drag process. The Output Offset is a set of two numbers, separated with a comma and no space. The numbers can be anything from zero up to tens of thousands. However, 10,000 is generally the highest number that is needed. To find the Output Offsets, you can use nslfindera.exe or trial and error. To use nslfindera.exe, download the utility from the Novell Support Web site (http://support.novell.com/servlet/filefinder?name=nslfindera.exe). A text file that explains how to use nslfinder is downloaded along with the utility. TID 2965468 provides the download. Also see "Finding Offsets" on page 143. To use the trial-and-error method, start with high numbers (for example: 10000,10000) and work your way down. The first number is the horizontal offset, and the second number is the vertical offset. Watch where the mouse starts to click and drag. Then lower the numbers until the mouse clicks in the top lefthand corner of the emulator screen. Normally, the Output Offset number is around 500,7000 or lower. Trial and error becomes easier with experience. **IMPORTANT:** The offsets for an Advanced Generic emulator depend on screen resolutions. Therefore, an offset for a workstation set to 800 x 600 pixels will differ from a workstation set to 1074 x 768 pixels. We recommend that you create multiple emulator definitions for each screen resolution. The actual SecureLogin script remains the same, but you deliver a unique Terminal Launcher configuration for each different screen resolution. **WARNING:** If you enter the wrong offsets, SecureLogin might select undesired locations on the workstation's desktop. These locations might close, maximize, or minimize other applications, resize the Windows task bar, or perform some other unwanted task.
Startup IDs	The Control ID numbers of any functions or buttons that you want Terminal Launcher to select before attempting to log in. An example of this is a Connect button if the emulator does not automatically connect If several functions or buttons are needed, separate them with a comma.

Field	Description
Windows Classes	Assist Terminal Launcher in detecting the emulator window. If no Window Class is specified, Terminal Launcher might not detect the emulator opening. To find the Window Class, use Window Finder. Run Window Finder, then right-click and drag the SecureLogin icon to the title bar of the emulator. The required value is shown as the third-from-last entry (Class Name) in Window Finder.
Child ID	A Child ID is given to each child window that the main application launches. Only enter a Child ID into the TLaunch configuration if it is necessary to interact with a child window.
Window Title	Assists Terminal Launcher in detecting the emulator window. If no Window Title is specified, Terminal Launcher might not detect the emulator opening. To find the Window Title, use Window Finder. Run Window Finder, then right-click and drag the SecureLogin icon to the title bar of the emulator. The required value will be shown as the second-from-last entry (Window Text) in Window Finder. Some emulators hide the real Window Title. There is no rule to describe which text you should enter into the Terminal Launcher configuration. (It depends on how the emulator hides it.) First, try the configuration without a Window Title specified. Next, try the text that is actually displayed in the title bar of the emulator. Finally, try the real Window Title.
Use Advanced Enter Method	Enables you to use the Advanced Enter method. This method is necessary for Lawson and StarNavigator emulators. Advanced Enter sends the \n character sequence to the emulator for the Type @E command.

5 In the Available Emulators dialog box, click Done.

Creating a Login for an Emulator

1 From the list in the Available Applications pane, click the application that you want to log in to, then click Add.



Login to:

Available applications:
AdvGenEm
DDE
GenEm
Jolly Giant QWS3270 Plus
VBA

Emulator: Eicon Aviva

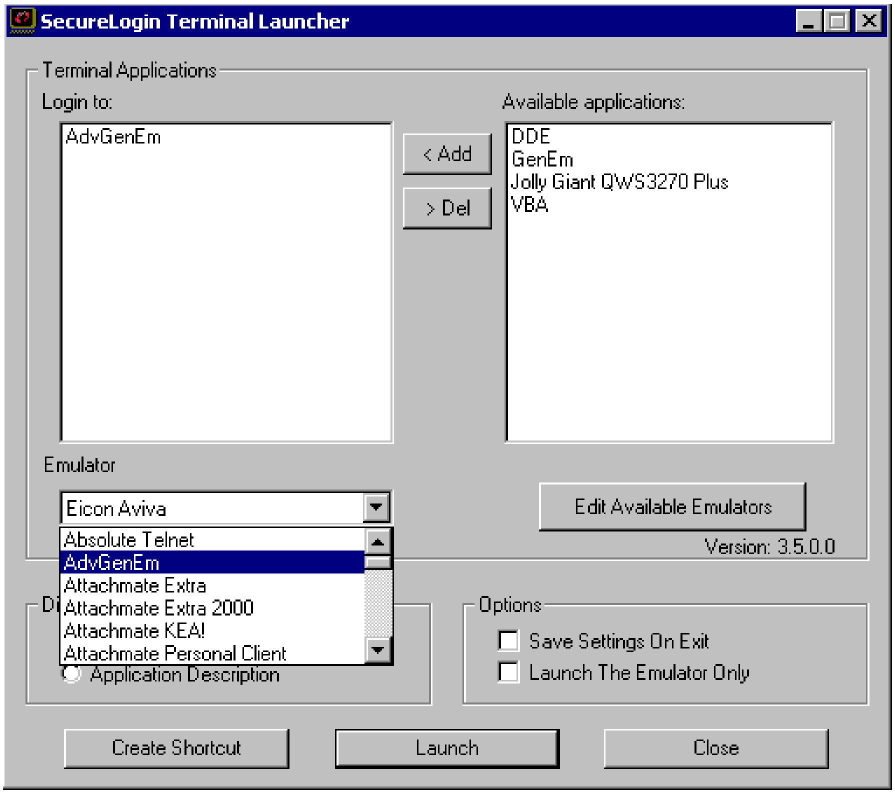
Version: 3.5.0.0

● Application Name
○ Application Description

□ Save Settings On Exit
□ Launch The Emulator Only

To move an entry from one side to the other, you can double-click it.

2 Select the emulator from the Emulator drop-down list, then click Launch.



Login to:
AdvGenEm

Available applications:
DDE
GenEm
Jolly Giant QWS3270 Plus
VBA

Emulator: Eicon Aviva
Absolute Telnet
AdvGenEm
Attachmate Extra
Attachmate Extra 2000
Attachmate KEA!
Attachmate Personal Client

Version: 3.5.0.0

○ Application Description

□ Save Settings On Exit
□ Launch The Emulator Only

The selected application script runs, using the selected emulator.

The first time the script is run, you encounter a prompt to enter your username and password. Enter the required values, then click OK. Terminal Launcher launches the emulator, enters your username and password, and logs you in to a session.

Setting Up a Shortcut

Terminal Launcher needs to start before the terminal emulator application for single sign-on starts. Therefore, you create a shortcut that has a command to first launch Terminal Launcher and then launch the emulator application. You can deploy the shortcut to user's desktops.

The following example shows how to create a terminal launcher desktop shortcut called Simple Login. This shortcut launches and logs the user into a Jolly Giant QWS3270 Plus session.

1. Record the exact name given to the terminal emulator in Terminal Launcher.
2. Right-click the desktop, then click New > Shortcut.
3. Enter (or browse to) the path for tlaunch.exe.

   For example, enter "c:\Program Files\novell\securelogin\tlaunch.exe". Include quotation marks.
4. To the end of this line, add "/auto/p[*application_name*]/e[*emulator_name*]".

   For example, type

   ```
   "/auto/pSimple Login/eJolly Giant"
   ```

   For information on the command line switches, see "Command Line Parameters Used in Terminal Launcher" on page 109.

   The shortcut box contains this shortcut line:

   ```
   "C:\Program Files\Novell\Securelogin\Tlaunch.exe" "/auto/pSimple Login/eJolly Giant"
   ```
5. Click Next, name the new application shortcut, then click Finish.

   When you double-click the shortcut, the shortcut launches Jolly Giant and runs the selected script.

Command Line Parameters Used in Terminal Launcher

Terminal Launcher can use the following command line parameters.

Parameter	Description
/auto	Indicates to Terminal Launcher that a following parameter will request execution of an application that is enabled for single sign-on. This parameter must be in the command line for the other command line options to work.
/b	Specifies background authentication mode.
/e*emulator_name*	Launches the specified emulator. You must enter the emulator name exactly as it is listed in the Emulator drop-down list.
/h*hllapi_short_name*	Forces Terminal Launcher to connect to the specified HLLAPI session.

Parameter	Description
/k*executable_name*	Kills the specified executable before launching an emulator.
/L	Instructs Terminal Launcher to not launch the emulator. Terminal Launcher doesn't launch the emulator but tries to run the script, assuming that the emulator has already been launched.
/m	Enables multiple (concurrent) connections to particular sessions. This parameter is required for background authentication.
/n	Launches the selected emulator without running a script. This is equivalent to checking the Launch the Emulator Only check box in the main Terminal Launcher window. This parameter doesn't function with VBA emulators.
/n*number_1-15*	Launches the specified number of sessions without running scripts. This parameter doesn't function with VBA emulators.
/p*application_name*	Runs the specified application. Type the application script name exactly as it is listed in Terminal Launcher's Available Emulators drop-down list. To run several applications scripts from a shortcut at once, add /p*another application name* for each extra application. SecureLogin Terminal Launcher can launch up to 15 application scripts at one time, provided there are enough sessions defined for the emulator named in the shortcut dialog box.
/q	Specifies Quiet Mode (no cancel dialog).
/s	Suppresses errors.
/t	Enables unlimited timeout when connecting to an emulator.
/w*process name*	Waits until the specified process name is running before running the script.
/x*parameters*	Sets HLLAPI session parameters before doing the HLLAPI connect. Not for general use.

The following examples include parameters that Terminal Launcher uses:

- `Tlaunch.exe /auto`

  Creates a shortcut that launches the SecureLogin Terminal Launcher.

- `Tlaunch.exe /auto /eEicon Aviva /pApplication1 /pApplication2`

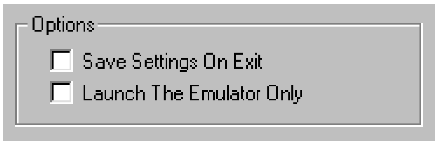
  Launches two SecureLogin Terminal Launcher application scripts. The scripts launch two sessions of Eicon Aviva, one named Application1, the other named Application2.

- `Tlaunch.exe /auto /pTSO`

  Launches the SecureLogin Terminal Launcher application script named TSO.

- `Tlaunch.exe /auto /n3`

Launches the SecureLogin Terminal Launcher and opens three sessions. The three sessions are whichever emulator was last used with the Launch the Emulator Only option selected and then closed with the Save Settings on Exit option selected.



Options

□ Save Settings On Exit

□ Launch The Emulator Only

Configuring Backup Sessions

Each terminal emulator that is configured must have a number of backup sessions configured for it. For most emulators, you are required to have one session file for every session that you want to have running at the same time. These are usually stored as separate files.

When you configure an HLLAPI, DDE, or VBA emulator for use with Terminal Launcher, you must input a session file for it to use.

NOTE: Inputting a session file doesn't apply to Generic or Advanced Generic emulators.

To configure Terminal Launcher to use more than one session file:

1. Launch Terminal Launcher, then click Edit Available Emulators.
2. Select the required emulator from the Available Emulators window, then click Edit.
3. Add the backup session files to the Session Files dialog box.

   Terminal Launcher can launch only as many emulator sessions as there are session files defined.

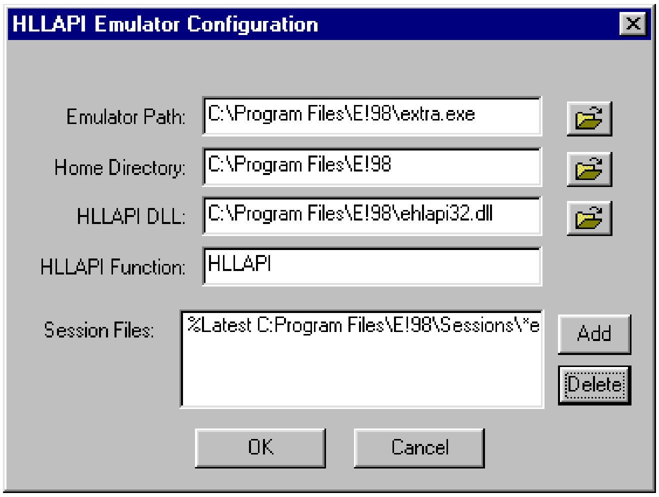
   NOTE: After the emulator is launched, these session files are executed as a command line parameter. Some emulators (such as QWS3270 Plus) do not have session files. Instead, these emulators have individual sessions stored in the registry. Think of these session files as command line parameters that are passed to the executable.

Determining Which Session File To Automatically Use

A session file tells the emulator how to connect to the mainframe. In some environments, and with emulators like Attachmate Extra, users on the network might have given their session file a unique name. This means that Terminal Launcher might need to be configured individually for each user.

Terminal Launcher includes an option that allows it to determine the last-used session file and start that mainframe configuration. This option reduces or eliminates the need to manually configure each user's environment when unique session filenames are used.

To configure Terminal Launcher to use the last-used configuration file, use the command %Latest in the Session Files section of Terminal Launcher. The following figure illustrates this option:



Emulator Path: C:\Program Files\E!98\extra.exe

Home Directory: C:\Program Files\E!98

HLLAPI DLL: C:\Program Files\E!98\ehlapi32.dll

HLLAPI Function: HLLAPI

Session Files: %Latest C:Program Files\E!98\Sessions\*e

This example entry causes Terminal Launcher to search the E!98\Sessions directory, looking for the .EDP file with the newest date and time. Terminal Launcher then launches that file with the emulator and connects to the mainframe.

If the file mainframe.edp had the most recent date and time in the Sessions directory, the command line would look like the following:

```
C:\Program Files\E!98\extra.exe c:\Program Files\E!98\Sessions\mainframe.edp
```

Using Terminal Launcher With Non-HLLAPI-Compliant Emulators

You can use Terminal Launcher with Terminal Emulators that do not support HLLAPI but do support scripting that is able to call external .dll files. To do this, you must create a script that asks SecureLogin for commands one at a time and then interprets the commands received.

Configuring Reflection 8 for UNIX and Digital

The following script has been tested with Reflection 8 for UNIX and Digital.

```
Sub SecureLogin()
 Dim SecureLoginObject As ISLBroker
 Dim ReturnCode As Long
 Dim Data As String
 Dim targ As Long
 Dim FunctType As Long
 Dim CR As String
 Dim temp As String

 Session.Wait 0.1’The waits are necessary for the screen to be updated.

 Set SecureLoginObject = New SLBroker
 CR = Chr$(rcCR) ' Chr$(rcCR) = Chr$(13) = Control-M
 SecureLoginObject.LoadScript
 While (1 = 1)
  FunctType = 0
  'retrieve command from VBABork
  SecureLoginObject.GetCommand FunctType, targ, Data
  If FunctType = SecureLoginObject.SetCursor Then
  ' SetCursor is not supported
    ReturnCode = 0
  ElseIf FunctType = SecureLoginObject.TypeText Then
```

```
    If (StrComp(Data, "@E", vbTextCompare) = 0) Then
      Session.Transmit CR
    Else
      Session.Transmit Data
    End If
    Session.Wait 0.1
    ReturnCode = 0
  ElseIf FunctType = SecureLoginObject.ScanForText Then
    bResult = Session.FindText(Data, Session.ScreenTopRow, 0)
    ReturnCode = 0
    If bResult = True Then
      ReturnCode = 1
    End If
  Else
    ' End of script
    GoTo ErrorHandler
  End If
  SecureLoginObject.SetReturnCode ReturnCode
 Wend
ErrorHandler:
End Sub
```

The script should also work for Reflection 7. Reflection 6 and earlier versions require a different Reflection script because these versions use Reflection Basic instead of VBA (Visual Basic for Applications). If you require a script for Reflection 5.21, contact Novell Support (http://support.novell.com).

To use Reflection for UNIX and Digital, you must add the Sub SecureLogin() script by using the macro editor in Reflection. In addition to adding this macro, you must go to the macro editor, select Tools > References, and check the check box titled vbabork2 1.0 Type Library.

If this option is not displayed, ensure that vbabork2.dll exists in the SecureLogin directory. If it does not, re-install SecureLogin, making sure to select Terminal Launcher.

If the vbabork2 1.0 Type Library option displays, you must register it.

1. Open a DOS shell.
2. Enter **regsvr32** followed by the path to vbabork2.dll.

   For example, enter

   ```
   regsvr32 "C:\Program Files\SecureLogin\ vbabork2.dll"
   ```

   A message should indicate that DllRegisterServer succeeded.
3. Add the reference to this module in Reflection as described above.

Only one session can be launched at a time using SecureLogin. To run the script, you must run the SecureLogin script macro after the session has been opened. This can be done automatically in Reflection by selecting Connect Macro from the Connection Setup menu.

By doing this procedure, the SecureLogin script macro will run every time the session is opened. Without this procedure, you will need to manually run the script macro when you want to run the script.

To run the script, you must set up the emulator in Terminal Launcher.

1. Launch Terminal Launcher, then click Edit Available Emulators. Set up the emulators as usual, but set the HLLAPI type to None.
2. Select the emulator.

3 Type anything in the hllapi dll and HLLAPI Function boxes.

4 Click OK, then click Done.

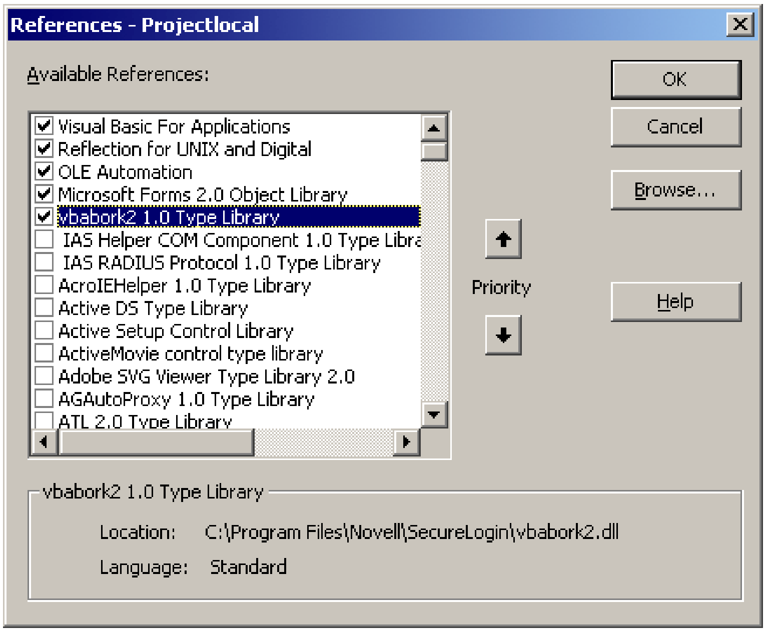
Configuring Reflection 9 for UNIX and Digital

1 Open Reflection for UNIX and Digital.

2 Click Macro at the top of the screen, then select Visual Basic Editor.

3 After the editor loads, click Tools at the top of the screen, then click References.

4 Scroll to vbabord2 1.0 Type Library, then check the check box.



Available References:

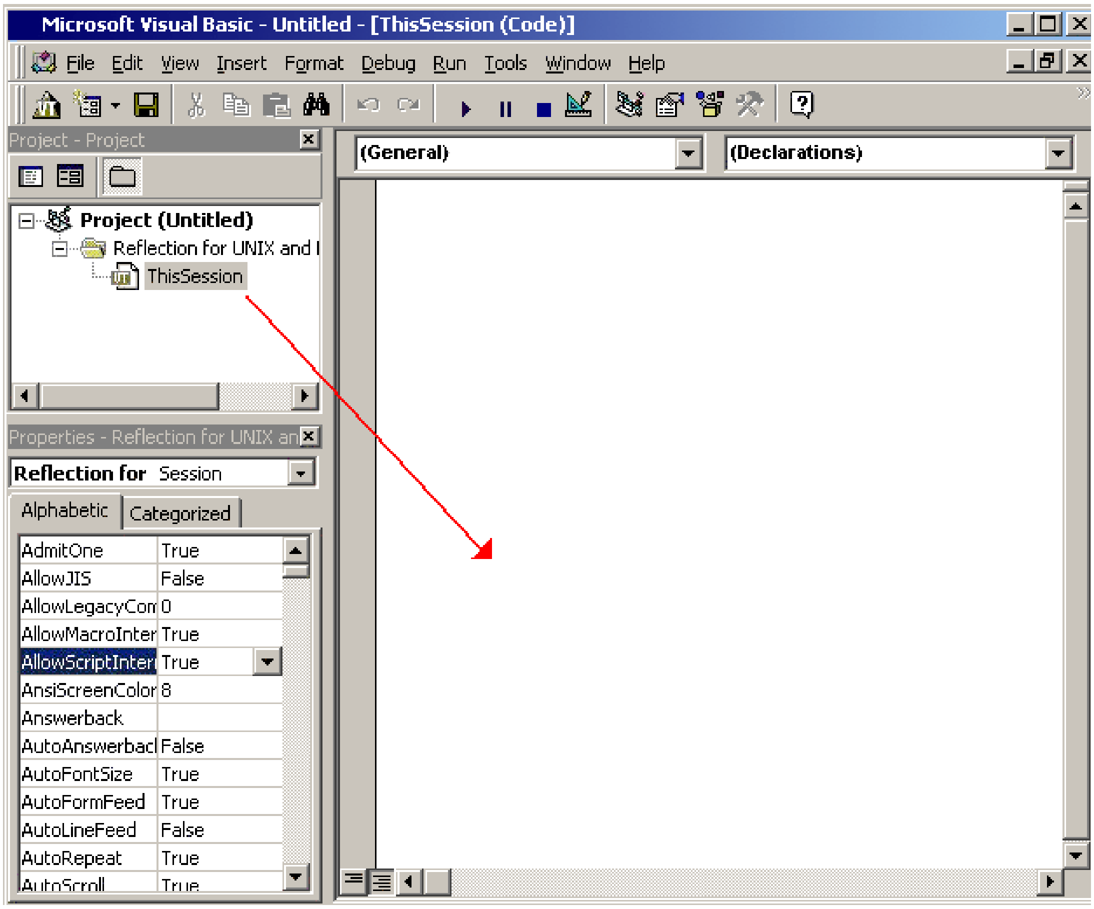
- ☑ Visual Basic For Applications
- ☑ Reflection for UNIX and Digital
- ☑ OLE Automation
- ☑ Microsoft Forms 2.0 Object Library
- ☑ vbabork2 1.0 Type Library
- □ IAS Helper COM Component 1.0 Type Libra
- □ IAS RADIUS Protocol 1.0 Type Library
- □ AcroIEHelper 1.0 Type Library
- □ Active DS Type Library
- □ Active Setup Control Library
- □ ActiveMovie control type library
- □ Adobe SVG Viewer Type Library 2.0
- □ AGAutoProxy 1.0 Type Library
- □ ATL 2.0 Type Library

vbabork2 1.0 Type Library

Location: C:\Program Files\Novell\SecureLogin\vbabork2.dll

Language: Standard

5 Return to the main editor screen, then double-click This Session, which is on the far left of the screen.



Microsoft Visual Basic - Untitled - [ThisSession (Code)]
File Edit View Insert Format Debug Run Tools Window Help
Project - Project
Project (Untitled)
Reflection for UNIX and I
ThisSession
Properties - Reflection for UNIX an
Reflection for Session
Alphabetic
Categorized
(General)
(Declarations)

AdmitOne	True
AllowJIS	False
AllowLegacyCon	0
AllowMacroInter	True
AllowScriptInter	True
AnsiScreenColor	8
Answerback	
AutoAnswerbacl	False
AutoFontSize	True
AutoFormFeed	True
AutoLineFeed	False
AutoRepeat	True
AutoScroll	True

6 Copy and paste the macro into the editor.

You can type text in the right pane of the screen. Type or copy and paste the following macro:

```
Sub SecureLogin()
  Dim SecureLoginObject As ISLBroker
  Dim ReturnCode As Long
  Dim Data As String
  Dim targ As Long
  Dim FunctType As Long
  Dim CR As String
  Dim temp As String

  Session.Wait 0.1 'The waits are necessary for the screen
  to be updated.

  Set SecureLoginObject = New SLBroker
  CR = Chr$(rcCR) ' Chr$(rcCR) = Chr$(13) = Control-M
  SecureLoginObject.LoadScript
  While (1 = 1)
    FunctType = 0
    'retrieve command from VBABork
    SecureLoginObject.GetCommand FunctType, targ, Data
    If FunctType = SecureLoginObject.SetCursor Then
    ' SetCursor is not supported
      ReturnCode = 0
    ElseIf FunctType = SecureLoginObject.TypeText Then
      If (StrComp(Data, "@E", vbTextCompare) = 0) Then
        Session.Transmit CR
      Else
        Session.Transmit Data
      End If
      Session.Wait 0.1
      ReturnCode = 0
    ElseIf FunctType = SecureLoginObject.ScanForText Then
     bResult = Session.FindText(Data,
     Session.ScreenTopRow, 0)
     ReturnCode = 0
     If bResult = True Then
       ReturnCode = 1
     End If
    Else
      ' End of script
      GoTo ErrorHandler
    End If
    Session.Wait 0.1
    SecureLoginObject.SetReturnCode ReturnCode
  Wend
ErrorHandler:
End Sub
```

7 Click File > Close, then click Exit to exit from the editor.

8 Click Open Connection at the top of the screen, then click Connection Setup.

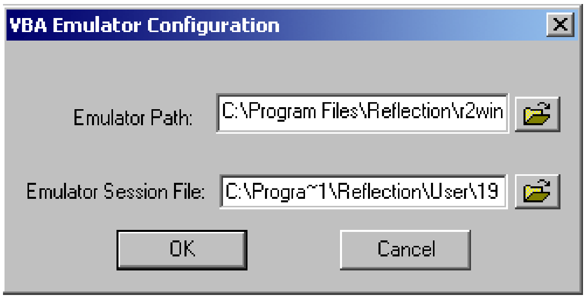
This is where you set up the host name and protocol that you are connecting to the mainframe.

9 Click Connect Macro and browse to the macro you just created.

10 Open Tlaunch.exe, then click Edit Available Emulators > New.

This step creates a new emulator.

11 Select a VBA emulator type, then type the required settings.



VBA Emulator Configuration

Emulator Path: C:\Program Files\Reflection\r2win

Emulator Session File: C:\Progra~1\Reflection\User\19

12 Create a script for the emulator to use.

5 Troubleshooting SecureLogin

This section contains information on the following:

For information on error codes, see Appendix F, "Error Codes," on page 151.

Interoperability Issues

Novell ®SecureLogin, Novell SecretStore®, Novell iChain®, and Novell Portal Services can share secrets when the formats for the secrets are the same. If you have a secret in iChain that you want to leverage with SecureLogin, the naming conventions must be the same. Because SecureLogin makes the naming convention, use this convention in other services.

1. Install SecureLogin.
2. Set up a Web application in SecureLogin.
3. Using SecretStore Manager, view the secret.

   See "Viewing a Secret" in the *Novell SecretStore 3.3.3 Administration Guide* (http://www.novell.com/documentation/secretstore33/index.html).
4. In the other service (for example, iChain), create the same type, with the same name.

SecureLogin and iChain

The authentication page in iChain has a Destination field. The SecureLogin client saves this field as an Optional parameter. This is the URL being requested. iChain is accelerating or securing the URL.

If iChain is also accelerating other Web pages or sites, the original Destination that SecureLogin saved when the user first saved the credentials will always be the URL that the user finally receives, regardless of the Web page or site that the user requested.

If the user needs to authenticate to iChain to get to the Web page, SecureLogin replaces the Destination where the user wants to go with the Destination that SecureLogin first saved.

Scenario: Changing the Destination Field. Markus Kurz wants to go to the Web server's index page. He enters the URL http://www.mkurz.com. SecureLogin saves this URL. The next time that

Markus wants to go to GW WebAccess (www.mkurz.com/servlet/webacc), SecureLogin changes the Destination to http://www.mkkurz.com. Markus has to do a manual operation to get to GWWebAccess.

To fix the problem, Markus uncomments the Type $Optional line from the script. SecureLogin then ignores the Destination field.

First-Time Login to DEX 4.1 Portal Services

When a user first logs in to DEX 4.1 Portal Services, SecureLogin prompts the user to save the credentials. After the credentials are saved, and the user logs out or accesses the login page again, SecureLogin does the following:

- Passes the credentials to the Web page.
- Displays the following error message:

```
It looks as though you may have put an incorrect password into this page.
Do you want to halt execution of this script?
```

SecureLogin copied the Username and Password values from the page and added them to its configuration. SecureLogin created a script that has the following lines:

```
Type $Username
Type $Password.
#Click #1
# If this script does not submit the data correctly, try uncommenting the
Click #1.
# If this script puts the username or password in the incorrect fields, try
counting the fields on
# the page and adding the correct number to the Type commands (for example,
Type $Username #2.)
```

To resolve the issue, uncomment the line that begins "#Click #1."

Integrating with BorderManager’s Java Applet for Proxy Authentication

1. Make sure that the SUN Java Runtime Environment is installed on the workstation and that Java has been enabled in SecureLogin.

   See “Enabling a Java Application” in the *Nsure SecureLogin 3.51.2 User Guide*.

2. Configure the BorderManager proxy to use a Java applet for authentication
3. Configure the browser to use the proxy.
4. Launch the browser, attempt to connect to a site that requires authentication, then click Yes.

   SecureLogin should detect the login to a Web site and prompt you to create a script.

5. On SecureLogin’s main dialog box, click Applications, select the BorderManager applications, then click Edit.
6. Click Script.

   The script for BorderManager should display the following lines:

```
# control: 1 name:  *null (class java.awt.TextField)
# control: 2 name:  *null (class java.awt.TextField)
# control: 3 name:  *null (class java.awt.TextField)
# control: 4 name:  * Ok (class java.awt.Button)
# control: 5 name:  *Cancel (class java.awt.Button)
# control: 6 name:  *null (class BMLFrame)
```

7 Add the following lines to the end of the script:

```
Dialog
Type $Username #1
Type $Password #2
Click #4
EndDialog
```

The revised script should display as follows:

```
# control: 1  name: *null (class java.awt.TextField)
# control: 2  name: *null (class java.awt.TextField)
# control: 3  name: *null (class java.awt.TextField)
# control: 4  name: * Ok (class java.awt.Button)
# control: 5  name: *Cancel (class java.awt.Button)
# control: 6  name: *null (class BMLFrame)
Dialog
  Type $Username #1
  Type $Password #2
  Click #4
EndDialog
```

8 Save the script and exit.

9 Close and restart the browser, then again attempt to connect to a site that requires proxy authentication.

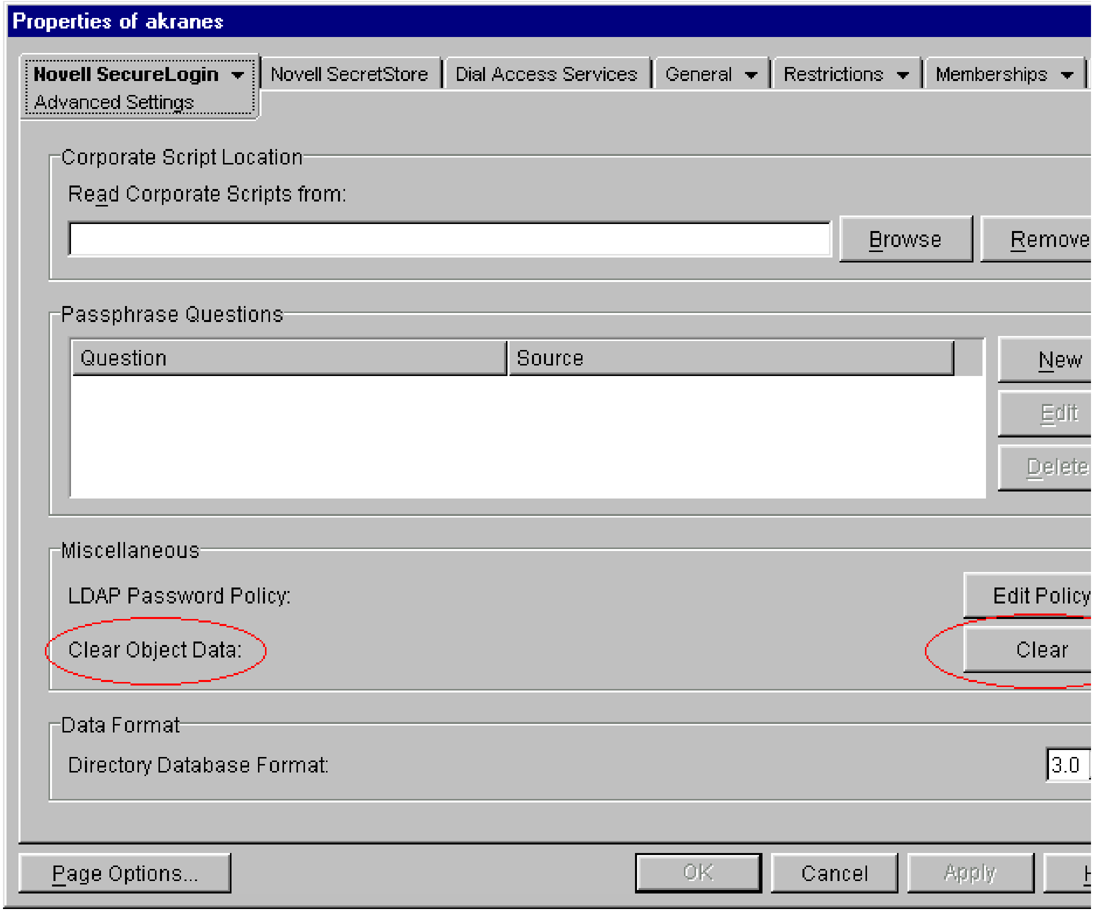
Don’t move the mouse while SecureLogin is completing the applet form. SecureLogin moves the mouse to the OK button, then clicks it. If you move the mouse, SecureLogin might not be able to click OK.

SecureLogin should now take you to the requested Web site.

Clearing Object Data

Object data is stored in the directory and in a local cache on the workstation. You can clear object data in the directory or in the local cache on the workstation.

Clearing Object Data in the Directory



Directory Database Format: 3.0

The Clear Object Data option can delete all manually configured User object data, Container object data, or OU object data in the directory, including:

- User IDs, including stored usernames and passwords
- Scripts (application connectors)
- Password policies
- Manually configured settings
- Passphrases

Any inherited data remains available to the object, as does the data in a workstation's local cache. Therefore, if the user reboots the workstation or resyncs between the workstation and the directory, the data stored in the cache on the workstation repopulates the data store in the directory.

If the SecureLogin directory attribute needs to be refreshed, you can quickly clear the data stored in the directory or SecretStore and let the data resync with the local cache files.

WARNING: Typically, don't use Clear Object Data at the container or OU level. All SecureLogin settings and applications enabled for single sign-on are deleted at that level.

To remove the attribute, use the SecureLogin snap-in to ConsoleOne®:

IMPORTANT: Before deleting the object data, ensure that all related user ID or credential information is recorded. For example, ask users to log their usernames and passwords to applications that will lose single sign-on functionality.

1. Right-click an object, then select Novell SecureLogin > Advanced Settings.
2. Locate the Clear Object Data label.
3. Click Clear.

   To completely remove or clear object data, also clear data on the workstation.

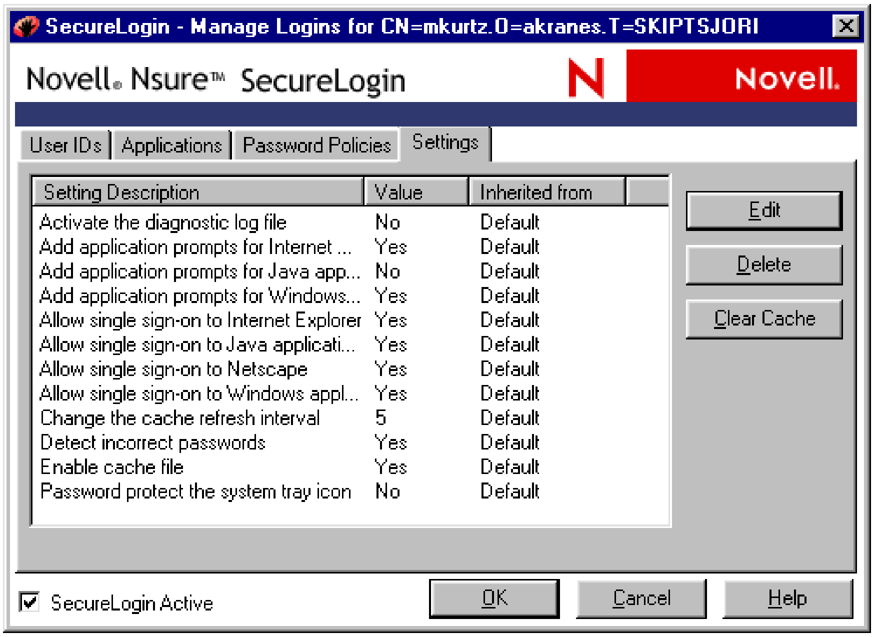
In SecureLogin 2.5, each user had a separate cache directory on the workstation. You could clear all object data from a specific user by clearing object data within the directory and then also deleting the cache files located on the workstation.

However, SecureLogin 3.51.2 assigns all cache files to the user that is currently logged in to the workstation. Users don't have separate directories. If users share accounts on a workstation, deleting one file can remove all of the cached credentials for all users.

Clearing Data on the Workstation

If a user's SecureLogin data needs to be refreshed on the workstation, you can quickly clear the data stored there and let the data resync with the directory's data store.

1. Select Manage Logins, then click Settings.


SecureLogin - Manage Logins for CN=mkurtz.O=akranes.T=SKIPTSJORI
Novell. Nsure™ SecureLogin
Novell.
User IDs
Applications
Password Policies
Settings
Edit
Delete
Clear Cache
OK
Cancel
Help

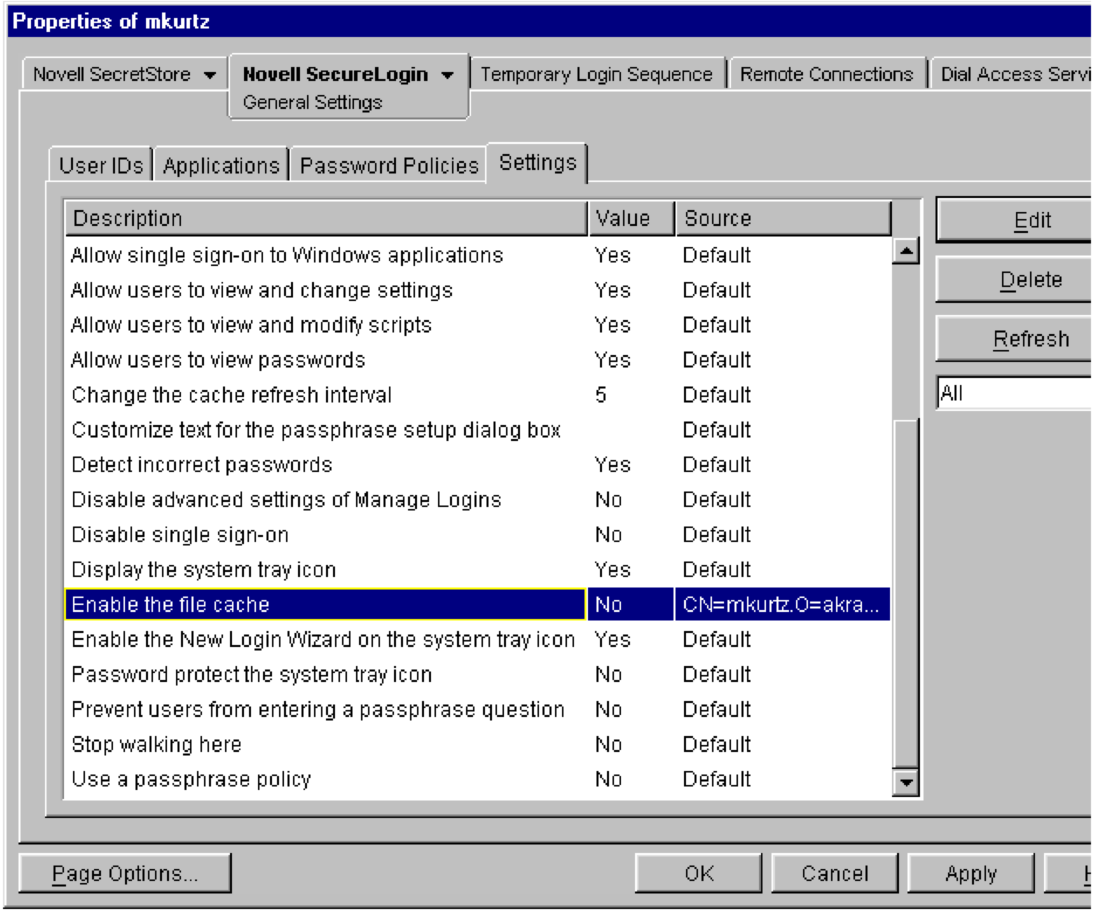
Setting Description	Value	Inherited from
Activate the diagnostic log file	No	Default
Add application prompts for Internet ...	Yes	Default
Add application prompts for Java app...	No	Default
Add application prompts for Windows...	Yes	Default
Allow single sign-on to Internet Explorer	Yes	Default
Allow single sign-on to Java applicati...	Yes	Default
Allow single sign-on to Netscape	Yes	Default
Allow single sign-on to Windows appl...	Yes	Default
Change the cache refresh interval	5	Default
Detect incorrect passwords	Yes	Default
Enable cache file	Yes	Default
Password protect the system tray icon	No	Default

☑ SecureLogin Active

2. Click Clear Cache, click Yes, then click OK.

You can force SecureLogin to delete a user's data on the local workstation:

1. Clear object data in the directory.
2. Using a management tool, select the User object, then click Properties.
3. Select Novell SecureLogin > General Settings > Settings.
4. Select Enable the File Cache, set the value to No, then click Apply.



Description	Value	Source
Allow single sign-on to Windows applications	Yes	Default
Allow users to view and change settings	Yes	Default
Allow users to view and modify scripts	Yes	Default
Allow users to view passwords	Yes	Default
Change the cache refresh interval	5	Default
Customize text for the passphrase setup dialog box		Default
Detect incorrect passwords	Yes	Default
Disable advanced settings of Manage Logins	No	Default
Disable single sign-on	No	Default
Display the system tray icon	Yes	Default
Enable the file cache	No	CN=mkurtz.O=akra...
Enable the New Login Wizard on the system tray icon	Yes	Default
Password protect the system tray icon	No	Default
Prevent users from entering a passphrase question	No	Default
Stop walking here	No	Default
Use a passphrase policy	No	Default

When the user logs in, data in the local cache on the workstation is removed.

Rights in Active Directory

Adsschema.exe extends the Active Directory schema and typically grants necessary rights. If rights haven’t been granted, you can manually assign rights to User objects or to an Organizational Unit object.

Assigning Rights to User Objects

To use SecureLogin, a user must have Read and Write rights to the protocom-SSO-Auth-Data, protocom-SSO-Entries, protocom-SSO-Entries-Checksum, protocom-SSO-Profile, protocom-SSO-Security-Prefs, and protocom-SSO-Security-Prefs-Checksum attributes on his or her User object. These rights enable users to add configuration data (for example, a passphrase) and create logins. To verify that these attributes are in the extended schema, see “Verifying the eDirectory Schema” in the *Nsure SecureLogin 3.51.2 Installation Guide*.

Default rights are set when SecureLogin is installed and the schema is extended for the first time.

If you don't assign rights to SELF, users are unable to read or write SecureLogin attributes.

To assign rights for Active Directory:

1 Bring up the MMC snap-in.

1a Click Console > Open.

1b Select the profile name that you previously saved, then click Open.

2 Click Active Directory Users and Computers > the domain name (for example, inet.nsrd.lab.vmp.com) > Users.

3 Right-click a container, select Delegate Control, then click Next.

For example, you can select the Users container. Active Directory automatically creates this predefined container. On the other hand, you can select a container that you have created (for example, RDlab).

IMPORTANT: This step is necessary for every container that you want rights to apply to.

If Container objects (for example, OU objects) contain users in subcontainers, you must set up the same rights as the ones assigned to Active Directory's built-in Users container. If branches exist in your Active Directory tree, ensure proper rights by assigning rights for each branch or by assigning rights globally at the Root.

4 Click Add > SELF.

5 Click Add > OK.

6 (Conditional) Click Create a Custom Task to Delegate > Next.

If you selected the predefined Users container, skip this step.

7 In the Active Directory Object Type window, click Only the Following Objects in the Folder, check the User Objects check box, then click Next.

8 Set permissions on new schema attributes.

8a Under Show These Permissions, check the General and Property- Specific check boxes.

8b In the Permissions list box, check the Read and Write check boxes for the protocom-SSO-Auth-Data, protocom-SSO-Entries, protocom-SSO-Entries-Checksum, protocom-SSO-Profile, protocom-SSO-Security-Prefs, and protocom-SSO-Security-Prefs-Checksum attributes.

Assigning User Rights to an Organizational Unit

Users need rights to corporate objects (for example, corporate scripts and serverPolicyOverride objects). Users can then inherit and use objects that you set up specifically for target users.

Typically, adsschema.exe assigns necessary rights when you assign user rights by container.

To manually accomplish this, set Read and Write permissions for the protocom-SSO-Entries attribute. You need to specify what containers to add rights to.

1 Bring up the MMC snap-in.

1a Click Console > Open.

1b Click the profile name that you previously saved, then click Open.

2 Click Active Directory Users and Computers, select the domain name (for example, inet.nsrd.lab.vmp.com), then click Users.

3 Right-click the container that you want to apply rights to, click Delegate Control, then click Next.

For example, you can select the Users container. Active Directory automatically creates this predefined container. On the other hand, you can select a container that you have created (for example, RDlab).

If Container objects (for example, OU objects) contain users in subcontainers, you must set up the same rights as the ones assigned to Active Directory's built-in Users container.

If branches exist in your Active Directory tree, ensure proper rights by assigning rights for each branch or by assigning rights globally at the Root.

4. (Conditional) Click Create a Custom Task to Delegate, then click Next.

   If you selected the predefined Users container, skip this step.

5. In the Active Directory Object Type window, click This Folder, Existing Objects in This Folder, and Creation of New Objects in This Folder, then click Next.
6. Set rights (permissions) on new schema attributes.
   - Under Show These Permissions, check the General and Property-Specific check boxes, click Next, then click Finish.
   - In the Permissions list box, check the Read and Write check boxes for the protocom-SSO-Entries attribute.
7. Click Next, then click Finish.

Frequently Asked Questions

Changing the Startup Order

How can I change the startup order of applications? I placed an application in the Startup folder, but SecureLogin doesn't recognize it.

Answer: Most likely, a password-protected application is starting before SecureLogin is initialized and able to process login requests. Try one of the options in Appendix B, "Changing the Startup Order of Applications," on page 131.

Entering a Passphrase

What's a passphrase? After I set up SecureLogin, a dialog box instructs me to enter my passphrase. However, the entry fields don't let me know which box is the passphrase box.

Answer: SecureLogin has two passphrase components: the passphrase question and the passphrase answer. If someone changes your password and tries to log in as you, that person must correctly answer the passphrase answer to the passphrase question that displays at relogin.

If you encounter the passphrase question, just answer it. An additional dialog box will instruct you to enter your Directory password, so that you can log in.

No User ID

Why doesn't a user ID appear when I'm prompted for a passphrase question?

Answer: The schema probably hasn't been extended for your store. Extend the schema for your Directory or environment.

No Passphrase Policies on Windows NT Domains

I created a passphrase policy on my Windows NT domain, but the clients don't seem to see it. Why?

Answer: Because of limitations in the domain system, passphrase policies aren't supported in Windows NT Domains.

Can't Log In Again to a Web Site

After changing a SecureLogin password to match a Web site password, why can't I log in to the Web site?

Answer: Internet Explorer's AutoComplete function can cause this problem. Disable AutoComplete.

Scenario. While in disconnected mode, Sandy successfully enters a SecureLogin username and password for a Web site. Using a script at the Web site, Sandy changes the password and then edits the SecureLogin entry, so that the SecureLogin password matches the Web site. The single sign-on login for the Web site now fails.

Sandy disables Internet Explorer's AutoComplete function and is able to log in.

Scripts for Web Sites

What's the best way to log in to Web sites?

Answer: Because SecureLogin recognizes a login panel on a Web page, the easiest method to create scripts for Web sites is to use the pop-up wizard. The second option is to run the wizard manually.

Why is SecureLogin unable to log me in to some Web sites?

Answer: You might need to change a registry entry value.

1. Open the registry and browse to HKEY_LOCAL_MACHINE\Software\Protocom\SecureLogin \Logging.
2. Set the "IESSO" DWORD value to 0.

   This setting logs any messages received from a SecureLogin script running in conjunction with Internet Explorer. The log file gets saved as C:\SSODebug.txt. Information in the log file can help in troubleshooting login scripts for Web sites that are difficult to log in to.

Task Bar Icon Stays Active

Why does the SecureLogin icon remain active? I used the User Preferences page to turn off the SecureLogin icon on the task bar. Then I refreshed the data.

Answer: This setting is only read at startup. After you restart your workstation, the task bar won't display the icon.

Novell SecureLogin Is Missing from the Program Group

When I click Start > Programs, Novell SecureLogin no longer appears in the Program group. How can I get it back?

Answer: Run the Repair option in Setup.exe.

No Attribute Mapping Tab

Why can't I locate the attribute mapping tab on the property page for the LDAP Group object? I'm trying to map protocom-SSO-Entries to the existing Prot:SSO entry.

Answer: You probably haven't installed the LDAP snap-in to ConsoleOne. Download the snap-in from the Novell Product Downloads (http://download.novell.com/pages/PublicSearch.jsp) Web page.

1. In the Search for a Product Download section, click Category.
2. From the Choose a Category drop-down list, select ConsoleOne Snap-ins.
3. From the Choose a Platform drop-down list, select NetWare.
4. Click Submit Search.
5. Under the eDirectory section, click Download for the 8.7 Snap-in for ConsoleOne.

   TIP: To select Download, you might have to scroll to the right side of the screen. If you click 8.7 Snap-in for ConsoleOne, the Web site displays information about downloading but doesn't actually download the product.

Terminal Launcher Doesn't Run

Why do I get an error message when TLaunch launches an emulator?

Answer: You probably typed the function name incorrectly in the HLLAPI Function text box while configuring Terminal Launcher.

Typical error messages for this scenario indicate that TLaunch was unable to do the following:

- Connect to the presentation space.
- Load the .dll file.
- Find the entry point.

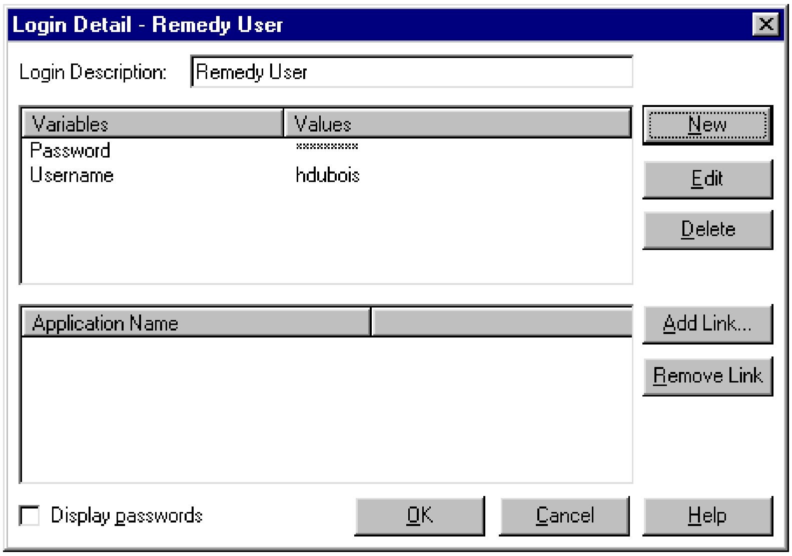
Use Dependency Walker to find the HLLAPI function export name, then enter it exactly.

Can't View Shadow Variables

What can't I view shadow variables?

Answer: You are probably running SecureLogin in a mixed SecureLogin 3.51.2 and SecureLogin 3.0.*x* environment. When you run SecureLogin in a mixed environment, you lose some SecureLogin 3.51.2 functionality.

Shadow variables are User-object variables that you can view from the server. When viewing the User object from the server, you can go into the user application details and view and manipulate the variables that the user has for the application.



Login Detail - Remedy User

Login Description: Remedy User

Variables	Values
Password	**********
Username	hdubois

Application Name	

□ Display passwords

Shadow variables are used for SecretStore so that you can see that variables like username or password exist. You can read the value of non-protected variables, for example Username.

Shadow variables act as a transfer station for data between the administrator and the user's SecretStore.

By using management utilities such as ConsoleOne and MMC, you can change the values of shadow variables. For example, you can reset a password to an application so that a user can log in. You can't view the actual value of password fields, but you can reset the values.

Error Codes for LDAP

Where can I find information about error codes for LDAP?

Answer: Get information from LDAP Server Return Codes (http://developer.novell.com/ndk/doc/ldapover/index.html?page=/ndk/doc/ldapover/ldap_enu/data/a3wyu4m.html), in the Novell Developer Kit (NDK).

1. Navigate to LDAP and NDS® Integration, select LDAP and NDS, then select LDAP Server Return Codes.
2. Expand LDAP Server Return Codes, then select an option from the following:
   - LDAP Client Return Codes
   - LDAP Server Return Codes
   - LDAP Result Code Structure

Resolving Error -426

What causes error -426?

Answer: The sysuser and syspassword values are empty. Either slinac.dll or slnmas.dll (the Novell NMAS client) was unable to get your credentials during the login.

When you log in with a biometric device to a Novell network, the NMAS client on the workstation won't be able to get your eDirectory credentials and store them in the sysuser and syspassword variables. The software works as designed when you use any NMAS method other than NDS.

To resolve this issue, don't use the sysuser and syspassword variables. Instead, user $Username and $Password.

If you encounter this issue with a Citrix* or Terminal Server installation, verify that you registered the slinas.dll while you were in install mode. Otherwise, the new slinas.dll will only be registered for the current user instead of being registered system-wide.

Resolving Error -602

How do I fix error -602?

Answer: Error -602 is "No Such Value". This is an NDS error code. Search on this error number at Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

TIP: Don't include the - (hyphen) when you type 602 into the Knowledgebase search box.

Resolving Error -672

Why did I receive error -672? When I logged in for the first time, I entered a passphrase and answer, but I couldn't save the data to the directory.

Answer: -672 is an NDS error: Access Denied. Most likely, Novell SecureLogin tried to write the passphrase information to the prot: * attributes but the user didn't have sufficient rights. As administrator, you need to run the rights assignment part of schema.exe, which is typically located in the c:\Program Files\novell\securelogin directory.

Resolving Error -1644

Why do I get error -1644 during installation?

Answer: You are probably installing on a Windows 2000 workstation. To install the SecureLogin client there, you must have Power User or Administrator privileges to the workstation.

Error Parsing Line

How do I resolve "Error parsing line"?

Answer: Put a Messagebox command between lines of the script.

If a script breaks down, SecureLogin typically displays "Error parsing line" to inform you that the script isn't working. However, occasionally the script breaks down even though there is no error parsing a line. By putting the Messagebox command between lines of the script, you can see exactly where the script stops functioning.

The following sample illustrates using the Messagebox command.

```
Type $Username
Messagebox "This is the first message box after username"
Type $Password
Messagebox "after password"
Click #1
Messagebox "after click#1"
Click #2
Message box "after click#2"
```

If the message box with the text “This is the first message box after username” appears, you know that the first line of the script executed successfully. To allow the script to continue to the next line, click OK on the message box.

For more information, see “MessageBox” in the *Nsure SecureLogin 3.51.2 Scripting Guide*.

Program Conflict

What causes the Program Conflict message? During installation, I checked Start SecureLogin Now. However, I get this message: “Unable to load all entry points from access library (ssman.dll). Please check that it is in the path and the correct version.”

Answer: If the Program Conflict message appears during installation, make sure that previous Novell Single Sign-on software components have been uninstalled or otherwise removed from the system.

Also, delete the following entries (if they exist) from the registry:

- HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Single Sign-on
- HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix

Support for Swing/AWT Standard Applications

SecureLogin 3.51.2 supports Swing/AWT Standard Applications. Java support requires the Sun Java JRE 1.4.2.

To get this file:

1. Go to http://java.sun.com.
2. Select Java 2 Platform, Standard Edition (J2SE), then click the J2SE 1.4.2 link.
3. Scroll to the Download J2SE v 1.4.2 section.
4. Select the link under the JRE column for your platform.

SecureLogin Displays LDAP Login Dialog Box after Workstation Unlock

After unlocking the workstation, SecureLogin displays the LDAP Login dialog box if all of the following occur:

- SecureLogin is installed in eDirectory mode with LDAP as the protocol
- NMAS component is selected during SecureLogin installation.
- NSL LDAP is installed as GINA

When the unlock occurs, SecureLogin cannot determine who actually unlocked the workstation. During the next refresh cache event, SecureLogin prompts to reauthenticate to ensure that the same user has unlocked the workstation.

SecureLogin refresh cache event occurs whenever any of the following happens:

- The user right-clicks the SecureLogin status bar (system tray) icon and selects Advanced, Refresh Cache
- The user double-clicks the SecureLogin status bar icon
- The user relaunches slproto.exe (path: Start > Programs > Novell SecureLogin)
- The refresh cache is exceeded

If the user clicks Cancel, SecureLogin attempts to switch to Offline mode. If the user is configured to not allow an Offline cache, it results in the message `You are not logged into a directory and SecureLogin was unable to find any cached user data and` SecureLogin closes down.

If the user has Offline cache enabled, then SecureLogin continues to operate in Offline mode until the workstation is rebooted or the user correctly logs in to SecureLogin.

It is recommended that the user enters login credentials instead of cancelling the login dialog box.

Useful TIDs

Issue	TID
Clearing the user ID but not the password	10082125 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10082125.htm)
Resetting a user's passphrase	10086375 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10086375.htm)
Logging in to GroupWise and GroupWise Verify at the same time	10085765 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10085765.htm)
Getting logged back into a Web site after logging out.	10087276 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10087276.htm)
How to configure SecureLogin to capture debug logs	10088017 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10088017.htm)

Unsupported Tools

There are certain additional, unsupported tools included on the SecureLogin 3.51.2 CD. Although Novell does not support these tools, they might assist users in troubleshooting and configuring SecureLogin.

Copy the unsupported tools from the following path:

SecureLogin_cd\SecureLogin\Tools\Unsupported

For further details, refer to the documentation provided in the Unsupported directory (along with each tool).

A Prebuilt Scripts

SecureLogin provides prebuilt login scripts for the following applications:

Application	Application	Application
401K Web Logon	iFolder® (JavaSSO)	PeopleSoft*
ActiveSync*	iFolder (Win)	Qualcomm* Eudora*
America Online*	iPlanet*	QuickBooks* Pro
BorderManager®	Lotus* Notes* (Win script)	Remedy* AR User
CNN* eMail Services	MSN Messenger	SAP* R/3
Citrix Management Console	Microsoft:* SQL	SecureRemote
eBay*	Monster.com	Tivoli* Helpdesk
Entrust*	myNovell	Trillian
Goldmine*	myRealBox℠	Visual SourceSafe*
GroupWise® Client	MYOB Client	VNC
GroupWise Notify	Nomad	Win95 /98 DialUp
Hotmail*	Oracle* Financials	Yahoo* Mail
Internet Explorer	OutLook*	Yahoo Messenger
I.E Proxy Authentication	pcANYWHERE	

B Changing the Startup Order of Applications

If a password-protected application starts before SecureLogin is initialized, SecureLogin is unable to process the login request for that application. To solve this problem, change the startup order of the applications. Use one of the following options, according to how your application has been configured to auto-start:

- "Using the Startup Group" on page 131
- "Using Startup Scripts" on page 131
- "Using DetectExisting.exe" on page 131
- "Using Novell Application Launcher to Start Applications" on page 132

Using the Startup Group

You can move the start commands for password-protected applications from HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run to the \Windows\Start Menu\Programs\Startup group.

However, this option has a drawback. Applications in the startup group can start in any order, and they do not need to finish loading before any other application starts running. Therefore, applications in the users' startup group occasionally start before SecureLogin.

Using Startup Scripts

Startup scripts are scripts that are executed during SecureLogin's startup. You can move application start commands from the Registry Run or the Startup group to a SecureLogin startup script.

Use the SecureLogin script Run command to start the application.

Be sure to include the full path of the application in the Startup script. For example:

```
Run "c"\winnt\email.exe"
```

Using DetectExisting.exe

IMPORTANT: DetectExisting.exe is not supported by Novell. Nevertheless, this along with some other tools are provided in the Unsupported directory of the SecureLogin product CD to assist users in troubleshooting and configuring SecureLogin.

The DetectExisting.exe detects applications that are already running (before SecureLogin is loaded). This utility detects all running applications and informs SecureLogin of their presence. Virtually, SecureLogin starts functioning as if the applications started running after SecureLogin.

DetectExisting.exe detects only the Windows applications. Also it supports the following platforms:

- Windows 95
- Windows 98
- Windows NT
- Windows 2000
- Woindows XP
- Windows 2003
- Advanced Server
- Terminal Server
- Citrix Metaframe
- Citrix Presentation Server

To use DetectExisting.exe:

1 Copy DetectExisting.exe from the SecureLogin 3.51.2 CD to your workstation.

   This file is available in the following directory:

   SecureLogin_cd\SecureLogin\Tools\Unsupported

2 Use the startup script to run the utility as in the following example, ensuring that you specify the full path.

```
Run c:\programfiles\NSL\SecureLogin\Utilities\DetectExisting.exe
```

   Adding the utility to a startup script ensures that it runs only when SecureLogin is active.

Using Novell Application Launcher to Start Applications

Use the Icon Order and Wait on Force Run options in Novell Application Launcher™. These options enable you to use Application Launcher to do the following:

- Launch Novell SecureLogin
- Launch (with a lower order) the other applications that you want to single sign-on to at startup

One possible drawback with this option is that some users might not want to start an application that Application Launcher launches.

C MS Terminal Server and Citrix MetaFrame Environments

SecureLogin supports Microsoft Terminal Server and Citrix Corporation MetaFrame* remote application environments. When you use SecureLogin with a remote desktop, no special configuration is required in either environment. However, when you plan for single sign-on you need to consider where the application is being run from.

To enable applications that are run from the server to use single sign-on functionality, install SecureLogin on the Terminal or MetaFrame server. See "Installing SecureLogin for Citrix" in the *Nsure SecureLogin 3.51.2 Terminal Services Guide*.

Terminal Server and MetaFrame send only keystrokes and screen images to the workstation. This process means that SecureLogin installed on the local computer is unable to determine which applications are running remotely. When SecureLogin is installed on Terminal Server, SecureLogin can see the applications' Windows and Terminal information natively and thus perform single sign-on.

SecureLogin includes a terminal services module for whenever single sign-on through the initial Citrix or Terminal Server GINA is required. This module automates the initial login to the terminal server GINA by providing the user's details from the local machine. See the Nsure SecureLogin 3.51.2 Terminal Services Guide.

D Finding Control IDs and Offsets of an Emulator

This section provides information on the following:

- "Finding Input and Output IDs" on page 135
- "Finding Offsets" on page 143

Finding Input and Output IDs

Every option (for example, File and Edit) in an emulator's menu has a unique Control ID number. Terminal Launcher uses these IDs to simulate the selection of options.

Terminal Launcher uses

- The IDs of the Select All and Copy functions as the Output IDs
- The ID of the Paste function as the Input ID

To find these numbers, use Winspector, available at the Gipsysoft Web site (http://www.gipsysoft.com/articles/winspector/), or Spy++, available from Microsoft's developer Web site.

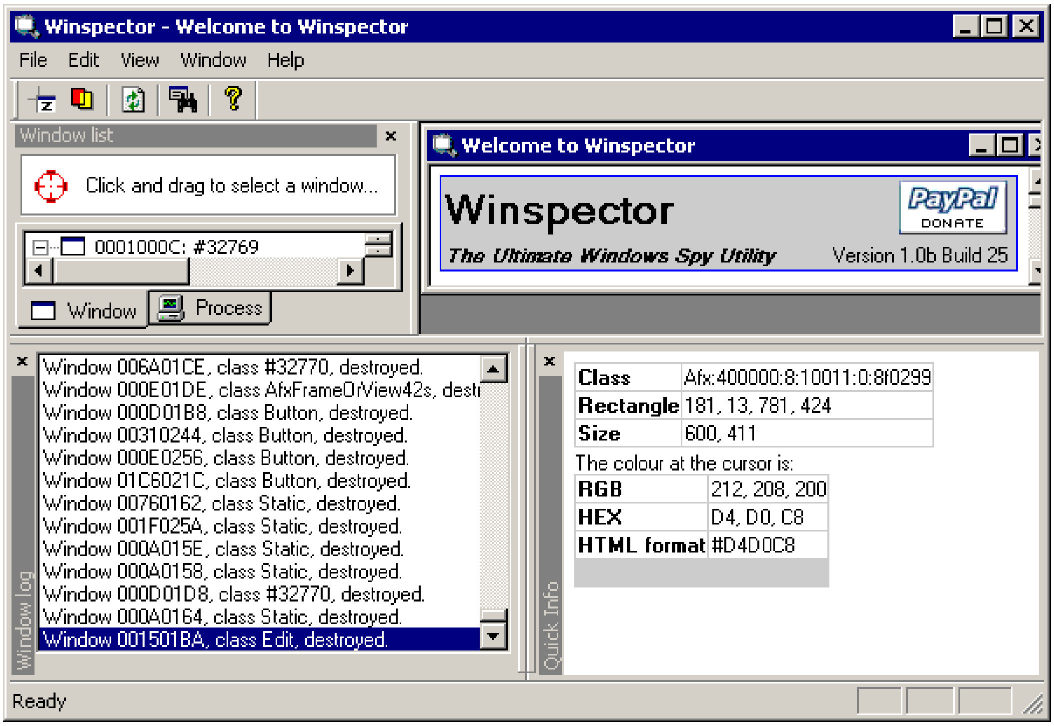
This section explains how to use Winspector.

Setting Up Winspector

1 Run the emulator. Don't close it.

   In this example, the emulator is Quick32.

2 Run Winspector.



```
Window 006A01CE, class #32770, destroyed.
Window 000E01DE, class AfxFrameOrView42s, destr
Window 000D01B8, class Button, destroyed.
Window 00310244, class Button, destroyed.
Window 000E0256, class Button, destroyed.
Window 01C6021C, class Button, destroyed.
Window 00760162, class Static, destroyed.
Window 001F025A, class Static, destroyed.
Window 000A015E, class Static, destroyed.
Window 000A0158, class Static, destroyed.
Window 000D01D8, class #32770, destroyed.
Window 000A0164, class Static, destroyed.
Window 001501BA, class Edit, destroyed.
```

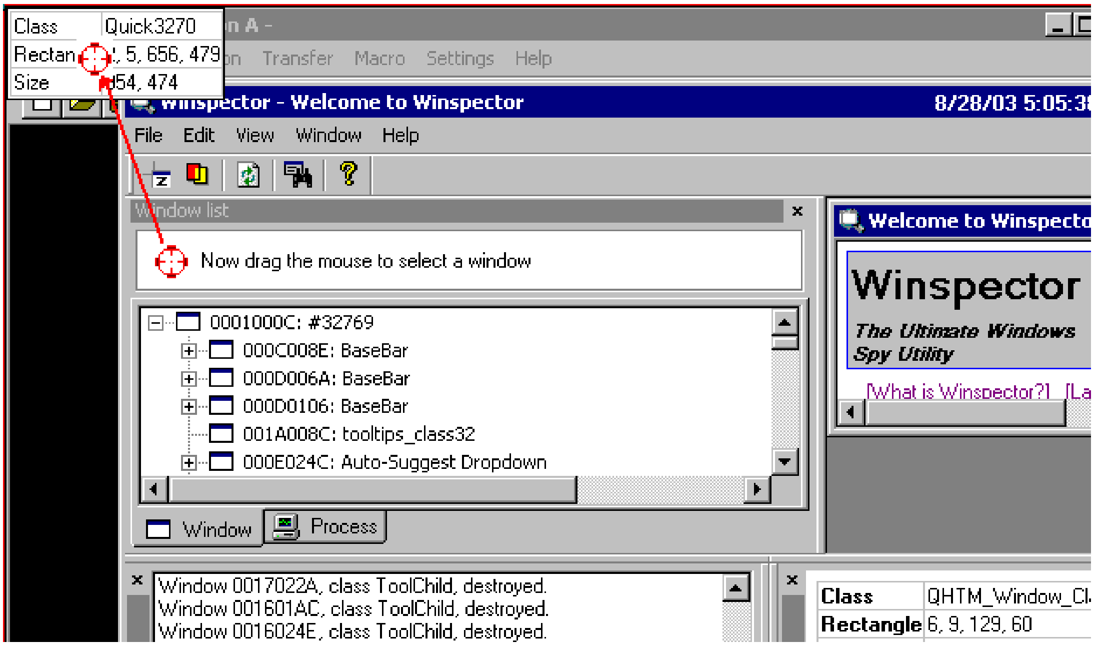
Class	Afx:400000:8:10011:0:8f0299
Rectangle	181, 13, 781, 424
Size	600, 411

The colour at the cursor is:

RGB	212, 208, 200
HEX	D4, D0, C8
HTML format	#D4D0C8

3 Arrange the windows so that emulator window and Winspector window are both visible on the screen.

4 Click and drag the Winspector icon to the title bar of the emulator, then release the mouse.


n A -
n Transfer Macro Settings Help
Winspector - Welcome to Winspector
8/28/03 5:05:3
File Edit View Window Help
Window list
Now drag the mouse to select a window
Window
Process
Welcome to Winspecto
Winspector
The Ultimate Windows Spy Utility
[What is Winspector?] [La

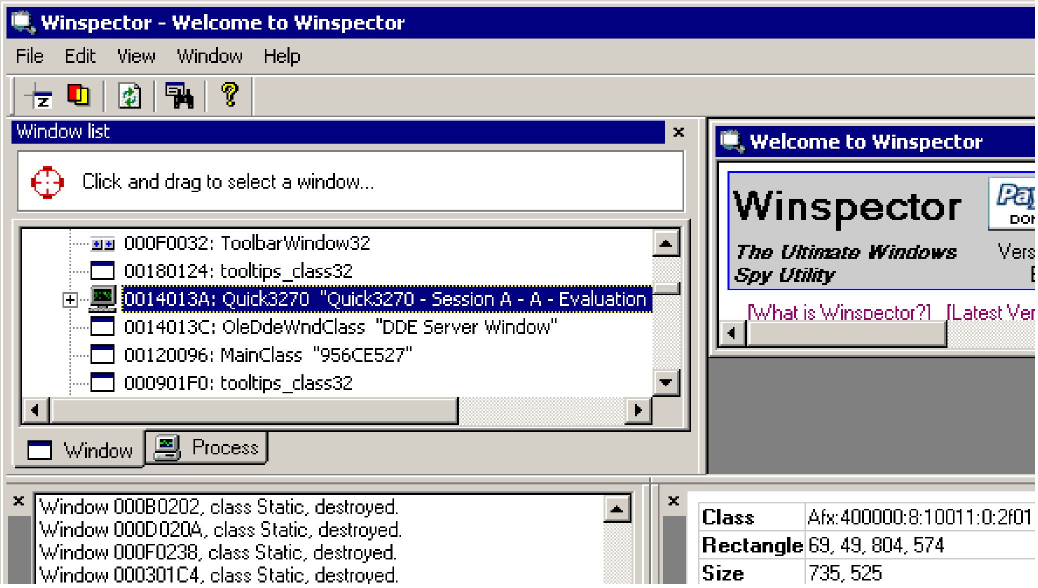
Class	Quick3270
Rectan	, 5, 656, 479
Size	54, 474

```
0001000C: #32769
  000C008E: BaseBar
  000D006A: BaseBar
  000D0106: BaseBar
  001A008C: tooltips_class32
  000E024C: Auto-Suggest Dropdown
```

```
Window 0017022A, class ToolChild, destroyed.
Window 001601AC, class ToolChild, destroyed.
Window 0016024E, class ToolChild, destroyed.
```

Class	QHTM_Window_Cl
Rectangle	6, 9, 129, 60

5 Verify that the title displayed on the emulator’s title bar is listed among applications in Winspector’s Click and Drag To Select a Window pane.

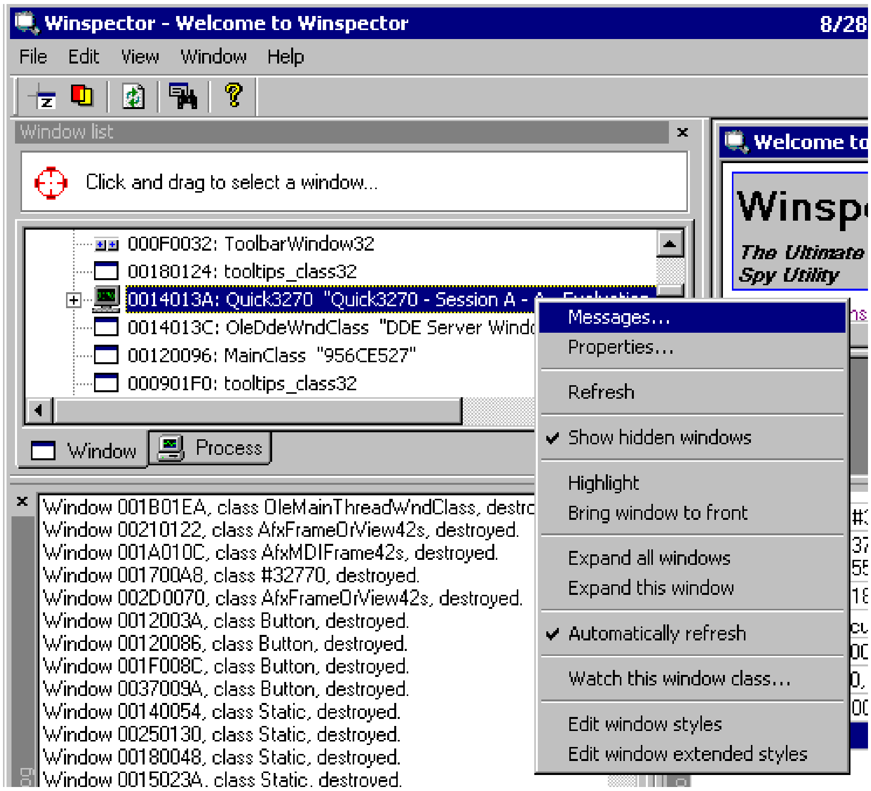

Winspector - Welcome to Winspector
File Edit View Window Help
Window list
Click and drag to select a window...
Window
Process
Welcome to Winspector
Winspector
The Ultimate Windows Spy Utility
[What is Winspector?] [Latest Ver

```
000F0032: ToolbarWindow32
00180124: tooltips_class32
0014013A: Quick3270  "Quick3270 - Session A - A - Evaluation
0014013C: OleDdeWndClass  "DDE Server Window"
00120096: MainClass  "956CE527"
000901F0: tooltips_class32
```

```
Window 000B0202, class Static, destroyed.
Window 000D020A, class Static, destroyed.
Window 000F0238, class Static, destroyed.
Window 000301C4, class Static, destroyed.
```

Class	Afx:400000:8:10011:0:2f01
Rectangle	69, 49, 804, 574
Size	735, 525

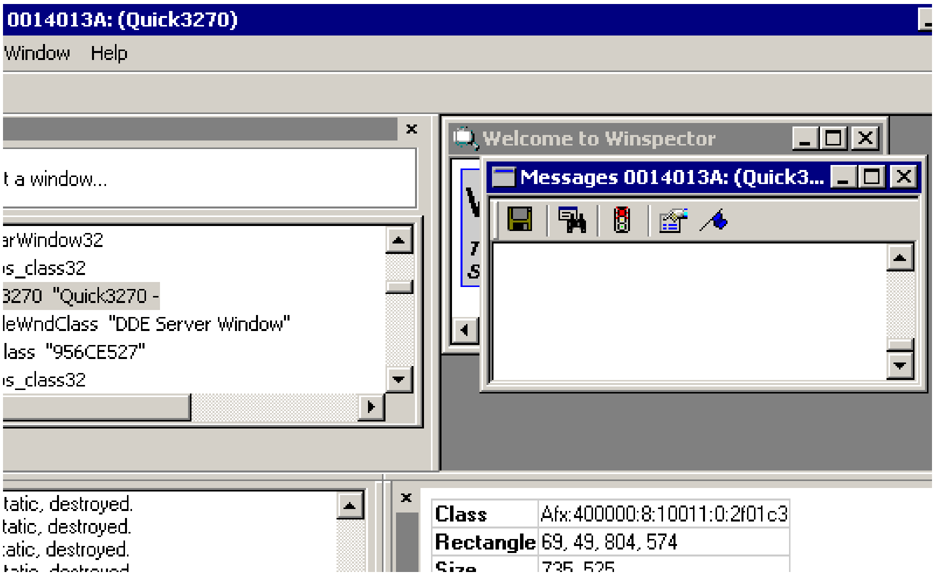
6 Right-click the emulator name, then click Messages.



```
000F0032: ToolbarWindow32
00180124: tooltips_class32
0014013A: Quick3270  "Quick3270 - Session A -
0014013C: OleDdeWndClass  "DDE Server Windc
00120096: MainClass  "956CE527"
000901F0: tooltips_class32
```

```
Window 001B01EA, class OleMainThreadWndClass, destrc
Window 00210122, class AfxFrameOrView42s, destroyed.
Window 001A010C, class AfxMDIFrame42s, destroyed.
Window 001700A8, class #32770, destroyed.
Window 002D0070, class AfxFrameOrView42s, destroyed.
Window 0012003A, class Button, destroyed.
Window 00120086, class Button, destroyed.
Window 001F008C, class Button, destroyed.
Window 0037009A, class Button, destroyed.
Window 00140054, class Static, destroyed.
Window 00250130, class Static, destroyed.
Window 00180048, class Static, destroyed.
Window 0015023A, class Static, destroyed.
```

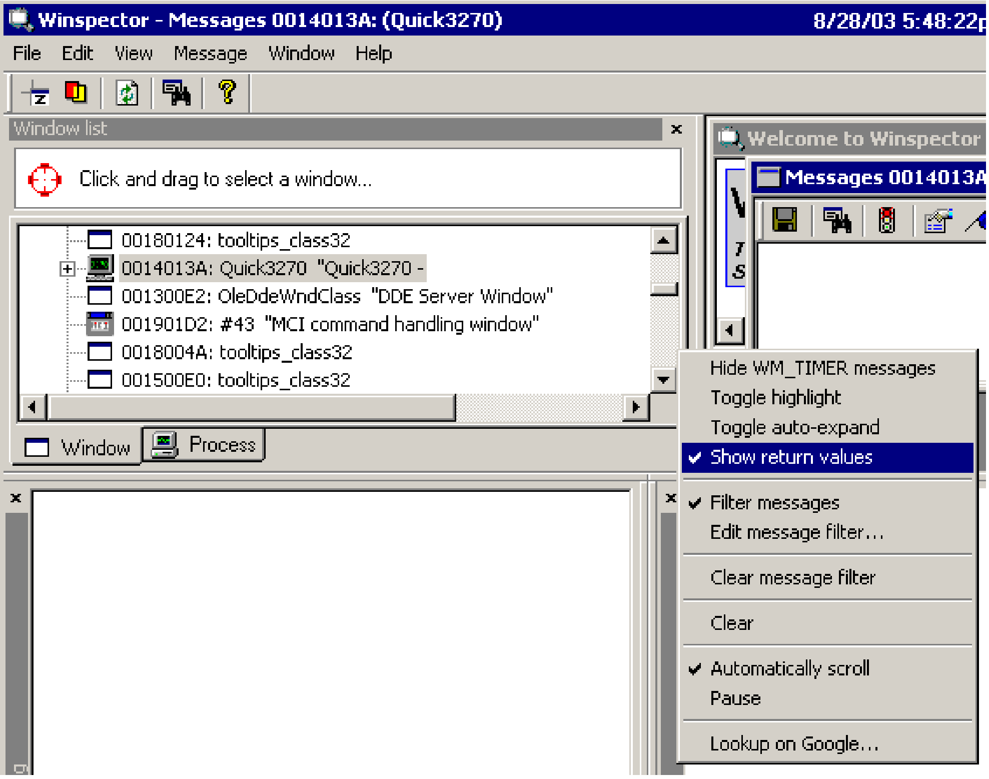
With the Messages window open, Winspector is ready to capture and log messages.



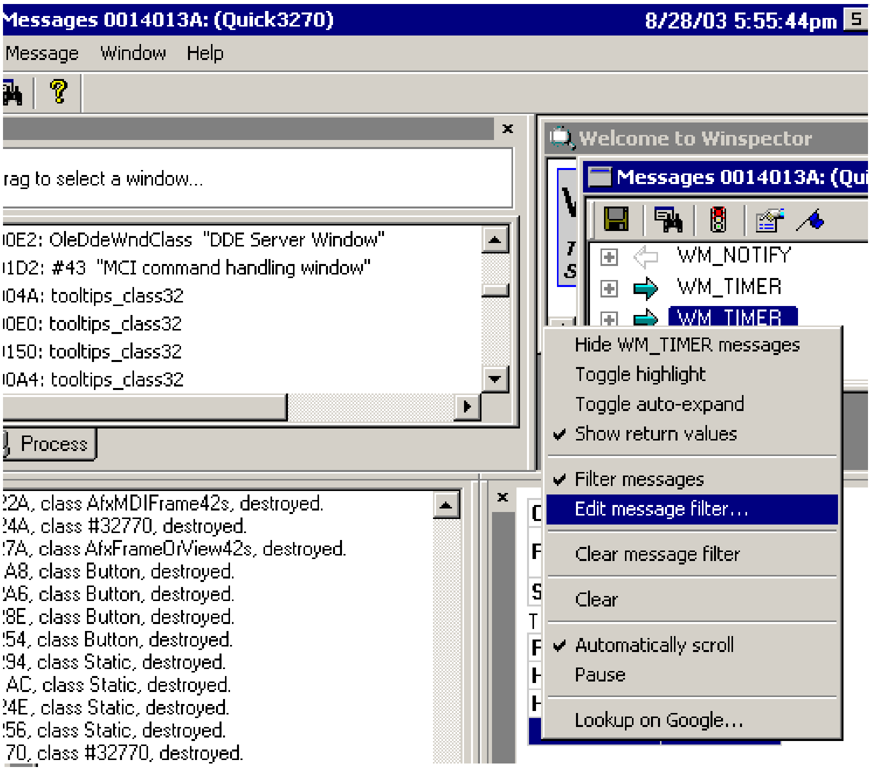
Class	Afx:400000:8:10011:0:2f01c3
Rectangle	69, 49, 804, 574
Size	735, 525

7 Limit what Winspector captures and logs.

7a Right-click in the Messages window, then uncheck Show Return Values.


Winspector - Messages 0014013A: (Quick3270)
8/28/03 5:48:22p
File Edit View Message Window Help
Window list
Click and drag to select a window...
00180124: tooltips_class32
0014013A: Quick3270 "Quick3270 -
001300E2: OleDdeWndClass "DDE Server Window"
001901D2: #43 "MCI command handling window"
0018004A: tooltips_class32
001500E0: tooltips_class32
Window
Process
Welcome to Winspector
Messages 0014013A
Hide WM_TIMER messages
Toggle highlight
Toggle auto-expand
✓ Show return values
✓ Filter messages
Edit message filter...
Clear message filter
Clear
✓ Automatically scroll
Pause
Lookup on Google...

7b Right-click in the Messages window, then click Edit Message Filter.



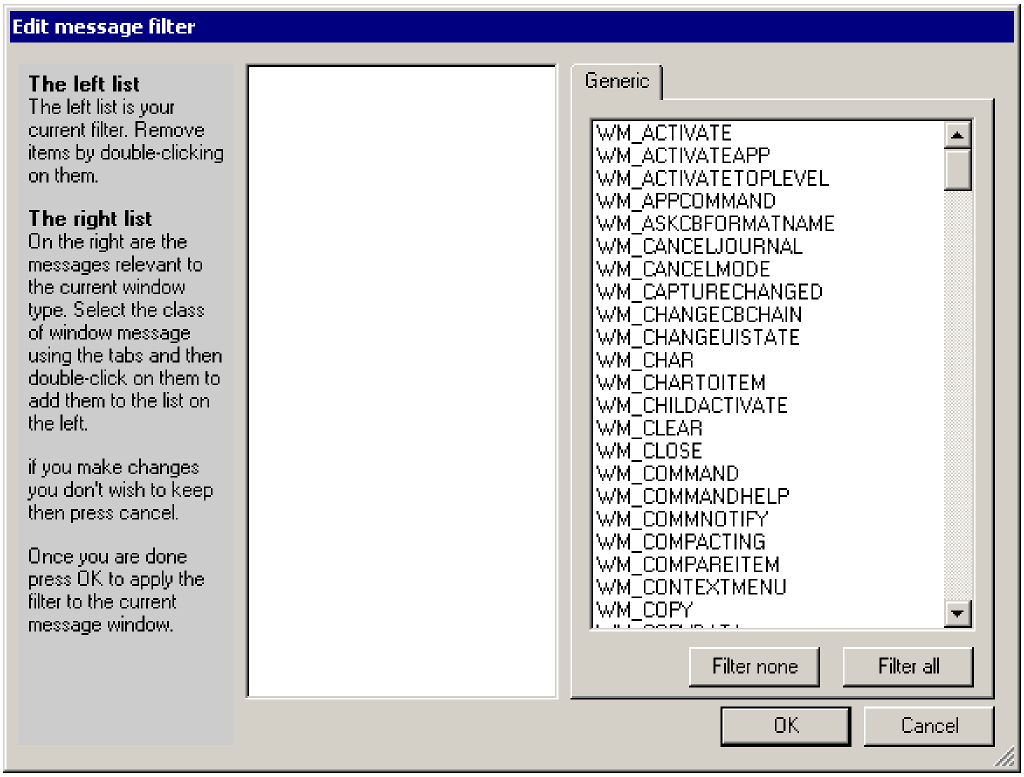
rag to select a window...

```
0E2: OleDdeWndClass  "DDE Server Window"
1D2: #43  "MCI command handling window"
04A: tooltips_class32
0E0: tooltips_class32
150: tooltips_class32
0A4: tooltips_class32
```

```
WM_NOTIFY
WM_TIMER
WM_TIMER
```

```
2A, class AfxMDIFrame42s, destroyed.
4A, class #32770, destroyed.
7A, class AfxFrameOrView42s, destroyed.
A8, class Button, destroyed.
A6, class Button, destroyed.
8E, class Button, destroyed.
54, class Button, destroyed.
94, class Static, destroyed.
AC, class Static, destroyed.
4E, class Static, destroyed.
56, class Static, destroyed.
70, class #32770, destroyed.
```

7c From the Edit Message Filter Window, click Filter All.



The left list
The left list is your current filter. Remove items by double-clicking on them.

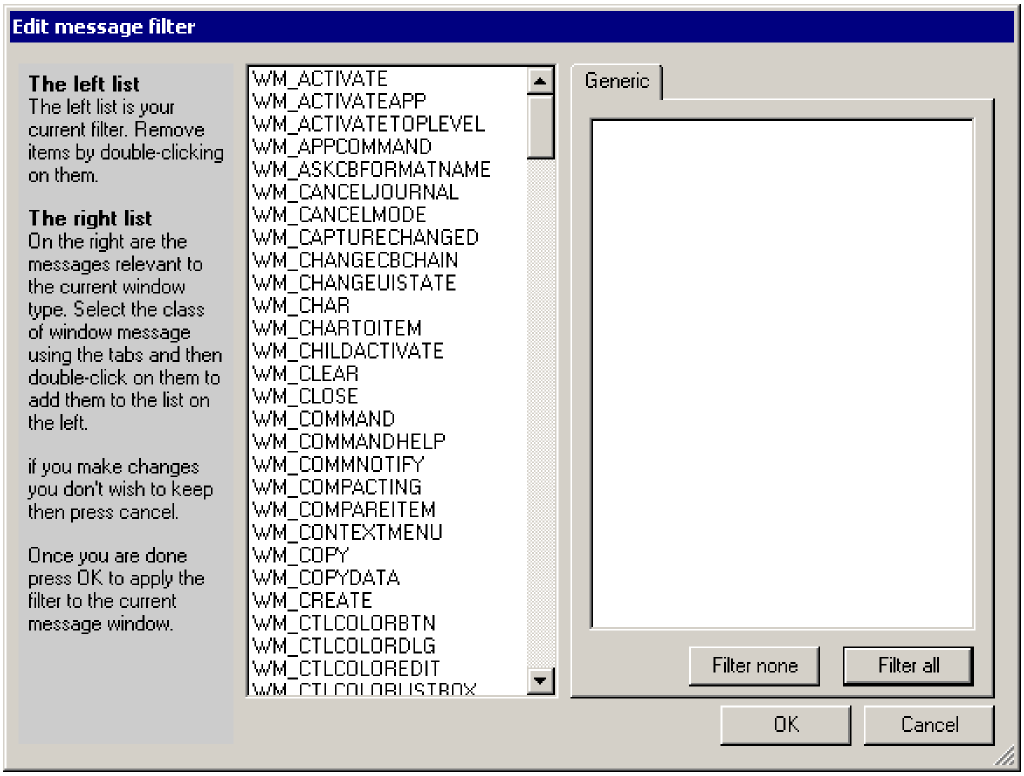
The right list
On the right are the messages relevant to the current window type. Select the class of window message using the tabs and then double-click on them to add them to the list on the left.

if you make changes you don't wish to keep then press cancel.

Once you are done press OK to apply the filter to the current message window.

```
WM_ACTIVATE
WM_ACTIVATEAPP
WM_ACTIVATETOPLEVEL
WM_APPCOMMAND
WM_ASKCBFORMATNAME
WM_CANCELJOURNAL
WM_CANCELMODE
WM_CAPTURECHANGED
WM_CHANGECBCHAIN
WM_CHANGEUISTATE
WM_CHAR
WM_CHARTOITEM
WM_CHILDACTIVATE
WM_CLEAR
WM_CLOSE
WM_COMMAND
WM_COMMANDHELP
WM_COMMNOTIFY
WM_COMPACTING
WM_COMPAREITEM
WM_CONTEXTMENU
WM_COPY
```

When all messages are filtered, Winspector rejects all messages. The Messages window won't be cluttered with unwanted messages.



The left list
The left list is your current filter. Remove items by double-clicking on them.

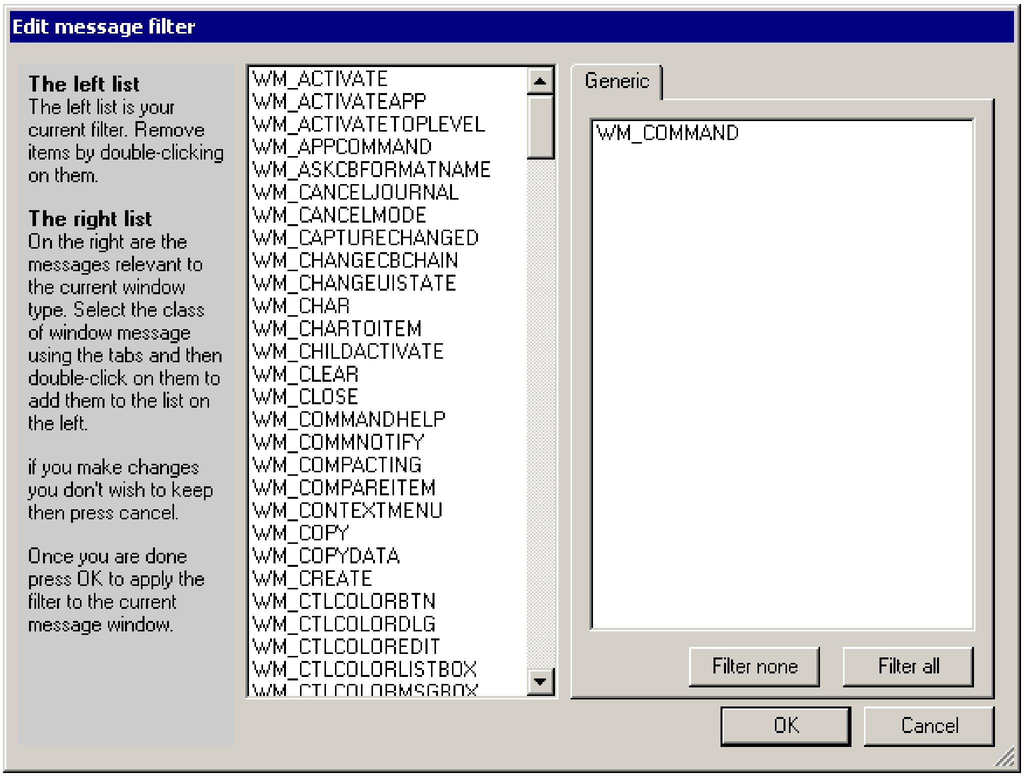
The right list
On the right are the messages relevant to the current window type. Select the class of window message using the tabs and then double-click on them to add them to the list on the left.

if you make changes you don't wish to keep then press cancel.

Once you are done press OK to apply the filter to the current message window.

```
WM_ACTIVATE
WM_ACTIVATEAPP
WM_ACTIVATETOPLEVEL
WM_APPCOMMAND
WM_ASKCBFORMATNAME
WM_CANCELJOURNAL
WM_CANCELMODE
WM_CAPTURECHANGED
WM_CHANGECBCHAIN
WM_CHANGEUISTATE
WM_CHAR
WM_CHARTOITEM
WM_CHILDACTIVATE
WM_CLEAR
WM_CLOSE
WM_COMMAND
WM_COMMANDHELP
WM_COMMNOTIFY
WM_COMPACTING
WM_COMPAREITEM
WM_CONTEXTMENU
WM_COPY
WM_COPYDATA
WM_CREATE
WM_CTLCOLORBTN
WM_CTLCOLORDLG
WM_CTLCOLOREDIT
WM_CTLCOLORLISTBOX
```

7d Scroll to and double-click WM_COMMAND, then click OK.



The left list
The left list is your current filter. Remove items by double-clicking on them.

The right list
On the right are the messages relevant to the current window type. Select the class of window message using the tabs and then double-click on them to add them to the list on the left.

if you make changes you don't wish to keep then press cancel.

Once you are done press OK to apply the filter to the current message window.

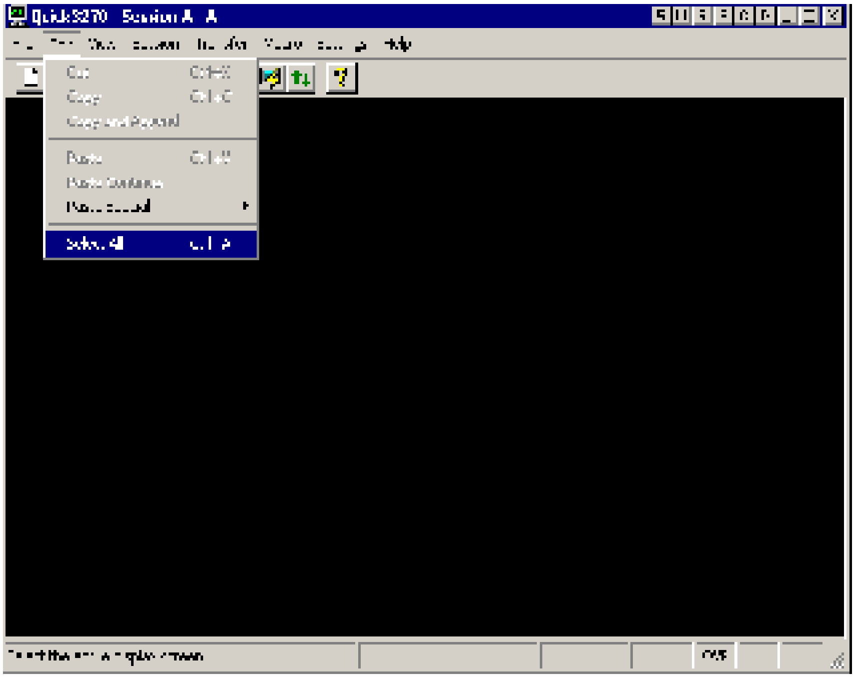
```
WM_ACTIVATE
WM_ACTIVATEAPP
WM_ACTIVATETOPLEVEL
WM_APPCOMMAND
WM_ASKCBFORMATNAME
WM_CANCELJOURNAL
WM_CANCELMODE
WM_CAPTURECHANGED
WM_CHANGECBCHAIN
WM_CHANGEUISTATE
WM_CHAR
WM_CHARTOITEM
WM_CHILDACTIVATE
WM_CLEAR
WM_CLOSE
WM_COMMANDHELP
WM_COMMNOTIFY
WM_COMPACTING
WM_COMPAREITEM
WM_CONTEXTMENU
WM_COPY
WM_COPYDATA
WM_CREATE
WM_CTLCOLORBTN
WM_CTLCOLORDLG
WM_CTLCOLOREDIT
WM_CTLCOLORLISTBOX
WM_CTLCOLORMSGBOX
```

```
WM_COMMAND
```

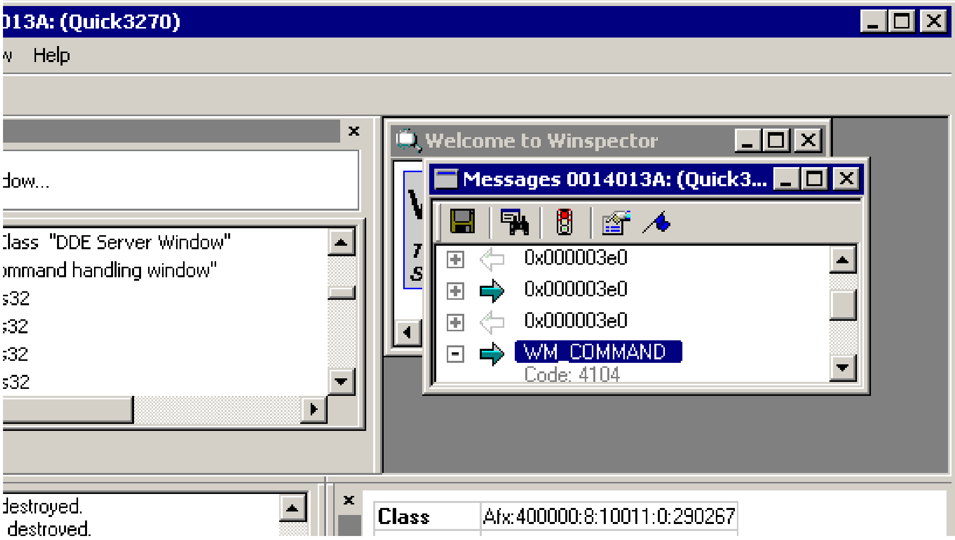
Viewing Control ID Numbers

1 (Conditional) From the emulator’s Edit drop-down list, click Select All.

If the emulator doesn’t have a Select All option, skip this step.



2 In Winspector’s Messages window, expand WM_COMMAND.



dow...

lass "DDE Server Window"
mmand handling window"
s32
s32
s32
s32

0x000003e0
0x000003e0
0x000003e0
WM_COMMAND
Code: 4104

destroyed.
destroyed.

Class	Afx:400000:8:10011:0:290267

3 View the Control ID.

Winspector uses the Code line to display the control ID. In this example, the control ID for Select All is 4104.

4 Find the Control IDs for the Copy and Paste functions by repeating Step 1 through Step 3.

5 Configure Terminal Launcher by adding the Control IDs.

Using Alternatives to Control ID Numbers

In the following situations, use an alternative to Control ID numbers:

- An emulator doesn't have standard Control IDs. Either no IDs are present or all functions have the same ID.
- The Control IDs in the Terminal Launcher configuration don't work.
- You don't have access to software such as Winspector or Spy++ to find the Control IDs.

The alternatives simulate keyboard shortcuts that achieve the same outcome. The keystrokes that you simulate depend on the keyboard shortcuts. The following tables lists the typical shortcuts:

Function	Keyboard Shortcut
Copy	Ctrl+C
Paste	Ctrl+V
Select All	Ctrl+A

For example, if the Select All Control ID 64 and the Copy Control ID 50 don't work with Terminal Launcher, try any of the following alternatives in the Output IDs text box.

Alternative One

```
\Alt+E,S,\Alt+E,C
```

This output simulates the following:

- Alt+E (displays the Edit menu list)
- S (selects Select All)
- Alt+E (brings up the Edit menu list)
- C (selects Copy)

Keys are not case sensitive.

Alternative Two

```
\Ctrl+a,\Ctrl+c
```

This output simulates the following:

- Control+A (a keyboard shortcut for Select All)
- Control+C (a keyboard shortcut for Copy)

Alternative Three

```
\Alt+e,\|40,\|40,\N,\Alt+e,\N
```

This output simulates the following:

- Alt+E (displays the Edit menu list)
- Down-arrow
- Down-arrow (scrolls down to Select All)

- Enter (selects Select All)
- Alt+E (displays the Edit menu list)
- Enter (selects Copy)

All of these alternatives might or might not work with particular emulators. They will all need customizing to suit the emulator. You can adapt the alternatives to suit any requirement (for example, selecting other menu items).

Finding a Terminal Launcher configuration, including finding alternatives to the Control IDs, requires trial and error, which becomes easier with experience.

When you use alternatives, the increased number of steps slows the Terminal Launcher process slightly.

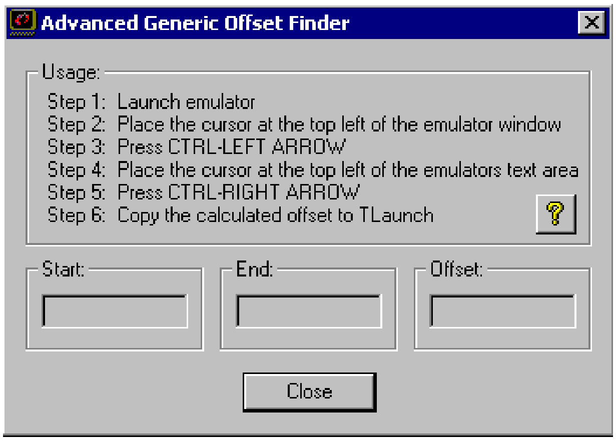
Finding Offsets

Advanced Generic emulators don’t have a Select All function. To compensate, you must gather information by dragging-and-dropping across the emulator’s screen, from the top-left corner to the bottom-right corner of the display area. Therefore, you need to know the offsets, so that you begin dragging at the correct location. Otherwise, the drag-and-drop process might cause unexpected behavior (Drag your tool bar or window off the screen, close an application, resize your desktop...).

You can easily find offsets required for Advanced Generic emulators by using nslfindera.exe. Download this utility from Novell’s Support Web site (http://support.novell.com/servlet/filefinder?name=nslfinder.exe).

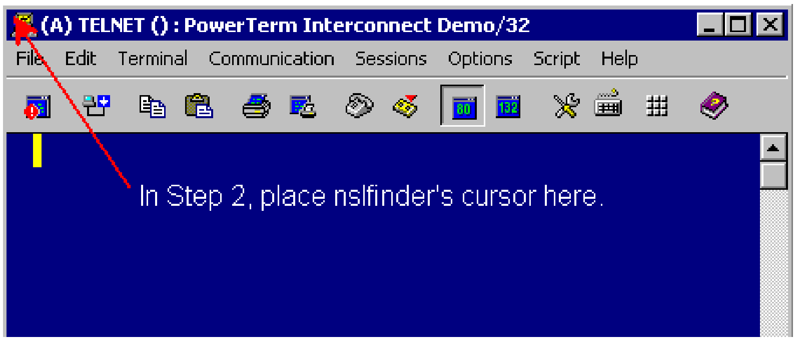
To find offsets:

1 Open the emulator, then open nslfindera.exe.



Step 1: Launch emulator
Step 2: Place the cursor at the top left of the emulator window
Step 3: Press CTRL-LEFT ARROW
Step 4: Place the cursor at the top left of the emulators text area
Step 5: Press CTRL-RIGHT ARROW
Step 6: Copy the calculated offset to TLaunch

2 Place nslfinder’s cursor in the top left corner of the emulator’s window.

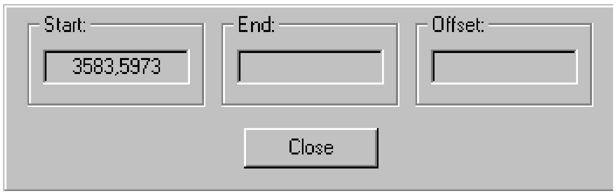


(A) TELNET () : PowerTerm Interconnect Demo/32
File Edit Terminal Communication Sessions Options Script Help
80
132

In Step 2, place nslfinder's cursor here.

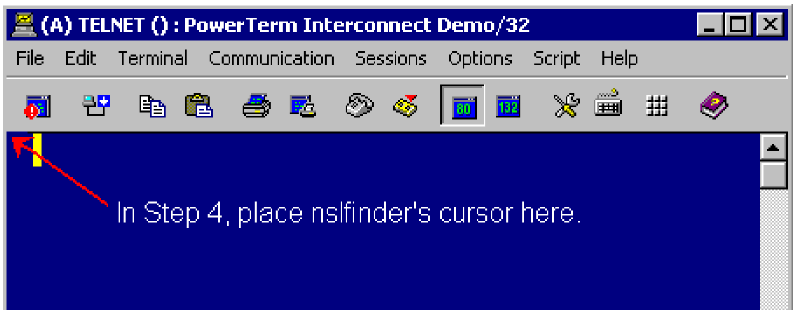
3 Type Ctrl+Left-arrow.

Nslfinder pastes the value into the Start text box.



Start: 3583,5973
End:
Offset:

4 Place nslfinder’s cursor in the upper left corner of the emulator’s text pane.

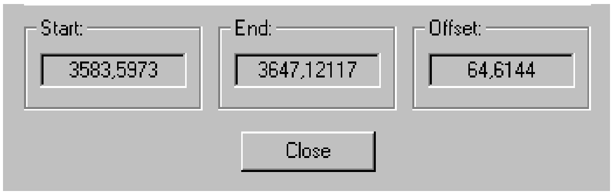


(A) TELNET () : PowerTerm Interconnect Demo/32
File Edit Terminal Communication Sessions Options Script Help
80
132

In Step 4, place nslfinder's cursor here.

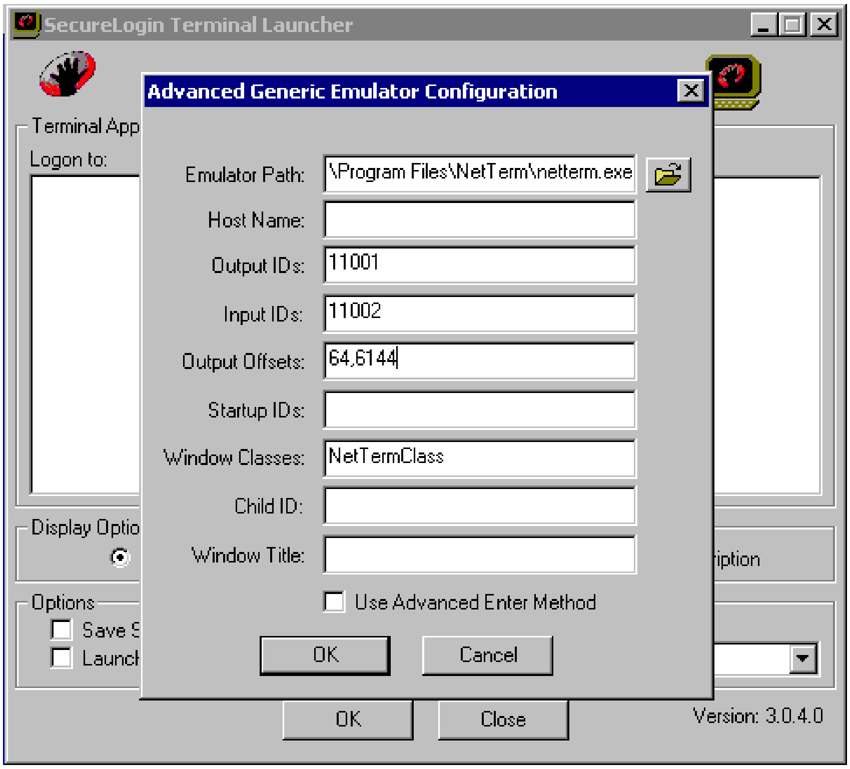
5 Type Ctrl+Right-arrow.

Nslfinder pastes the end value of the emulator’s tool bar and menu areas into the End text box and pastes the offset numbers into the Offset text box.



Start: 3583,5973
End: 3647,12117
Offset: 64,6144

6 Copy the offset values into Terminal Launcher’s Output Offsets text box.



Emulator Path: \Program Files\NetTerm\netterm.exe

Host Name:

Output IDs: 11001

Input IDs: 11002

Output Offsets: 64,6144

Startup IDs:

Window Classes: NetTermClass

Child ID:

Window Title:

□ Use Advanced Enter Method

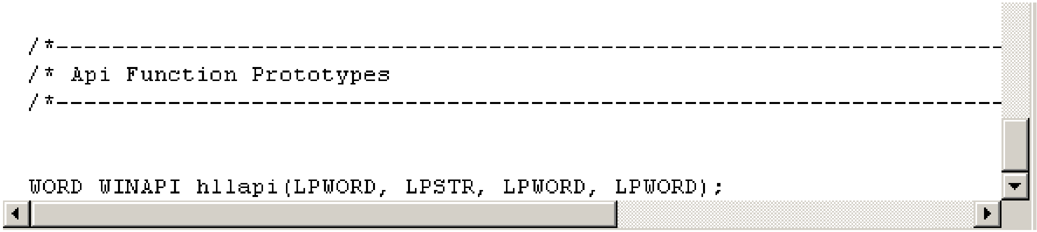
E Finding HLLAPI Types

This section provides information on the following:

- "Using Header Files" on page 147
- "Using Dependency Walker" on page 147

Using Header Files

If the emulator has an accompanying .h file, search it to find the HLLAPI function. The function might be named hllapi, HLLAPI, or some variation. The following figure illustrates the hllapi notation in the .h file for Quick3270:



```
/*--------------------------------------------------------------------
/* Api Function Prototypes
/*--------------------------------------------------------------------


WORD WINAPI hllapi(LPWORD, LPSTR, LPWORD, LPWORD);
```

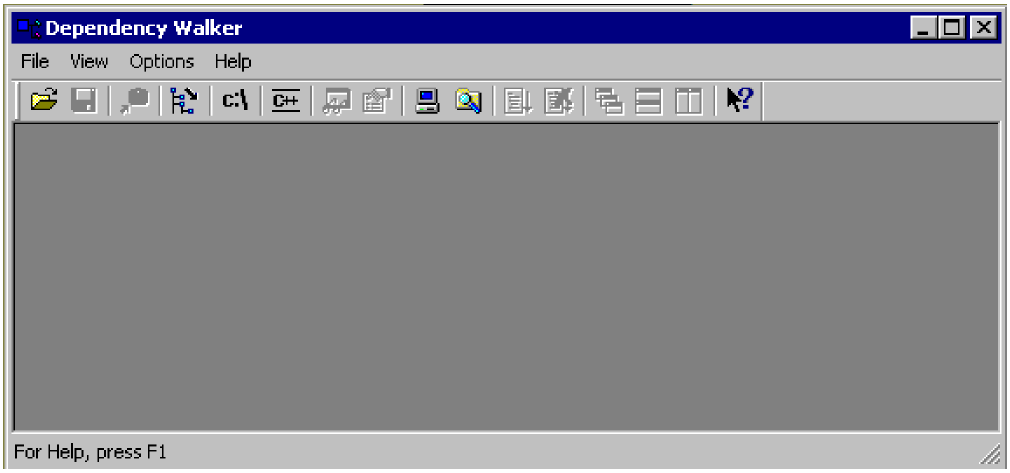
Using Dependency Walker

Dependency Walker (depends.exe) can help you configure terminal emulators for SecureLogin's single sign-on functionality.

NOTE: Dependency Walker doesn't work with 16-bit HLLAPI emulators.

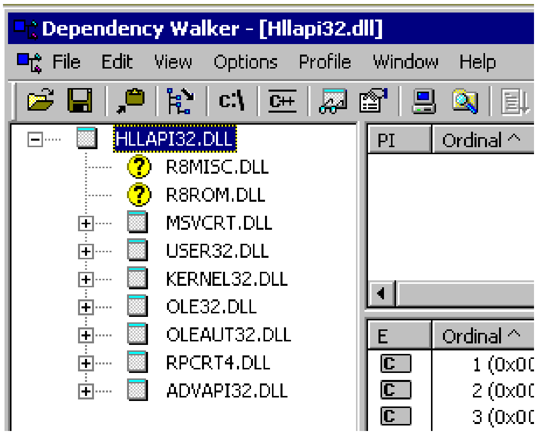
Dependency Walker is available from the Dependency Walker Web site (http://www.dependencywalker.com).

1 Run depends.exe.



2 Click File > Open, then navigate to and open the hllappi.dll file.

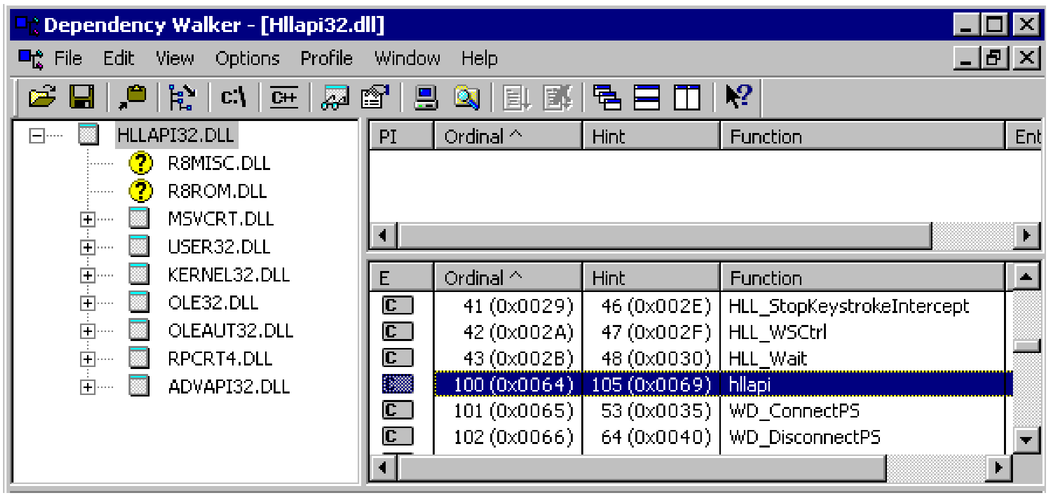
Look for a .dll file with the name "HLLAPI" (or some variation) in it. For example, the file for Quick3270 is QHLLAPI.DLL, found in the c:\Program Files\Quick3270 directory.



3 In the function exports window, scroll through the exports until you locate "hllapi".

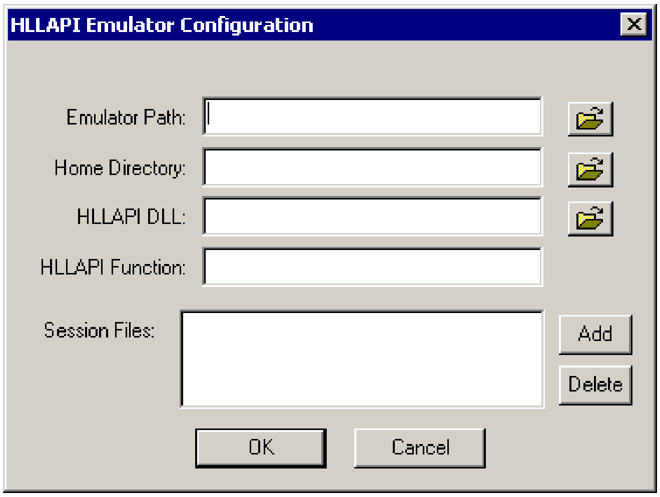
The hllapi.dll file contains many HLLAPI functions. Use Dependency Walker to identify the HLLAPI initialization function or entry point. Typically, this function is called hllapi, Hllapi, Winhllapi, or WinHllapi. Look for some variation of hllapi.

As the following figure illustrates, the export function displayed for Quick3270 is hllapi.



E	Ordinal ^	Hint	Function
C	41 (0x0029)	46 (0x002E)	HLL_StopKeystrokeIntercept
C	42 (0x002A)	47 (0x002F)	HLL_WSCtrl
C	43 (0x002B)	48 (0x0030)	HLL_Wait
C	100 (0x0064)	105 (0x0069)	hllapi
C	101 (0x0065)	53 (0x0035)	WD_ConnectPS
C	102 (0x0066)	64 (0x0040)	WD_DisconnectPS

4 Enter this function type in Terminal Launcher’s HLLAPI Function text box.



The function is case sensitive. For example, if the function is Hllapi and you enter hllapi, the emulator won’t work.

F Error Codes

This section contains error codes for SecureLogin.

For help with error codes that provide possible causes along with actions you can take, see "Error Codes with Tips" on page 151.

For a list of error codes that require help from Novell® Technical Services, see "Other Error Codes" on page 169.

For information on error codes for LDAP, see LDAP and NDS Integration (http://developer.novell.com/ndk/doc_jldapunx.htm) in the Novell Developer Kit (NDK). Navigate to an option under LDAP Server Return Codes. For example, select LDAP and NDS®, select LDAP Return Codes, then select LDAP Server Return Codes.

Error Codes with Tips

The error codes in this section provide information on what caused the error and possible actions to resolve the error.

-102 BROKER_NO_SUCH_ENTRY

Possible Cause: You tried to load a script or variable that doesn't exist. For example, you set up Terminal Launcher to run from a shortcut or to run a particular script, but the script doesn't exist.

Action: Check that the name of the script is actually defined is SecureLogin. Verify that the name is the same as specified in the script editor.

-103 BROKER_INVALID_CLASS_CREATED

Possible Cause: You are running an earlier version. SecureLogin is trying to create a new version of the script data format that was stored in the directory.

Action: Upgrade the older SecureLogin client to the new client. Install the latest SecureLogin software.

-104 BROKER_CREATE_CLASS_FAILED

Possible Cause: The SecureLogin client has run out of memory.

Action: Free up some memory. Try again later.

-107 BROKER_ENTRY_NOT_FOUND

Possible Cause: You tried to load a script or variable that doesn't exist.

Action: Check that the name of the script is actually defined is SecureLogin. Verify that the name is the same as specified in the script editor.

-109 BROKER_SCRIPT_BUFFER_ALLOC_FAILED

Possible Cause: The SecureLogin client has run out of memory.

Action: Free up some memory. Try again later.

-112 BROKER_NO_SUCH_VARIABLE

Possible Cause: You are trying to use an undefined variable. Because SecureLogin isn't prompting you for the variable, data has become unusable, or some other situation is preventing the software from working as expected.

Action: Call Novell Technical Services.

-114 BROKER_PRIMARY_NOT_AVAILABLE

Possible Cause: You are not logged in to the directory. You are using the offline cache. Therefore, some directory functions can't be performed. (For example, you can't change your passphrase.)

Action: Log in to the directory.

-116 BROKER_HEADER_DATA_CORRUPT

Possible Cause: Data isn't available. You might have had a customized build for your site but have installed a standard version of SecureLogin, or have gone from a standard version to a customized build for your site.

Action: Clear the local cache and try again.

Action: Call Novell Technical Services.

-123 BROKER_CACHE_PASSWORD_INCORRECT

Possible Cause: You have tried to log in from offline mode, but the password you entered does not match the expected password from the local cache. Typically, the offline password is the passphrase answer. However, if you have installed the NMAS™ module, the passphrase can be the passphrase answer or your current directory password.

Action: Enter the correct passphrase answer or directory password.

-129 BROKER_ENTRY_LIST_NOT_NULL

Possible Cause: The software is not working as intended.

Action: Clear the local cache and try again.

Action: Call Novell Technical Services.

-131 BROKER_SYM_LIST_NOT_NULL

Possible Cause: Memory is not being handled as expected.

Action: Call Novell Technical Services.

-138 BROKER_SYMBOL_DATA_CORRUPT

Possible Cause: SecureLogin is unable to use the data in the local cache file or in the directory.

Action: Clear the local cache and try again.

Action: Call Novell Technical Services.

-140 BROKER_SCRIPT_DATA_CORRUPT

Possible Cause: SecureLogin is unable to use data in scripts.

Action: Clear the local cache and try again.

Action: Call Novell Technical Services.

-166 BROKER_INVALID_DES_KEY

Possible Cause: Hex strings are invalid. The DES_KEY variable requires hexadecimal (0-9, A-F) numbers.

Action: Make sure that the DES_KEY variable contains only hexadecimal numbers.

-167 BROKER_INVALID_DES_OFFSET

Possible Cause: Hex strings are invalid. The DES_OFFSET variable requires hexadecimal (0-9, A-F) numbers.

Action: Make sure that the DES_OFFSET variable contains only hexadecimal numbers.

-168 BROKER_DESKEY_NOT_FOUND

Possible Cause: You tried to generate a one-time password for a platform. However, you haven't defined the DES_KEY variable.

Action: Create the DES_KEY variable.

-169 BROKER_DESOFFSET_NOT_FOUND

Possible Cause: You tried to generate a one-time password for a platform. However, you haven't defined the DES_OFFSET variable.

Action: Create the DES_OFFSET variable.

-171 BROKER_CACHE_FILE_OPEN_FAIL

Possible Cause: SecureLogin tried to read or write to the offline cache. However, SecureLogin is unable to open the cache file.

Action: Assign rights so that the specified user has rights to the cache directory.

-174 BROKER_CACHE_SAVE_FAILED

Possible Cause: SecureLogin tried to save data to the offline cache but is unable to.

Action: Assign rights so that the specified user has rights to the cache directory.

-175 BROKER_CACHE_SECRETS_INCORRECT

Possible Cause: The offline cache password is incorrect. The key that is being used to decrypt the cache file is not the key that the cache file was encrypted with.

Possible Cause: After logging in as a user and creating a cache file, you went to another workstation, reset your passphrase, and logged in. You receive this error when you return to the original workstation.

Action: Clear the cache.

-176 BROKER_PUBLIC_KEY_READ_FAILED

Possible Cause: SecureLogin is unable to read the public key from the directory.

Action: Troubleshoot the directory.

-179 BROKER_RTVALUE_DOES_NOT_EXIST

Possible Cause: You tried to read a runtime variable that has not been defined.

Action: Check the script. Make sure that the variable has been set before it is read or used as a command.

-180 BROKER_DS_VARIABLE_NOT_READ

Possible Cause: You used one of the % variables to read a directory attribute, but SecureLogin can't read the variable.

Action: Make sure that you have spelled the attribute name correctly.

Action: Troubleshoot the directory.

-181 BROKER_WRONG_PASS_PHRASE

Possible Cause: You entered the wrong passphrase.

Possible Cause: You tried to change your passphrase but typed it incorrectly.

Possible Cause: You enabled a preference relating to SecureLogin's hand icon. You double-clicked the hand icon but typed the passphrase incorrectly.

Action: Enter the passphrase correctly.

-190 BROKER_NO_AUTH_DATA_FOUND

Possible Cause: Although the Prot:SSO Entry attribute has data, the Prot:SSO Auth attribute was blank. Someone deleted the Prot:SSO Auth attribute.

Action: Delete the Prot:SSO Entry attribute. SecureLogin creates these attributes the next time that you run SecureLogin.

-192 BROKER_UNABLE_TO_INSTANTIATE

Possible Cause: A module (for example, WinSSO) has tried to connect to slbroker.exe but is unable to.

Action: If you are using Windows 95, make sure that you have the latest DCOM update, or reinstall Internet Explorer. For other platforms, reinstall SecureLogin.

-199 BROKER_ERROR_COMMAND_NOT_HANDLED

Possible Cause: A script parser encountered an unrecognizable command.

Action: Make sure that you have spelled the command correctly.

Action: Make sure that the If/EndIf blocks match.

-201 BROKER_UNEXPECTED_END_OF_SCRIPT

Possible Cause: If/EndIf or Repeat/EndRepeat blocks don't match. SecureLogin reached the end of the script without finding an expected EndIf or EndRepeat command.

Action: Check the script. Make sure that If/EndIf and Repeat/EndRepeat blocks match.

-211 BROKER_ENTRY_ALREADY_IN_LIST

Possible Cause: You tried to add a script or variable, but a script or variable with that name already exists.

Action: Use a different name for the script or variable, or use the script editor to rename the existing script or variable.

-217 BROKER_ARG_NUM

Possible Cause: In script language, each command expects a certain number of arguments. You have used either too few or too many arguments for a given command.

Action: Check the documentation for that command. Make sure that you are passing to the command the correct number of arguments.

-219 BROKER_NOT_A_NUMBER

Possible Cause: The script language was expecting a decimal number, but characters other than 0-9 appeared.

Action: Remove incorrect characters.

-220 BROKER_HLLAPI_FUNCTION_NOT_FOUND

Possible Cause: In the Terminal Launcher configuration, you specified a hllapi.dll and the name of the function in that DLL. The name of the function cannot be found in the DLL.

Action: Check the configuration for the emulator. Make sure that you typed the HLLAPI function correctly. See "Configuring WinHLLAPI, HLLAPI, or 16-Bit HLLAPI Emulators" on page 93.

-222 BROKER_HLLAPI_DLL_LOAD_FAILED

Possible Cause: Terminal Launcher was unable to load the hllapi.dll that you specified.

Action: Make sure that the path and file that you entered for the DLL are correct.

Possible Cause: The hllapi.dll for that emulator is looking for other .dll files that don't exist or haven't been installed for that emulator.

Action: You have probably chosen the wrong .dll file or have specified the wrong HLLAPI function (for example, HLLAPI or WinHLLAPI). Find the correct .dll and function. Check the vendor's documentation for information about that emulator.

You can use Microsoft* Spy++ to find Input and Output IDs.

-224 BROKER_ERROR_DURING_WINHLLAPICLEANUP

Possible Cause: Terminal Launcher has called the WinHLLAPI cleanup function for a WinHLLAPI emulator.

Action: Check the vendor's documentation for information about that emulator.

-225 BROKER_CANNOT_FIND_WINHLLAPISTARTUP_FUNCTION_IN_DLL

Possible Cause: In the Terminal Launcher configuration, you incorrectly specified that the emulator is a WinHLLAPI emulator.

Action: Check the configuration for the emulator. Specify the correct emulator type.

-226 BROKER_ERROR_DURING_WINHLLAPISTARTUP

Possible Cause: The terminal emulator does not support the right version of HLLAPI (requires at least V.1.1).

Possible Cause: The attempt to reset a connection to a HLLAPI terminal emulator has failed.

Action: Check the vendor's documentation for information about that emulator.

-227 BROKER_CANNOT_FIND_WINHLLAPICLEANUP_FUNCTION_IN_DLL

Possible Cause: In the Terminal Launcher configuration, you incorrectly specified that the emulator is a WinHLLAPI emulator.

Action: Using the Nsure SecureLogin 3.51.2 Configuration Guide for Terminal Emulation, check the configuration for the emulator. Specify the correct emulator type.

-228 BROKER_BUTTON_NOT_FOUND

Possible Cause: For a Windows single sign-on application, no button exists for the control ID that you specified. For example, if you specified Click #3, no button exists for control ID 3.

Action: Specify the correct control ID number for the button.

-230 BROKER_SETPLAT_FAILED

Possible Cause: The regular expression that you supplied in the SetPlat command is invalid.

Action: Check the syntax of the regular expression that you provided.

-232 BROKER_UNABLE_TO_START_PROGRAM

Possible Cause: The Run command was unable to find and start the requested program.

Action: Make sure that the executable program exists and that the path is correct.

-236 BROKER_CHANGEPASSWORD_INVALID_VARIABLE_SYNTAX

Possible Cause: One of the parameters that you pass to the ChangePassword command must be a variable. The parameter that you provided is not a variable.

Action: Specify a variable.

-237 BROKER_MAD_COMMAND_SET_INVALID_VARIABLE_SYNTAX

Possible Cause: The first parameter that you pass to the Set command must be a variable. The parameter that you provided is not a variable.

Action: Specify a variable.

-239 BROKER_POLICY_SCRIPT_ARG_NUM

Possible Cause: One of the commands in a password policy script has too few or too many arguments.

Action: Include the correct number of arguments.

-240 BROKER_VALID_CHARS_OUTNUMBERED

Possible Cause: A password is unable to satisfy a password policy because the maximum number of allowable characters is less than the minimum number of allowable characters.

Action: Set the maximum number of a particular class of characters to a greater number than the minimum number of specified allowable characters.

-241 BROKER_PASSWORD_LOGIC_ERROR

Possible Cause: You have incorrectly set up a password policy. No password can satisfy all the settings.

Action: Work through each restriction in the password policy, making sure that one restriction doesn't contradict another restriction in the policy.

-242 BROKER_EXCEPTION_CHARACTER_FOUND

Possible Cause: You entered a password that contains a character that isn't allowed.

Action: Use allowable characters in your password.

-243 BROKER_PASSWORD_TOO_SHORT

Possible Cause: You entered a password that doesn't have enough characters.

Action: Provide enough characters in your password.

-244 BROKER_PASSWORD_TOO_LONG

Possible Cause: You entered a password that has too many characters.

Action: Type the correct number of characters.

-245 BROKER_INSUFFICIENT_UPPERCASE_CHARS

Possible Cause: You entered a password that has too few uppercase characters.

Action: Use the specified number of uppercase characters in your password.

-246 BROKER_TOO_MANY_UPPERCASE_CHARS

Possible Cause: You entered a password that has too many uppercase characters.

Action: Use the specified number of uppercase characters in your password.

-247 BROKER_INSUFFICIENT_LOWERCASE_CHARS

Possible Cause: You entered a password that has too few lowercase characters.

Action: Use the specified number of lowercase characters in your password.

-248 BROKER_TOO_MANY_LOWERCASE_CHARS

Possible Cause: You entered a password that has too many lowercase characters.

Action: Use the specified number of lowercase characters in your password.

-249 BROKER_INSUFFICIENT_PUNCTUATION_CHARS

Possible Cause: You entered a password that has too few punctuation characters.

Action: Use the specified number of punctuation characters in your password.

-250 BROKER_TOO_MANY_PUNCTUATION_CHARS

Possible Cause: You entered a password that has too many punctuation characters.

Action: Use the specified number of punctuation characters in your password.

-251 BROKER_INSUFFICIENT_NUMERALS

Possible Cause: You entered a password that has too few numerals.

Action: Use the specified number of numerals in your password.

-252 BROKER_TOO_MANY_NUMERALS

Possible Cause: You entered a password that has too many numerals.

Action: Use the specified number of numerals in your password.

-256 BROKER_UNABLE_TO_GET_NT_CACHE_DIR

Possible Cause: You are using NT 4 Domains mode, but you haven't defined or mapped a home drive.

Action: Log in as the user to determine whether the home drive and home path variables are set. If the variables are not set, use the NT domain administrative tools to set them.

-257 BROKER_UNABLE_TO_CREATE_NT_CACHE_DIR

Possible Cause: The User object didn't have rights to create a directory on the user's home drive.

Action: Grant the User object rights to the directory.

-259 BROKER_MUST_BEGIN_WITH_UPPERCASE

Possible Cause: You entered a password that didn't begin with an uppercase character.

Action: Type an uppercase character at the beginning of the password.

-261 BROKER_ENTRY_SRC_OBJECT_MISMATCH

Possible Cause: You are using a platform other than eDirectory™ and have moved an object. The directory object that you are reading entries from is not the directory object that the entries were saved to.

Action: Manually copy and paste the scripts between the objects.

-262 BROKER_CACHE_FILE_INCORRECT_VERSION

Possible Cause: The cache file that you are trying to load was created by a later version of SecureLogin.

Action: Use the version of SecureLogin that created the cache file.

Action: Install the latest version of SecureLogin.

-264 BROKER_DDE_CONNECT_FAILED

Possible Cause: Terminal Launcher couldn't connect to a specified DDE emulator.

Action: Make sure that the emulator launched correctly and the emulator's DDE support is turned on.

-265 BROKER_DDE_DISCONNECT_FAILED

Possible Cause: An attempt to disconnect from a DDE-supporting terminal emulator failed.

Action: Refer to the vendor's documentation.

-266 BROKER_NT_FILE_STORAGE_SAVE_FAILED

Possible Cause: Using NT 4 Domains mode, the User object was unable to save to the equivalent of a cache file in the Home directory.

Action: Grant the User object rights so that the user can write files to the Home directory.

-269 BROKER_NOT_A_PASSWORD_POLICY_COMMAND

Possible Cause: An invalid command was used in a password policy.

Action: Make sure that the command is spelled correctly.

-271 BROKER_PASSWORD_UNACCEPTABLE

Possible Cause: The password didn't meet requirements as specified in password policies.

Action: Enter the password correctly.

-273 BROKER_MSTELNET_OPERATION_NOT_SUPPORTED

Possible Cause: The generic emulator can't support a particular operation (for example, SetCursor).

Action: For generic emulators, don't use the command.

-279 BROKER_EMULATOR_LAUNCH_FAILED

Possible Cause: In Terminal Launcher, you can configure the path to the executable that will run. However, the specified executable is unable to run.

Action: Make sure that the path to the emulator is correct.

-280 BROKER_UNABLE_TO_CREATE_EMULATOR

Possible Cause: You have specified an invalid terminal type in TLAUNCH.INI (or the Terminal Launcher configuration).

Action: Specify the correct terminal type.

-281 BROKER_INVALID_CHARACTER_FOUND_IN_PASTE_ID_LIST

Possible Cause: A comma doesn't separate decimal numbers for input and output control IDs.

Action: For generic emulators, you must specify a set of input and output control IDs. Use a comma to separate decimal numbers.

-282 BROKER_INVALID_CHARACTER_FOUND_IN_COPY_ID_LIST

Possible Cause: A comma doesn't separate decimal numbers for copy IDs

Action: For generic emulators, you must specify a set of copy control IDs. Use a comma to separate decimal numbers.

-283 BROKER_UNABLE_TO_READ_TLAUNCH_INI

Possible Cause: SecureLogin is unable to read the tlaunch.ini file because the file has been deleted.

Action: Create a blank tlaunch.ini file.

Action: Create a default tlaunch.ini file by reinstalling SecureLogin.

-284 BROKER_NO_TERMINAL_TYPE_DEFINED

Possible Cause: The tlaunch.ini file contains an error. The terminal type for the emulator has not been defined.

Action: Using Terminal Launcher, specify a terminal type for the emulator.

-290 BROKER_FILE_LOAD_FAILED

Possible Cause: You don’t have enough rights to convert an earlier tlaunch.ini file to a later format, read an earlier tlaunch.ini file, or create a new tlaunch.ini file.

Action: The network administrator must assign necessary rights.

-294 BROKER_SETPLAT_VARIABLE_MUST_BE_RUN_TIME

Possible Cause: The first argument to a SetPlat argument can be a variable. If it is a variable, it must be a runtime variable. The variable used is not a runtime variable.

Action: Make the first argument a runtime variable.

-295 BROKER_ERROR_CONDITIONAL_COMMAND_NOT_HANDLED

Possible Cause: SecureLogin doesn’t handle text in the second part of an If command.

Action: Make sure that the command is one listed and documented in the *SecureLogin Scripting Guide*.

-298 BROKER_RAW_MODE_MUST_BE_SECOND_ARG

Possible Cause: For the Click command, you have placed the -X and -Y arguments before -Raw.

Action: If you use -Raw, place it as the first argument.

-299 BROKER_DISALLOWED_REPEATS_EXIST

Possible Cause: You have tried to use repeated characters in a password, but a password policy doesn’t allow them.

Action: Avoid repeated characters.

-300 BROKER_DISALLOWED_SEQUENTIALS_EXIST

Possible Cause: You have tried to use sequential characters in a password, but a password policy doesn’t allow them.

Action: Avoid sequential characters.

-301 BROKER_DISALLOWED_KEYBOARD_ADJACENTS_EXIST

Possible Cause: You entered a password that has an unacceptable sequence of characters.

Action: Enter an approved sequence of characters.

-303 BROKER_CHARACTER_NOT_IN_REQUIRED_POSITION

Possible Cause: You entered a password that doesn’t have a character in a required position.

Action: Enter the password correctly.

-308 BROKER_BAD_POSITION_ARGUMENT

Possible Cause: While calling a SetCursor command, you tried to move the cursor to an invalid position (for example, out of the terminal session's boundary).

Action: Specify a valid position.

-309 BROKER_ERROR_CONVERTING_POSITION

Possible Cause: The conversion from -X and -Y coordinates for the SetCursor command has failed.

Action: Specify the -X and -Y coordinates for one offset from the top left-hand corner of the screen.

-310 BROKER_NOT_A_WRITEABLE_VARIABLE

Possible Cause: You tried to save a new value to type of variable that can't be written to.

Action: Use a runtime or normal variable.

-314 BROKER_COPY_BACKUP_FAILED

Possible Cause: When SecureLogin begins to update the cache file, SecureLogin first copies the current cache file to a file with the same name but uses the extension .good. SecureLogin was unable to copy the file. The .good file is already open because another process is using it.

Action: Close the process and try again.

Possible Cause: You don't have rights to create files in the directory.

Action: Ask the administrator to assign you rights to the directory.

-315 BROKER_GOTO_LABEL_ALREADY_DEFINED

Possible Cause: You have used a GoTo command, but the label that you directed it to has already been used.

Action: Remove the second label command.

-316 BROKER_GOTO_LABEL_NOT_DEFINED

Possible Cause: You have used a GoTo command, but the label that you directed it to hasn't been defined.

Action: Define the label.

-317 BROKER_INCORRECT_DATABASE_VERSION

Possible Cause: The version of SecureLogin that you are using doesn't handle the version of SecureLogin that is stored in the directory.

Action: Upgrade to the latest version of SecureLogin.

-318 BROKER_DIRECTORY_CRC_DOES_NOT_MATCH

Possible Cause: Whenever SecureLogin stores an entry in the directory, SecureLogin employs a redundancy check. If the redundancy check doesn't match when SecureLogin reloads the entry, the data in the directory is unusable.

Action: Troubleshoot the directory.

-319 BROKER_DISALLOWED_DUPLICATES_EXIST

Possible Cause: You entered a password that has unacceptable duplicate characters.

Action: Enter the password correctly.

-321 BROKER_SUBROUTINE_NOT_DEFINED

Possible Cause: A Call command is calling a subroutine that hasn't yet been defined.

Action: Define the subroutine.

-325 BROKER_ENTRY_MUST_HAVE_NON_NULL_KEY

Possible Cause: You tried to add a script or variable that is a blank string.

Action: Provide a name for the script or variable.

-326 BROKER_VARIABLE_REQUIRED

Possible Cause: Some commands (for example, ReadText) require a variable to copy the data that they are returning to. The argument must be a variable but isn't.

Action: Change the argument to a variable.

-327 BROKER_OBJECT_NOT_FOUND

Possible Cause: LDAP or Active Directory* can't locate the User object in the directory.

Action: Troubleshoot the directory.

-328 BROKER_ADS_MEMORY_FAILURE

Possible Cause: The Active Directory library was unable to allocate memory.

Action: Close one or more applications and try again.

-329 BROKER_ADS_ERROR_GETTING_ATTRIBUTE

Possible Cause: Although data exists in Active Directory, SecureLogin is unable to read the data.

Action: Troubleshoot Active Directory.

-330 BROKER_ADS_INSUFFICIENT_RIGHTS_TO_DELETE

Possible Cause: When you removed a script, SecureLogin tried to delete part of an attribute from Active Directory. However, you are unable to delete the attribute because you don't have sufficient rights to Active Directory.

Action: The administrator must assign sufficient Active Directory rights for each user so that the user can modify SecureLogin attributes.

-331 BROKER_ADS_ERROR_DELETING_VALUE

Possible Cause: Active Directory was unable to delete a value.

Action: Troubleshoot Active Directory.

-332 BROKER_NO_PASSWORD_FIELD_VARIABLE_IN_SCRIPT

Possible Cause: A Web script must have at least one Type command that has “password” as the second argument. The following lines illustrate a typical script:

```
Type $Username
Type $Password Password.
```

However, the script has no Type command followed by the Password attribute.

Action: Add a Type command followed by the Password attribute.

-333 BROKER_REGEX_GET_REPLACE_STRING_FAILED

Possible Cause: On the RegSplit command, the string that you are running through the regular expression didn’t match.

Action: Change the regular expression.

-335 BROKER_REGEX_COMPILE_FAILED

Possible Cause: The syntax of the regular expression was incorrect.

Action: Revise the syntax of the regular expression.

-336 BROKER_DIRECTORY_AUTH_DATA_CORRUPT

Possible Cause: There is a problem with the Prot:SSOAuth data attribute.

Action: Call Novell Technical Services.

-340 BROKER_UNKNOWN_DATABASE_VERSION

Possible Cause: You are using an earlier version of SecureLogin.

Action: Upgrade to the latest version of SecureLogin.

-349 BROKER_UNABLE_TO_FIND_SESSION_FILE

Possible Cause: Terminal Launcher couldn’t find a session file for an emulator.

Action: Configure Terminal Launcher to have the correct path to the file for the emulator session.

-353 BROKER_RECURSIVE_SCRIPT_INCLUDE_DETECTED

Possible Cause: While using the Include command, you included a script twice.

Action: Only include a script once.

-354 BROKER_NETWORK_PASSWORD_INCORRECT

Possible Cause: You have turned on the option to prompt the user for the network password before the user can access options on the task bar. The user entered an incorrect password.

Action: Enter the correct password.

-356 BROKER_INVALID_CHARACTER_FOUND_IN_STARTUP_ID_LIST

Possible Cause: For generic emulators, you specify the startup control ID. A comma must separate a list of numbers. You have used a character other than a comma.

Action: Remove unacceptable characters.

-361 BROKER_NMAS_DLL_NOT_AVAILABLE

Possible Cause: SecureLogin can't load the .dll file for NMAS, for use with the AAVerify command.

Action: To use features for AAVerify, install NMAS.

-362 BROKER_NMAS_LEGACY_RELOGIN_NOT_FOUND

Possible Cause: SecureLogin couldn't find the NMAS relogin function in the .dll for NMAS.

Action: Install the latest version of NMAS.

-363 BROKER_STANDARD_VARIABLE_REQUIRED

Possible Cause: The command requires a $ variable. However, you provided a ? variable.

Action: Provide a $ variable.

-365 BROKER_LDAP_INIT_FAILED

Possible Cause: The initialization of the LDAP SSL layer failed.

Action: Contact Novell Technical Services.

-372 BROKER_ACCESS_IS_DENIED

Possible Cause: For LDAP, you don't have rights to the part of the directory that you are trying to access.

Action: Grant users the correct rights.

-373 BROKER_HLLAPI_CONNECT_FAILED

Possible Cause: Terminal Launcher was unable to connect to the emulator.

Action: Make sure that the emulator has HLLAPI enabled.

-375 BROKER_NOT_RUNNING_NT

Possible Cause: Although you aren't running NT, you tried to use a feature that is only available through NT.

Action: Don't use that feature unless you are running NT.

-380 BROKER_HLLAPI_NOT_CONNECTED_TO_PS

Possible Cause: Terminal Launcher tried to use a HLLAPI function. However, the hllapi.dll is not connected to the emulator presentation space.

Action: Make sure that Terminal Launcher is set up correctly with the emulator.

-381 BROKER_HLLAPI_SPECIFYING_PARAMETERS_ERROR

Possible Cause: Incorrect parameters were given to a command that uses a HLLAPI function.

Action: Contact Novell Technical Services.

-382 BROKER_HLLAPI_INVALID_PS_POSITION

Possible Cause: An attempt was made to move the cursor or read text from an invalid (out of bounds) position on the emulator presentation space.

Action: Correct the positioning parameter in the script.

-383 BROKER_HLLAPI_SYSTEM_ERROR

Possible Cause: Terminal Launcher is not configured correctly for the emulator.

Action: Make sure that Terminal Launcher is set up correctly with the emulator and that the emulator correctly supports HLLAPI.

-384 BROKER_HLLAPI_PS_BUSY_ERROR

Possible Cause: A HLLAPI function is being called while the emulator presentation space is unavailable.

Action: Make sure that the emulator is not being used by other HLLAPI applications.

-385 BROKER_HLLAPI_INPUT_REJECTED

Possible Cause: The emulator rejected an attempt to input data into the emulator presentation space.

Action: Make sure that the emulator presentation space is not locked.

-386 BROKER_HLLAPI_ERROR_QUERYING_SESSIONS

Possible Cause: SecureLogin is unable to query available HLLAPI sessions.

Action: Make sure that Terminal Launcher is set up correctly with the emulator.

-387 BROKER_LAST_NDS_USER_NOT_FOUND

Possible Cause: The last eDirectory User object, as stored in the registry, could not be read for use in an NMAS login.

Action: Make sure that the last eDirectory user is stored correctly in the registry.

-388 BROKER_LAST_NDS_USER_UNWORTHY

Possible Cause: The last eDirectory User object, as stored in the registry, was not in the correct format. An NMAS login was unable to use the format.

Action: Make sure that the last eDirectory User object is stored correctly in the registry.

-389 BROKER_NMAS_DISCONNECTED_LOGIN_NOT_FOUND

Possible Cause: The NMAS disconnected login function was not found in nmas.dll.

Action: Make sure that the correct nmas.dll is installed.

-390 BROKER_LDAP_SSL_INIT_FAILED

Possible Cause: SecureLogin could not initialize the LDAP SSL libraries.

Action: Call Novell Technical Services.

-391 BROKER_LDAP_SSL_ADD_CERT_FAILED

Possible Cause: SecureLogin could not open the certificate you supplied for LDAP over SSL. Either the file doesn't exist or it is in the incorrect format.

If the certificate file specified ends in .der, SecureLogin uses Distinguished Encoding Rules (DER) format. Otherwise SecureLogin uses B64 format.

Action: Make sure that the path to the certificate is correct and that it is in DER format.

-392 BROKER_BUILTIN_VARIABLE_NOT_FOUND

Possible Cause: A built-in variable such as ?sysversion was not found.

Action: Make sure that the variable name is correct.

-394 BROKER_LDAP_PASSWORD_INCORRECT

Possible Cause: The password supplied to login to LDAP was incorrect.

Action: Check the password.

-395 BROKER_LDAP_USER_NON_EXISTENT

Possible Cause: The username that you used to log in to LDAP does not exist.

Action: Make sure that the username exists in the directory and that the LDAP context is correct.

-396 BROKER_LDAP_SERVER_DETAILS_INCORRECT

Possible Cause: One or more of the LDAP server parameters supplied was incorrect.

Action: Check the LDAP server address and port number.

Action: Make sure that the LDAP server you are connected to is running.

-399 BROKER_DIVIDE_BY_ZERO_IS_BAD

Possible Cause: Using the Divide command, you attempted division by zero.

Action: Don't attempt to divide by zero.

-400 BROKER_WRONG_SECTION_NAME

Possible Cause: You manually edited a wizard-generated script.

Action: When editing a script, don't edit the specially generated comments. Only edit the actual commands. If this error occurs, you will no longer be able to use the wizard for that script.

-401 BROKER_INVALID_GLOBAL_WIZARD_CONFIG

Possible Cause: You manually edited a wizard-generated script.

Action: When editing a script, don't edit the specially generated comments. Only edit the actual commands. If this error occurs, you will no longer be able to use the wizard for that script.

-402 BROKER_LDAP_ATTRIBUTE_DOES_NOT_EXIST_IN_SCHEMA

Possible Cause: You are running LDAP on eDirectory, but you have not correctly mapped the LDAP attributes.

Action: Check your LDAP attribute mappings. See "Installing in LDAP Environments" in the *Nsure SecureLogin 3.51.2 Installation Guide*.

Possible Cause: You are running LDAP on a platform other than eDirectory. However, the schema is not extended for that platform.

Action: Extend the LDAP schema.

-403 BROKER_AAVERIFY_DLL_NOT_AVAILABLE

Possible Cause: SecureLogin was unable to load sl_aaverify.dll.

Action: Make sure that you have the correct .dll files installed for AAVERIFY.

-404 BROKER_AAVERIFY_FUNCTION_NOT_FOUND

Possible Cause: You are using the incorrect version of sl_aaverify.dll.

Action: Check the version of sl_aaverify.dll.

-405 BROKER_AAVERIFY_CONSISTENCY_FAILURE

Possible Cause: You are using the incorrect version of sl_aaverify.dll.

Action: Check the version of sl_aaverify.dll.

-406 BROKER_AAVERIFY_ERROR

Possible Cause: You are using the incorrect version of sl_aaverify.dll.

Action: Check the version of sl_aaverify.dll.

-410 BROKER_NOT_A_STRING_ATTRIBUTE

Possible Cause: You are using % variables, but the attribute you are reading is not a plain string attribute (SYN_CE_STRING or SYN_CI_STRING on eDirectory).

Action: Check the schema a definition of the attribute to confirm that the syntax is SYN_CE_STRING or SYN_CI_STRING.

-411 BROKER_LDAP_INVALID_DN_SYNTAX

Possible Cause: The format of your LDAP username was invalid.

Action: Check the format of the username that you entered.

-412 BROKER_INVALID_OPTION_COMBINATION

Possible Cause: An invalid combination of options was passed to a script command. For example, you passed -Right and -Raw to the Click command.

Action: Review the documentation for the script command.

-413 BROKER_AAVERIFY_SLOGIN_DOES_NOT_EXIST

Possible Cause: Sl_aaverify.dll generates these errors. There is a problem connecting to the SecureLogin server.

Action: Troubleshoot service location problems by reviewing documentation on SecureLogin Advanced Authentication.

-414 BROKER_AAVERIFY_ERR_SLOGIN_NOT_RUNNING

Possible Cause: Sl_aaverify.dll generates these errors. There is a problem connecting to the SecureLogin server

Action: Troubleshoot service location problems by reviewing documentation on SecureLogin Advanced Authentication.

-415 BROKER_AAVERIFY_ERR_LOAD_LIB_SLPAM

Possible Cause: Sl_aaverify.dll generates these errors. There is a problem connecting to the SecureLogin server.

Action: Troubleshoot service location problems by reviewing documentation on SecureLogin Advanced Authentication.

-416 BROKER_WI_GETEXENAME_ERR

Possible Cause: The wizard was unable to retrieve the executable name for the window you selected.

Action: For this application, don't use the wizard.

-417 BROKER_ADS_PUT_OCTET_INSUFFICIENT_RIGHTS

Possible Cause: You don't have sufficient rights to ADS to perform the current operation.

Action: Ask the ADS administrator to assign you additional ADS rights.

-418 BROKER_ADS_CLR_OCTET_INSUFFICIENT_RIGHTS

Possible Cause: You do not have sufficient rights to ADS to perform the current operation.

Action: Ask the ADS administrator to assign you additional ADS rights.

-423 BROKER_ERROR_INITIALIZING_DATA_STORES

Possible Cause: SecureLogin was unable to initialize either the primary or secondary datastore.

-424 BROKER_UNABLE_TO_LOAD_SLOTP_DLL

Possible Cause: Slotp.dll could not be loaded. This .dll file is required for synchronizing one-time passwords to LDAP directories.

Action: Review documentation for one-time passwords.

-425 BROKER_LDAP_NO_SUCH_ATTRIBUTE

Possible Cause: You have used a % variable on LDAP. However, the requested attribute does not exist.

Action: Check the spelling of the attribute name against the LDAP schema.

-426 BROKER_SYS_VARIABLE_NOT_AVAILABLE

Possible Cause: A system variable (for example, ?syspassword) was requested but was not available. slinac.dll or slnmas.dll must be correctly installed for these variables to function.

Action: Make sure that either slinac.dl or slnmas.dll is installed.

-430 BROKER_MUST_BE_CALL_OR_GOTO

Possible Cause: When using the OnException command, the second parameter must be either Call or GoTo.

Action: Check the script documentation for OnException.See "OnException/ClearException" in the *Nsure SecureLogin 3.51.2 Scripting Guide*.

-442 BROKER_CHAR_UCASE_NOT_IN_REQUIRED_POSITION

Possible Cause: A password doesn't have an upper-case character in a position where the password policy code requires one.

Action: Make sure that the password complies with the password policy.

-443 BROKER_CHAR_LCASE_NOT_IN_REQUIRED_POSITION

Possible Cause: A password doesn't have a lower-case character in a position where the password policy code requires one.

Action: Make sure that the password complies with the password policy.

-444 BROKER_PUNCTUATION_NOT_IN_REQUIRED_POSITION

Possible Cause: A password doesn't have a punctuation character in a position where the password policy code requires one.

Action: Make sure that the password complies with the password policy.

- 2147016656 Error opening specified object

Possible Cause: Active Directory code error message (value 0x80072030): There is no such object on the server.

Action: You have entered an incorrect object or container definition when assigning user rights. Re-enter the correct object or container definition.

Other Error Codes

Most likely, you won't see the following error codes. If you do encounter one, call Novell Technical Services.

- -101 BROKER_NO_MORE_COMMANDS
- -105 BROKER_REMOVE_ENTRY_FAILED
- -106 BROKER_UPDATE_GET_ENTRY_FAILED
- -110 BROKER_NO_MORE_PLATFORMS
- -111 BROKER_NO_MORE_VARIABLES
- -120 BROKER_INVALID_PREF_DATA_TYPE
- -121 BROKER_PREFERENCE_DATA_CORRUPT
- -122 BROKER_TARGET_ENTRY_LIST_NOT_LOADED
- -129 BROKER_ENTRY_LIST_NOT_NULL
- -130 BROKER_ENTRY_LIST_NULL
- -132 BROKER_SYM_LIST_NULL
- -141 BROKER_PREF_INVALID
- -142 BROKER_SET_PREF_INVALID

- -173 BROKER_NO_MORE_CACHE_FILE_DATA
- -177 BROKER_PUBLIC_KEY_HAS_CHANGED
- -195 BROKER_FILE_TRAITS_OP_NOT_IMPLEMENTED
- -196 BROKER_DUMMY_OP_NOT_IMPLEMENTED
- -200 BROKER_END_OF_SCRIPT
- -206 BROKER_BREAK_BLOCK
- -207 BROKER_END_SCRIPT_NOW
- -210 BROKER_CORPORATE_MOD_ABORTED
- -213 BROKER_NDS_OP_NOT_IMPLEMENTED
- -214 BROKER_UNABLE_TO_GET_CURRENT_OU
- -221 BROKER_HLLAPI_OBJECT_UNINITIALZED
- -223 BROKER_HLLAPI_OBJECT_ALREADY_INITIALIZED
- -231 BROKER_AUTH_CANCEL
- -234 BROKER_FREE_PLATFORM_SCRIPT_NULL_PTR
- -235 BROKER_VBA_LOGIN_INTERFACE_NOT_IMPLEMENTED
- -253 BROKER_NT_FILE_TRAITS_OP_NOT_IMPLEMENTED
- -260 BROKER_NO_DATA_STORES_LOADED
- -263 BROKER_DDE_LOGIN_INTERFACE_NOT_IMPLEMENTED
- -285 BROKER_EMULATOR_INFO_NOT_FOUND
- -286 BROKER_RELOAD_NOT_ENABLED
- -287 BROKER_TERMINAL_CONNECT_TRY_AGAIN
- -289 BROKER_WRONG_OBJECT_TYPE
- -292 BROKER_DLL_NOT_INITIALIZED
- -297 BROKER_PARSER_ELSE_STATEMENT_FOUND
- -311 BROKER_RUN_SCRIPT_AGAIN
- -312 BROKER_NO_OU_PERIOD_FOUND
- -320 BROKER_GOTO_LIST_ASSERTION
- -322 BROKER_UNABLE_TO_FIND_PASSWORD_FIELD
- -323 BROKER_PASSWORD_FIELD_STYLE_NOT_SET
- -324 BROKER_WEB_ACTION_NOT_SUPPORTED
- -337 BROKER_DES_KEY_NOT_SET
- -338 BROKER_DES_INVALID_BLOCK_LEN
- -339 BROKER_INVALID_ENCRYPTION_TYPE
- -341 BROKER_USER_KEY_NOT_SET
- -343 BROKER_PRIMARY_KEY_DECRYPT_FAILED
- -344 BROKER_SECONDARY_KEY_DECRYPT_FAILED

- -345 BROKER_MERGE_WRONG_ENTRY_TYPE
- -348 BROKER_PASSWORD_RESET_DETECTED
- -352 BROKER_AUTH_DATA_INCORRECT
- -355 BROKER_USER_ABORTED_LOAD_PROCESS
- -357 BROKER_ERROR_REG_CACHE_NO_DETAILS
- -358 BROKER_ERROR_REG_CACHE_SAVE_FAILED
- -359 BROKER_ERROR_REG_CACHE_SPLIT
- -360 BROKER_PASSWORD_VARIABLE_NOT_ALLOWED
- -364 BROKER_LDAP_LOGIN_CANCELLED
- -367 BROKER_REG_AUTH_CACHE_MISMATCH
- -368 BROKER_LDAP_TOKEN_DELETED
- -369 BROKER_CRED_LIST_NOT_NULL
- -370 BROKER_CRED_LIST_NULL
- -371 BROKER_NO_MORE_CRED_SETS
- -374 BROKER_DUPLICATE_ENTRIES_EXIST
- -376 BROKER_WINNT_CACHE_AUTH_REG_FAILED
- -377 BROKER_WINNT_CACHE_AUTH_REG_WRONG_USER.
- -378 BROKER_INVALID_PIPE_STRING_FOUND
- -379 BROKER_HEX_LENGTH_INCORRECT
- -398 BROKER_WIZ_CP_WRONG_SCRIPT_TYPE
- -408 BROKER_DES_KEY_DATA_CORRUPT
- -409 BROKER_OPERATION_ABORTED_BY_USER
- -420 BROKER_SLAASSO_ERR_CRYPTO_KEY_NOT_SET
- -421 BROKER_SLAASSO_ERR_UNKNOWN_DATA.
- -422 BROKER_SLAASSO_OUT_OF_MEMORY
- -427 BROKER_USERNAME_UNSUITABLE_FOR_READING_SLINA_CREDS
- -428 BROKER_NO_EXCEPTION_HANDLER_DEFINED
- -429 BROKER_EXCEPTION_RAISED