

Novell Nsure™ SecureLogin

3.51

www.novell.com

ADMINISTRATION GUIDE

April 22, 2004



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 export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2002-2003 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Nsure SecureLogin 3.51 Administration Guide
[April 22, 2004](#)

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

Novell Trademarks

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

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

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

eDirectory is a trademark of Novell, Inc.

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

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

MyRealBox is a service mark of Novell, Inc.

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

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

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

Novell Application Launcher is a trademark of Novell, Inc.

Novell Client is a trademark of Novell, Inc.

NMAS is a trademark of Novell, Inc.

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

Nsure is a trademark of Novell, Inc.

Third-Party Trademarks

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

Contents

About This Guide	9
1 Overview: Single Sign-On	11
SecureLogin As a Solution	11
Understanding SecureLogin	12
SecureLogin Architecture	12
Script Language	12
SecureLogin Components	13
What's New	18
2 Managing SecureLogin	19
Accessing Management Tools	19
Accessing SecureLogin in ConsoleOne	19
Accessing SecureLogin from MMC	21
Accessing SecureLogin from SecureLogin Manager	23
Managing User IDs	24
Creating User IDs	24
Editing User IDs	28
Deleting User IDs	28
Managing Applications	28
Adding Applications for Single Sign-On	29
Editing Scripts	32
Modifying Settings for Applications	33
Managing Password Policies	34
Creating or Editing a Password Policy	34
Allowable Punctuation Characters	37
Using Password Policies in Scripts	38
Setting the Default Domain Policy	41
Managing Administrative and User Settings	41
Understanding the Configuration Hierarchy	41
Configuring SecureLogin Settings	41
Using SecureLogin with Client Software	52
Copying, Exporting, and Importing SecureLogin Settings	53
Copying SecureLogin Settings	53
Exporting SecureLogin Settings	54
Importing SecureLogin Settings	55
Setting Up Multiple IDs for an Application	56
Defining Applications That SecureLogin Detects	58
Changing the Startup Order of Applications	60
Using the Startup Group	60
Using Startup Scripts	60
Using Novell Application Launcher to Start Applications	61
3 Using SecureLogin	63
Accessing SecureLogin's Main Window	63
Using the SecureLogin Icon	64

Adding Applications	65
Responding to Pop-Up prompts	65
Manually Adding Applications	67
Using Prebuilt Scripts	67
Adding a Windows Application.	71
Adding a Web Application	74
Adding a Java Application	76
Linking User IDs to Applications.	78
Changing Settings	79
Disabling the Workstation's Cache	79
Toggling the Active Setting	80
Changing Your Passphrase	80
4 Using Login Watcher	83
5 Working with Terminal Emulators	85
Terminal Launcher	85
Setting Up Terminal Emulation	86
Creating a SecureLogin Script	86
Configuring Terminal Launcher	88
Creating a Login for an Emulator	102
Setting Up a Shortcut	104
Command Line Parameters Used in Terminal Launcher	104
Configuring Backup Sessions	106
Determining Which Session File To Automatically Use	106
Using Terminal Launcher With Non-HLLAPI-Compliant Emulators	107
6 Troubleshooting SecureLogin	113
Interoperability Issues	113
SecureLogin and iChain	113
First-Time Login to DEX 4.1 Portal Services.	113
Integrating with BorderManager's Java Applet for Proxy Authentication	114
Clearing Object Data	115
Rights in Active Directory	116
Assigning Rights to User Objects	116
Assigning User Rights to an Organizational Unit	117
Frequently Asked Questions	118
Changing the Startup Order	118
Entering a Passphrase.	118
No User ID	118
No Passphrase Policies on Windows NT Domains	118
Can't Log In Again to a Web Site	118
Scripts for Web Sites	119
System Tray Icon Stays Active	119
Novell SecureLogin Is Missing from the Program Group	119
No Attribute Mapping Tab	119
Terminal Launcher Doesn't Run	120
Can't View Shadow Variables	120
Error Codes for LDAP	121
Resolving Error -426.	121
Resolving Error -602.	121
Resolving Error -672.	121
Resolving Error -1644	122
Error Parsing Line	122
Program Conflict	122
Useful TIDs	123

A	Prebuilt Scripts	125
B	MS Terminal Server and Citrix MetaFrame Environments	127
C	Finding Control IDs and Offsets of an Emulator	129
	Finding Input and Output IDs	129
	Setting Up Winspector	129
	Viewing Control ID Numbers	135
	Using Alternatives to Control ID Numbers	136
	Finding Offsets	137
D	Finding HLLAPI Types	141
	Using Header Files	141
	Using Dependency Walker	141
E	Error Codes	145
	Error Codes with Tips.	145
	Getting Help from Novell Technical Services.	163
F	Documentation Updates	167
	December 11, 2003.	167
	February 10, 2004	167
	April 22, 2004.	168

About This Guide

This guide for network administrators provides information on the following:

- ♦ Chapter 1, “Overview: Single Sign-On,” on page 11
- ♦ Chapter 2, “Managing SecureLogin,” on page 19
- ♦ Chapter 3, “Using SecureLogin,” on page 63
- ♦ Chapter 4, “Using Login Watcher,” on page 83
- ♦ Chapter 5, “Working with Terminal Emulators,” on page 85
- ♦ Chapter 6, “Troubleshooting SecureLogin,” on page 113
- ♦ Appendix A, “Prebuilt Scripts,” on page 125
- ♦ Appendix B, “MS Terminal Server and Citrix MetaFrame Environments,” on page 127
- ♦ Appendix E, “Error Codes,” on page 145

Additional Documentation

For documentation on installing SecureLogin or migrating secrets from earlier versions, see the [Nsure SecureLogin 3.51 Installation Guide](#).

For documentation on scripting commands and example scripts for applications, see the [Nsure SecureLogin 3.51 Scripting Guide](#).

For documentation on terminal services, see the [Nsure SecureLogin 3.51 Terminal Services Guide](#).

For documentation on configuring Terminal Launcher for selected terminal emulators, see [Nsure SecureLogin 3.51 Configuration Guide for Terminal Emulation](#).

For documentation on Novell® SecretStore®, see the [Novell SecretStore 3.3.0 Administration Guide](#).

Documentation Updates

For the most recent version of the *Novell SecureLogin 3.51 Administration Guide*, see [SecureLogin \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) at the Novell Documentation Web page.

Documentation Conventions

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

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

1

Overview: Single Sign-On

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

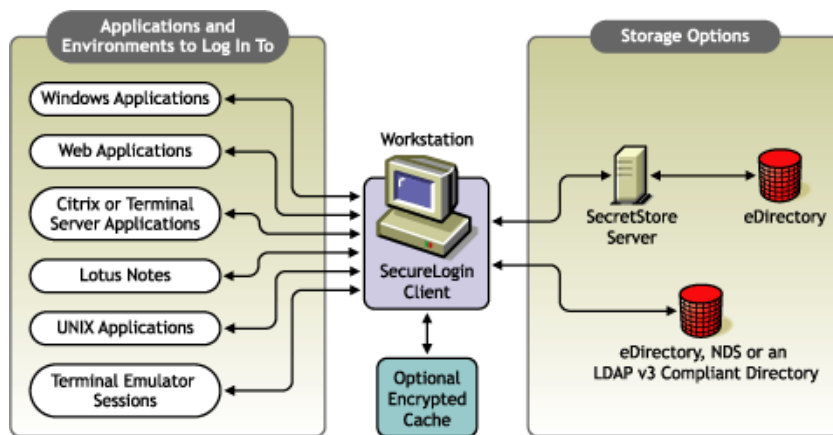
- ♦ Log in from anywhere and get the same capabilities as if they were at their own desks.

- ◆ 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® and Active Directory.

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:

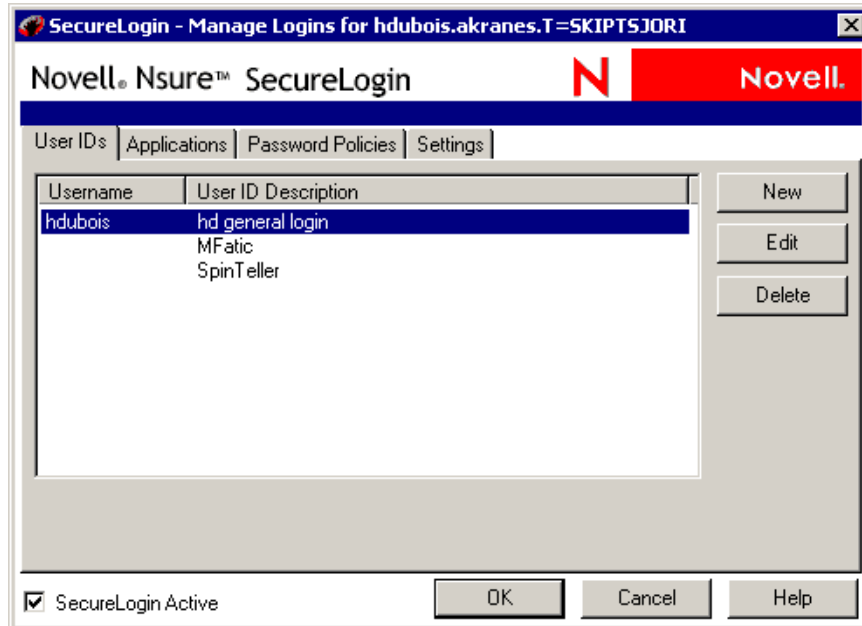
- ◆ Workstation Administration
- ◆ Container and User object snap-ins
- ◆ Terminal Launcher
- ◆ Window Finder
- ◆ Login Watcher

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
- ◆ 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:



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 system tray.



Terminal Launcher

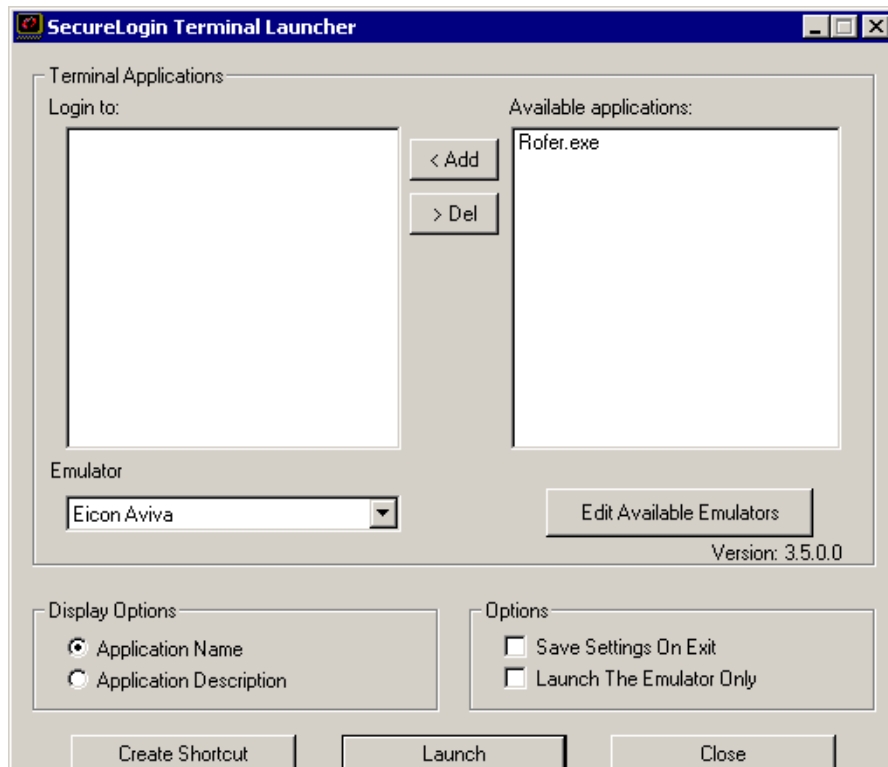
Terminal Launcher enables you to log into any type of host that requires a user to log in using an emulator (for example, an ACF2 or RACF mainframe, a UNIX host, or a Cisco* router). Either you or the user configures Terminal Launcher to connect to the mainframe or host, wait for the login sequence,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



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

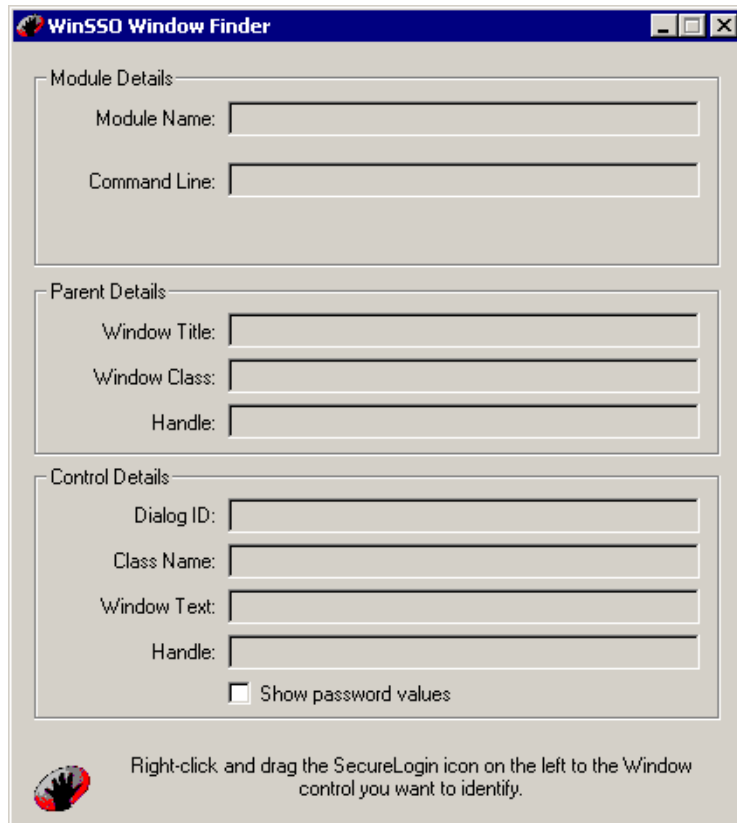
Taking advantage of the directory architecture, SecureLogin allows users to roam with their authentication details. Because there are no workstation dependencies, users can move freely from office to office. Their credentials follow them.

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:



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.

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 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 to which SecureLogin authenticates.

What's New

SecureLogin 3.51 includes the following new features:

- ◆ Complete and Custom installation options for Novell eDirectory, LDAP, Active Directory, NT/2000/2003, and standalones
- ◆ An automate.ini option, so that you can customize installations before distributing SecureLogin for installs
- ◆ A redesigned user interface, which incorporates recommendations from customers
- ◆ Increased support for moving User objects and for administratively resetting passwords
- ◆ A non-Novell LDAP client that acts as a GINA, credential manager, and a network provider
- ◆ Using NMAST[™] advanced authentication
- ◆ Java[®] application support for Swing/AWT standard applications
- ◆ Advanced Windows Scripting, to handle secondary logins
- ◆ Support for one-time passwords

2

Managing SecureLogin

You can manage Novell® SecureLogin by using any of the following:

- ♦ The SecureLogin client

Each workstation running SecureLogin has a SecureLogin client. This client can only alter the current user's SecureLogin information.

- ♦ The SecureLogin snap-in to ConsoleOne®, installed on a workstation
- ♦ The Microsoft Management Console (MMC), which runs on a Windows server
MMC is installed with Active Directory.
- ♦ SecureLogin Manager (slmanager.exe)

You use the same processes at the workstation as from the server.

This section provides information on the following:

- ♦ “Accessing Management Tools” on page 19
- ♦ “Managing User IDs” on page 24
- ♦ “Managing Applications” on page 28
- ♦ “Managing Password Policies” on page 34
- ♦ “Managing Administrative and User Settings” on page 41
- ♦ “Using SecureLogin with Client Software” on page 52
- ♦ “Copying, Exporting, and Importing SecureLogin Settings” on page 53
- ♦ “Setting Up Multiple IDs for an Application” on page 56
- ♦ “Defining Applications That SecureLogin Detects” on page 58
- ♦ “Changing the Startup Order of Applications” on page 60

Accessing Management Tools

To manage SecureLogin, you can use the SecureLogin snap-in to ConsoleOne, MMC, or slmanager.exe. The same functionality exists in the three tools.

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.

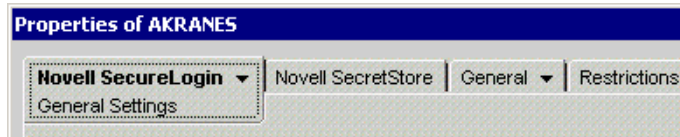
For information on these tasks see “SecureLogin on Novell eDirectory” in the [Nsure SecureLogin 3.51 Installation Guide](#).

To access SecureLogin in ConsoleOne:

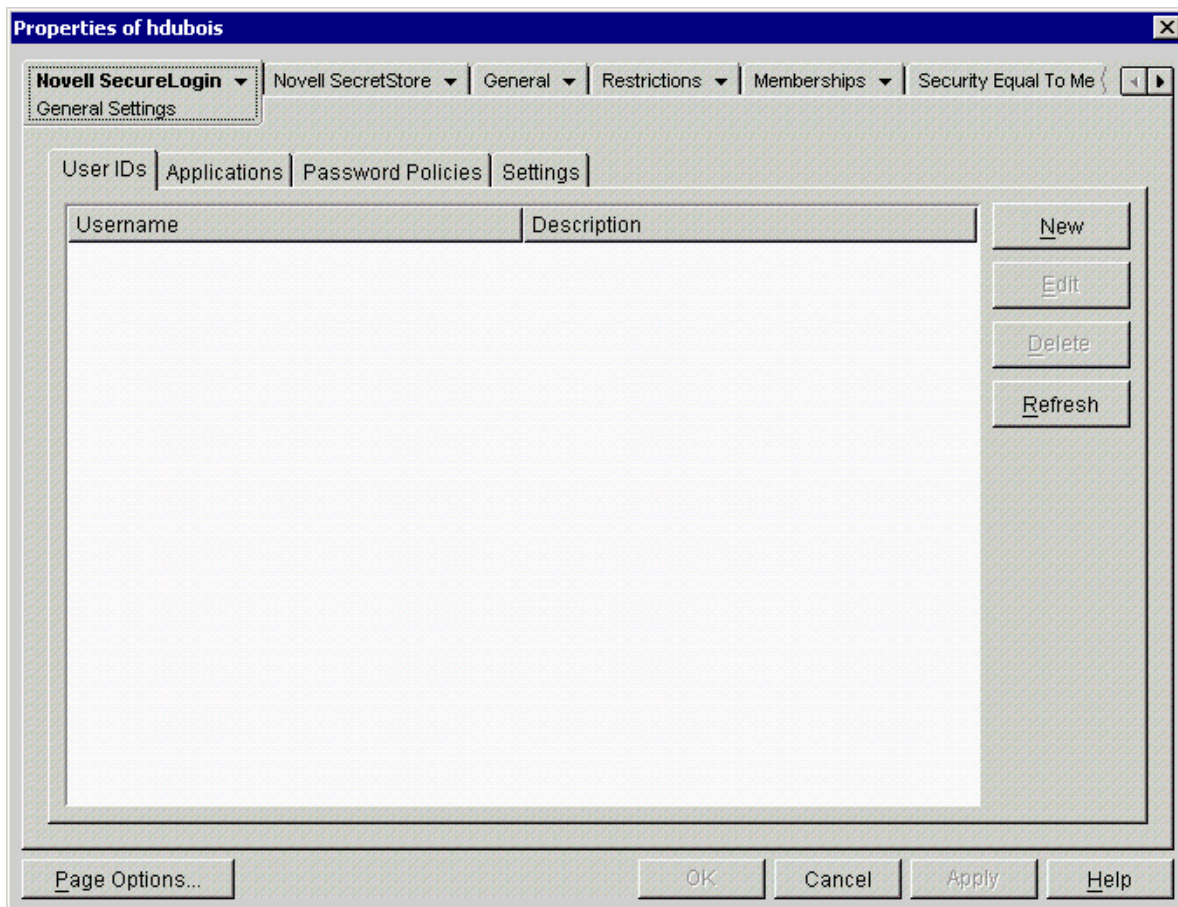
- 1 Run consoleone.exe.

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 management options that are available on SecureLogin's main page in ConsoleOne:



Accessing SecureLogin from MMC

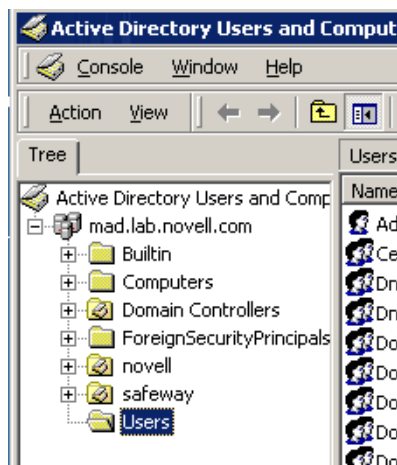
Before you can access MMC, you must complete the following tasks:

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

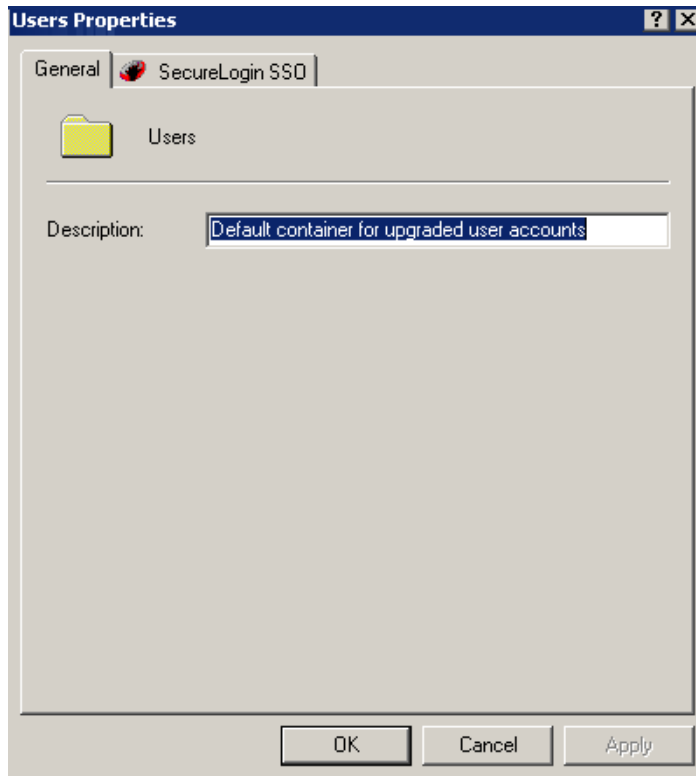
For information on these tasks, see [“SecureLogin on Active Directory”](#) in the [Nsure SecureLogin 3.51 Installation Guide](#).

To access SecureLogin:

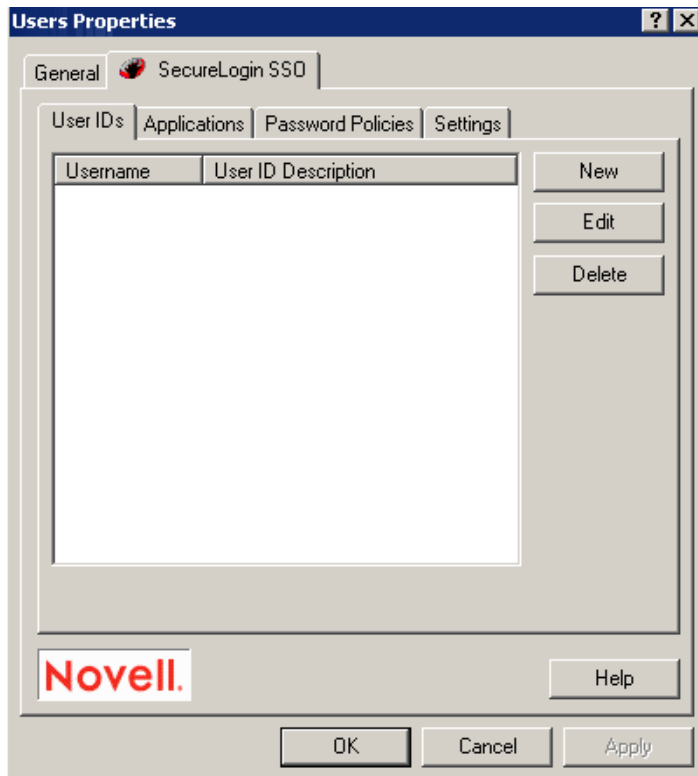
- 1** Click Start > Programs > Administrative Tools > Active Directory Users and Computers.
- 2** In the Active Directory Users and Computers pane, right-click an organizational unit (for example, Users).



- 3** Click Properties, then click SecureLogin SSO.



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, and manage settings.



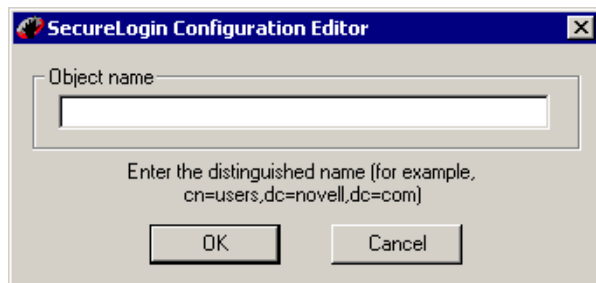
Accessing SecureLogin from SecureLogin Manager

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.



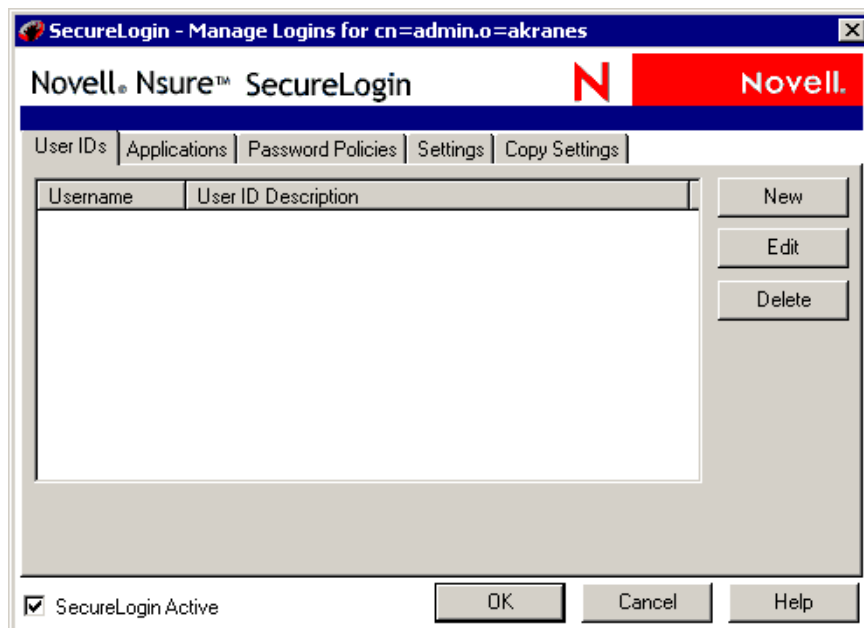
- 2 Log in as administrator.

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=admin.o=akranes`

The following figure illustrates SecureLogin Manager's main page:



Managing User IDs

A user ID consists of whatever is required of a user to authenticate to a network or directory. For example, authentication might require a password and PIN. 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.

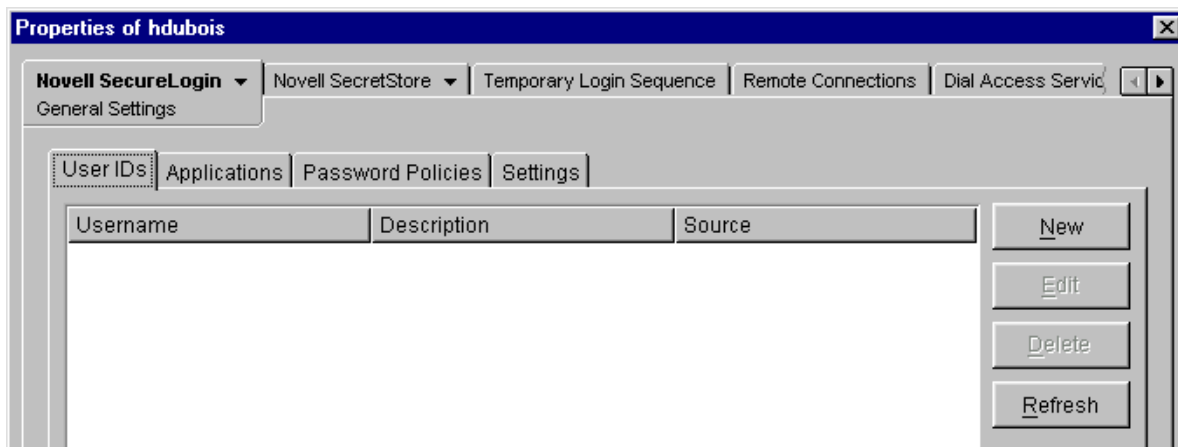
You manage user IDs by using the SecureLogin snap-in to ConsoleOne, Active Directory Users and Computers in MMC, SecureLogin Manager, or the SecureLogin workstation client.

Using the User ID tab of the object or user properties, you can define a user ID that several different applications can share. For example, gmail.novell.com and grpwise.exe can both use the GroupWise user ID.

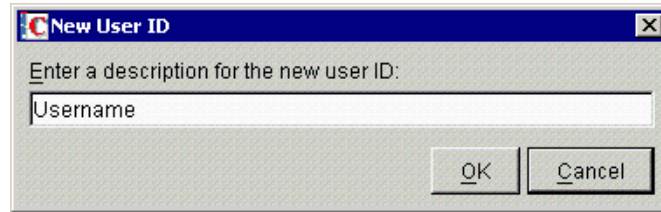
Creating User IDs

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.



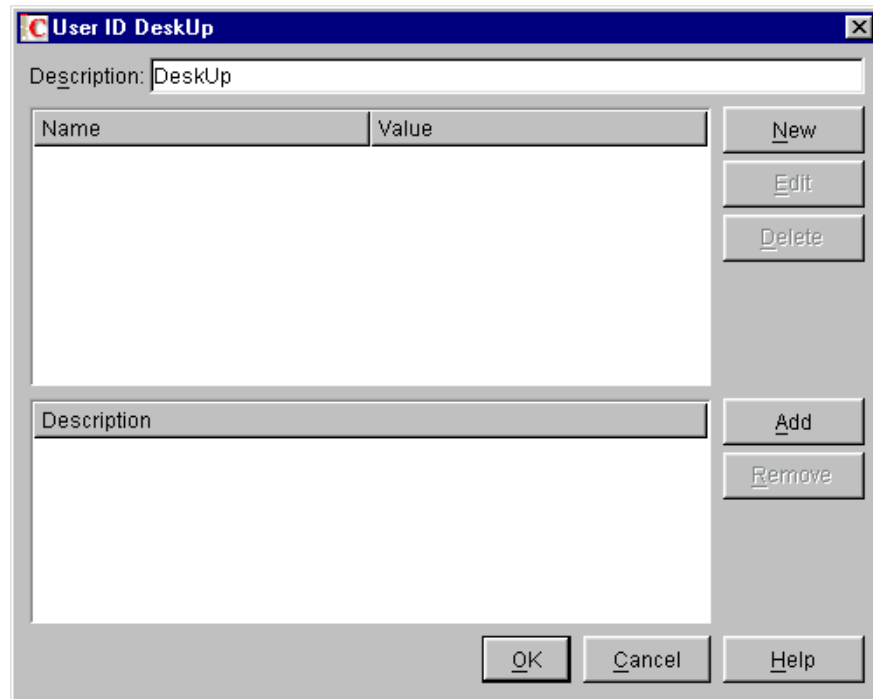
Adding a Username Variable and Value

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

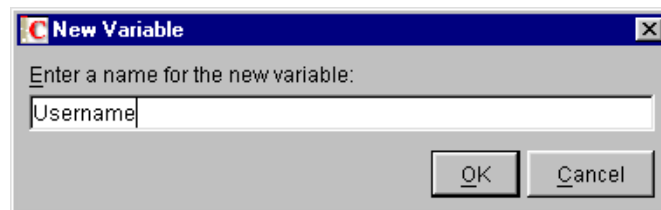
- 1 (Conditional) To add a username variable to an existing user ID, click the user ID, then click Edit.

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

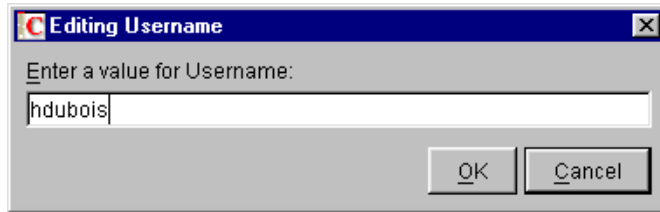
This dialog box is used to manage the variables (for example, username and password) associated with a login.



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



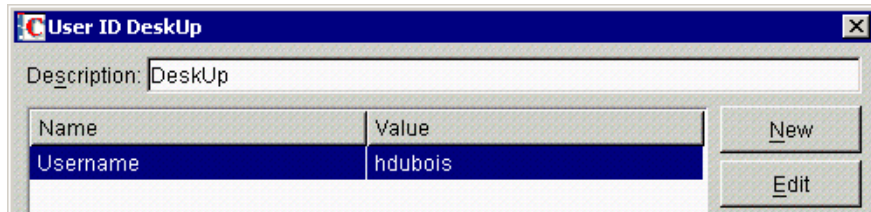
- 3 Type a value (for example, hdubois) for the new variable, then click OK.



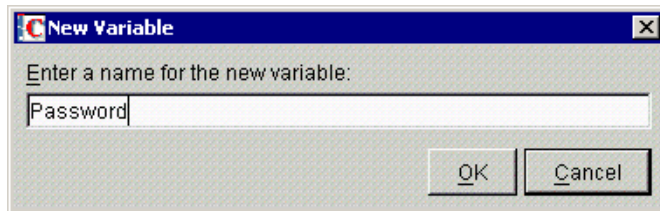
Adding a Password Variable and Value

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.

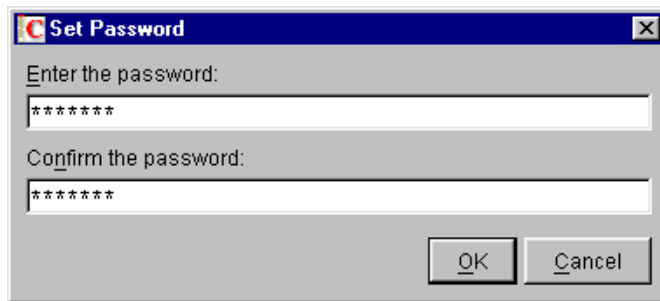
- 1 Click New.



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

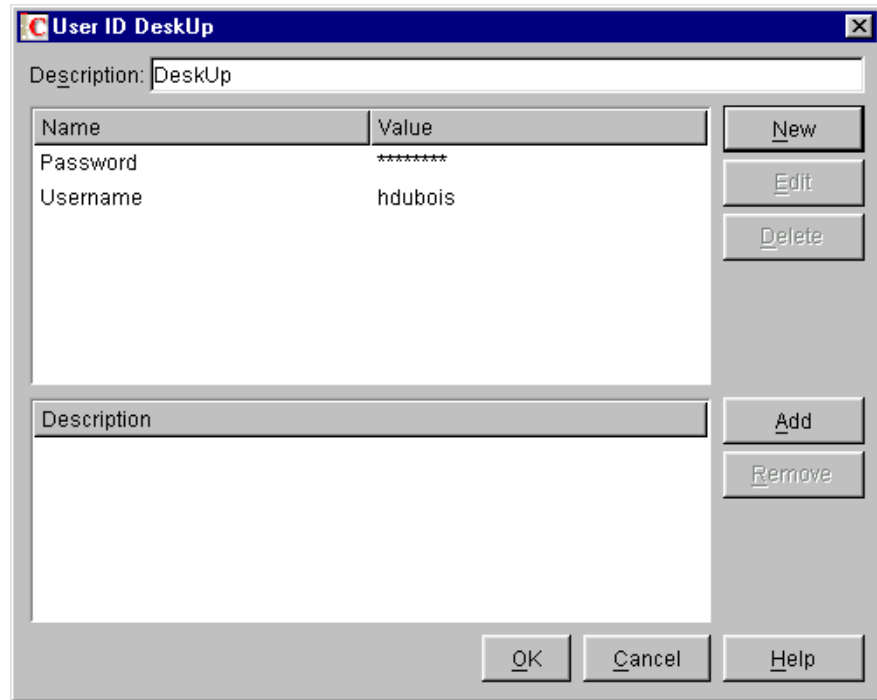


- 3 Type and confirm the new password, then click OK.

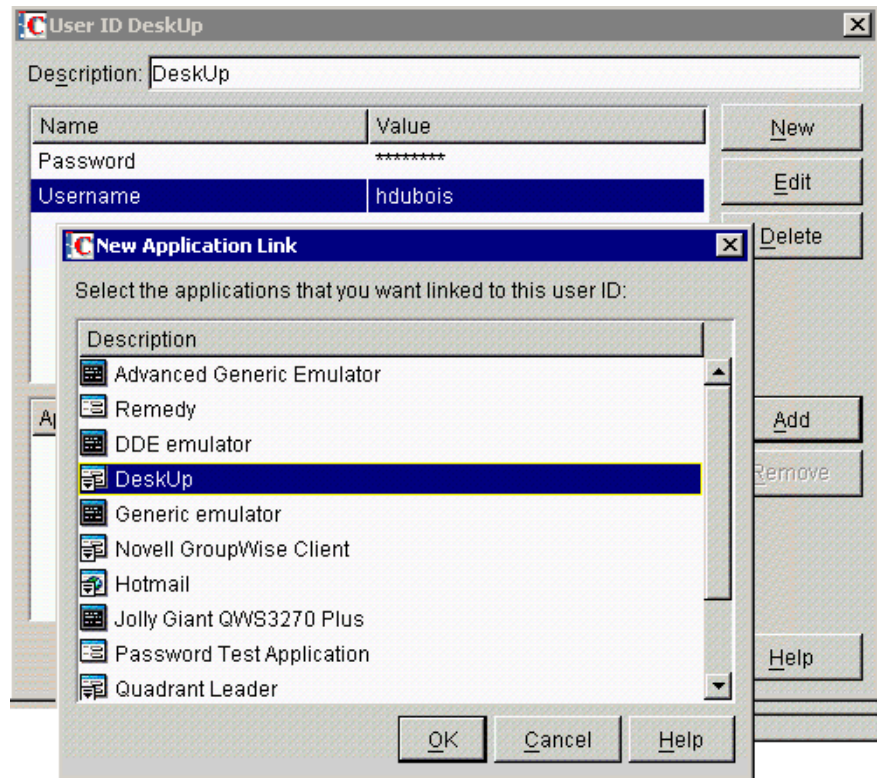


If you are using the properties of your own User object, the user ID values are saved to the local cache and a directory cache.

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



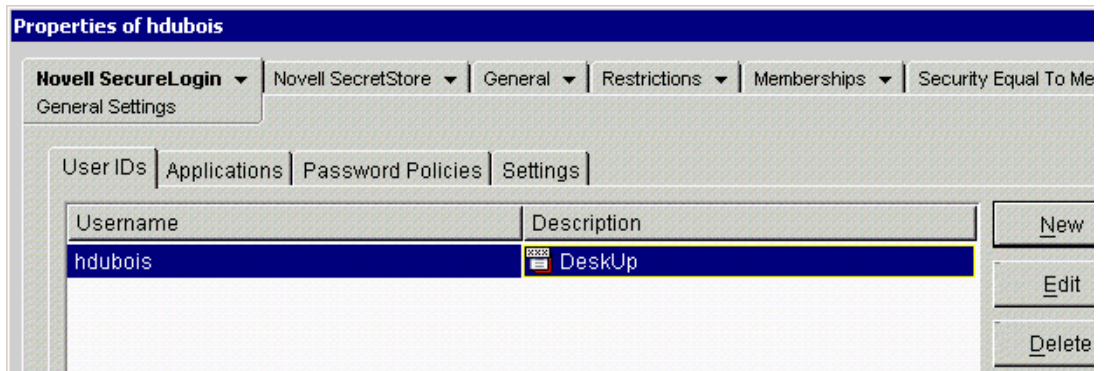
- 4 (Optional) Link the user ID to an application by clicking Add, selecting the application, then clicking OK.



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.

- 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:



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

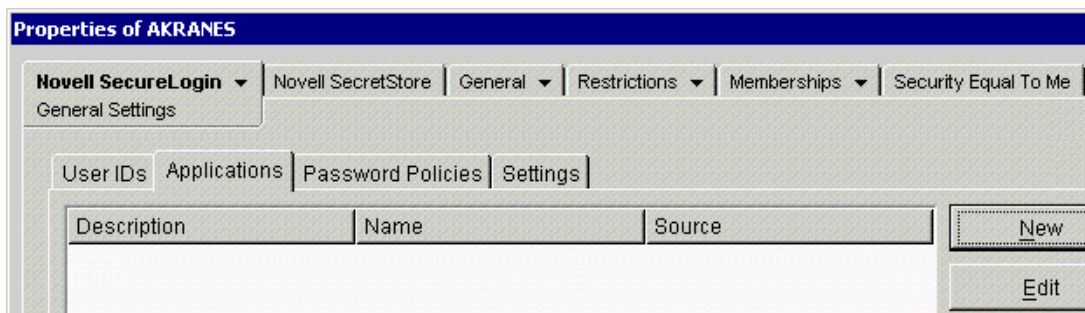
- 1 Click a user ID, then click Delete.
You can't delete an inherited user ID.
- 2 Save the data by clicking OK or Apply.

Managing Applications

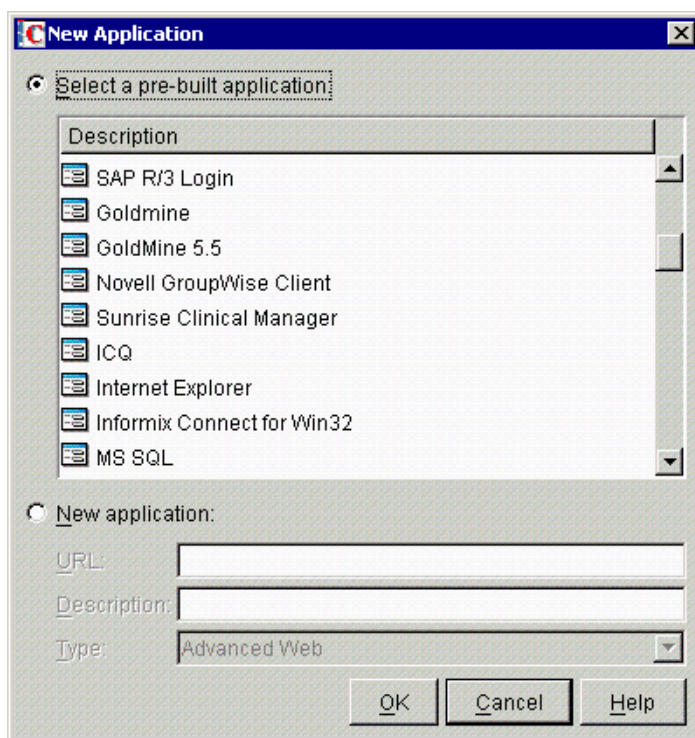
The Applications page lists applications that have been enabled for single sign-on. You can enable applications by using the Applications feature or the Add Applications Wizard.

Adding Applications for Single Sign-On

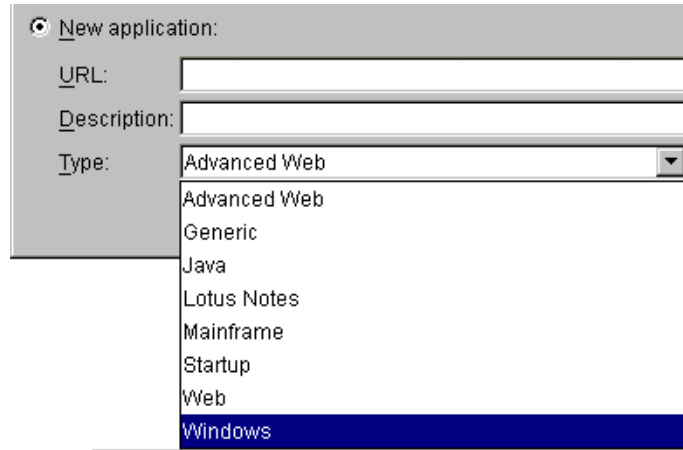
- 1 Click Applications > New.



- 2 (Optional) Add an application that has a prebuilt script.
 - 2a Click Select a Prebuilt Application.
 - 2b Click an application listed in the Description pane.



- 2c Add the application to the list by clicking OK.
- 3 (Optional) Add an application that SecureLogin will build a script for.
 - 3a Select New Application.
 - 3b Provide information for the text boxes and Type field.



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

Executable Name/Name: In the Executable Name or Name text box, type the executable filename (for example, PlainFare.exe).

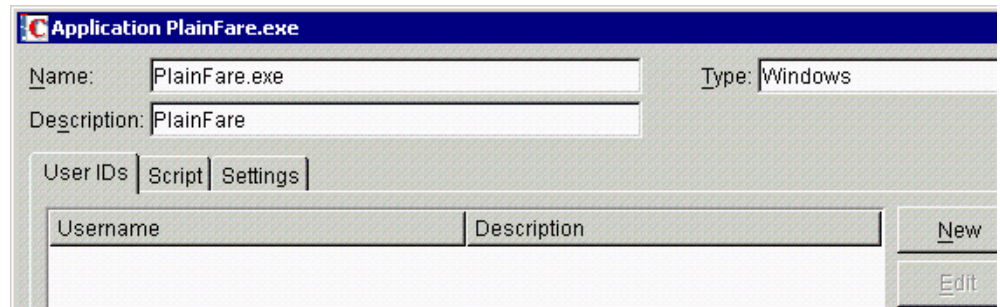
If you clicked Web or Advanced Web as the application type, the text-box label is URL. In the URL text box, type the URL where the application is found (for example, <http://www.hotmail.com>). For information on Advanced Web, see [“Using the Advanced Web Type” on page 31](#).

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

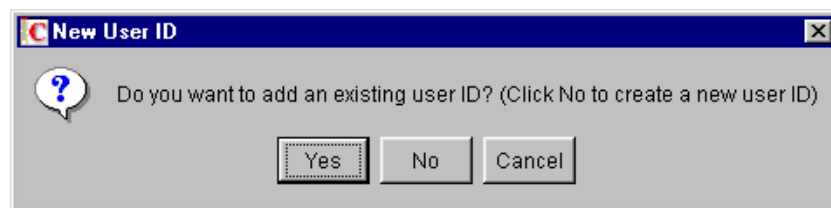
3c Click Create.

3d Add a user ID and a script for the application.

The User IDs page displays the user IDs linked to or associated with this application.



To add a user ID, click User ID, then click New. As the following figure illustrates, you can use an existing user ID or create a new one.



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.

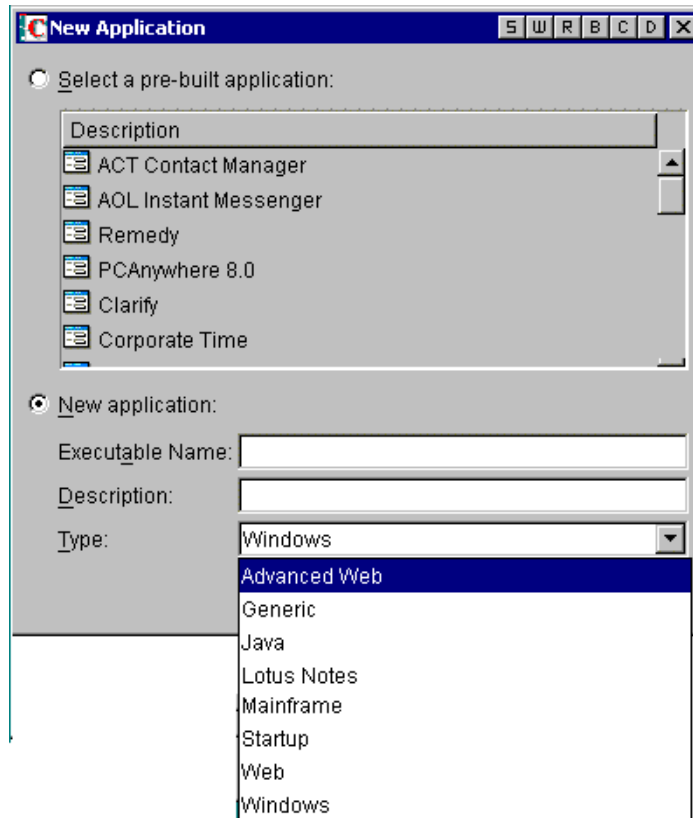
To create a new user ID, click No, then see [“Creating User IDs” on page 24](#).

To edit a user ID, on the Applications tab, 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.

3e Save the data by clicking OK or Apply on the main page.

Using the Advanced Web Type

When you select New Application to add a Web application in SecureLogin 3.51, you can select either the Web type or the new Advanced Web type.



The Web option remains in SecureLogin 3.51 so that customers who upgrade from previous versions of SecureLogin don't lose their existing Web scripts. In SecureLogin 3.51, 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 Scripting Guide](#).

Using the Generic Script Type

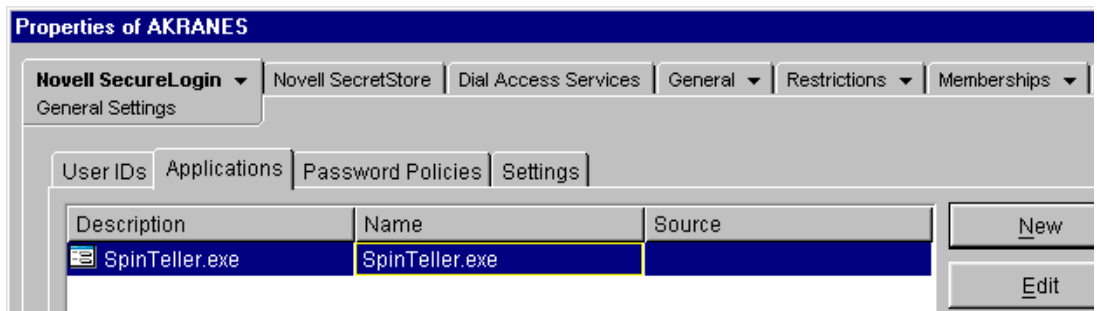
The Generic script type is for generic scripts. Generic scripts can be common to many scripts. Instead of copying and pasting the script, you can keep the script in a generic platform and include it in all scripts.

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

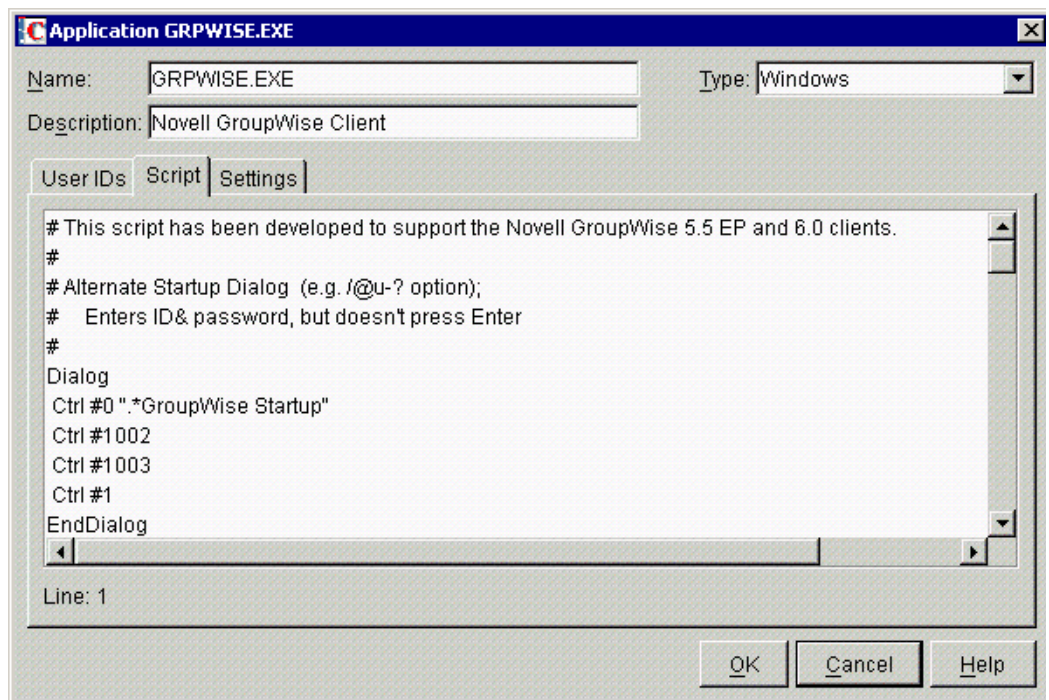
When you add an application, SecureLogin either uses a prebuilt script that you select or creates a script for the application. You can view, edit, or modify the script.

- 1 Click Applications.



- 2 Click the application, then click Edit.

- 3 Click Script.

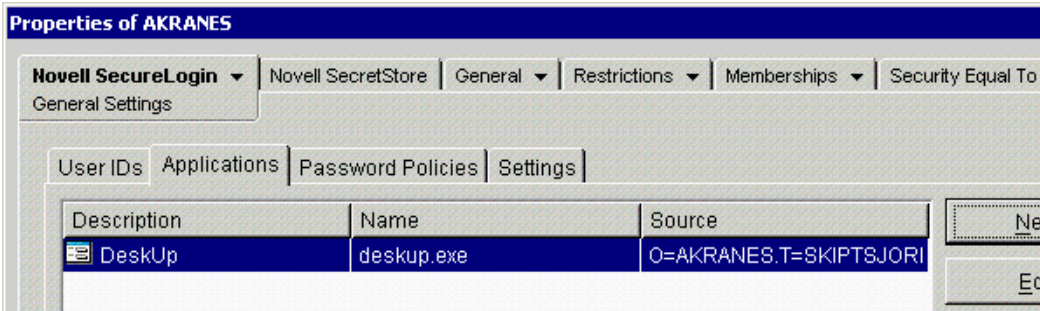


- 4 Edit the script, then click OK.

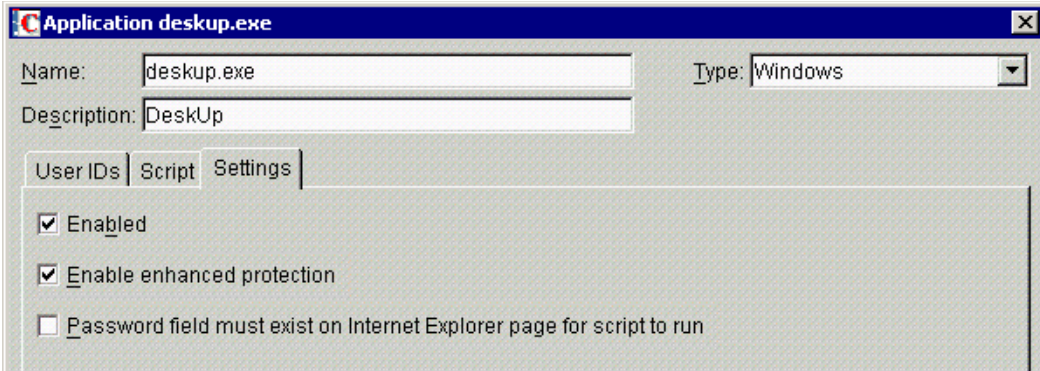
For information on scripts, see the [Nsure SecureLogin 3.51 Scripting Guide](#).

Modifying Settings for Applications

1 Click Applications.



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



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	<p>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).</p> <p>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.</p>

Preference	Description
Password Field Must Exist on Internet Explorer Page for Script to Run	<p>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.</p> <p>If you check the check box, the script runs only on the pages that have a password field.</p> <p>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.</p>

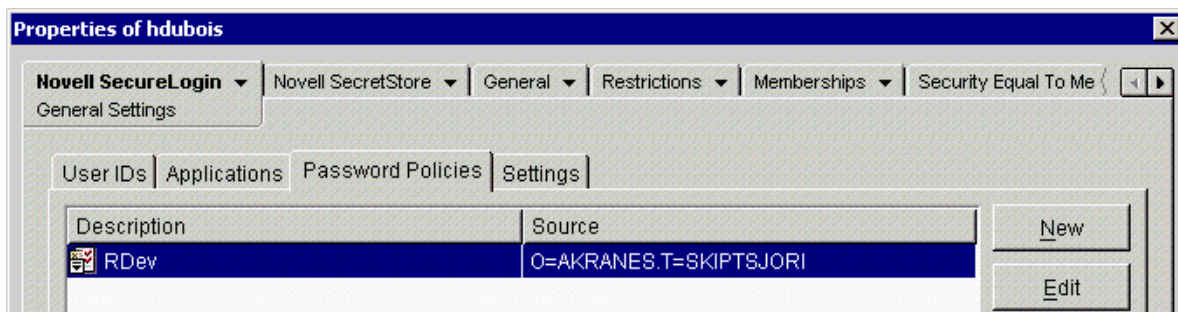
Managing Password Policies

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.

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.

Creating or Editing a Password Policy

- 1 Click Password Policies.

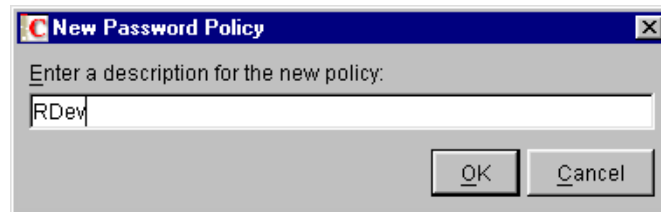


The Description column displays the name of the password policy. A down-arrow icon on the icon indicates that the policy is inherited.

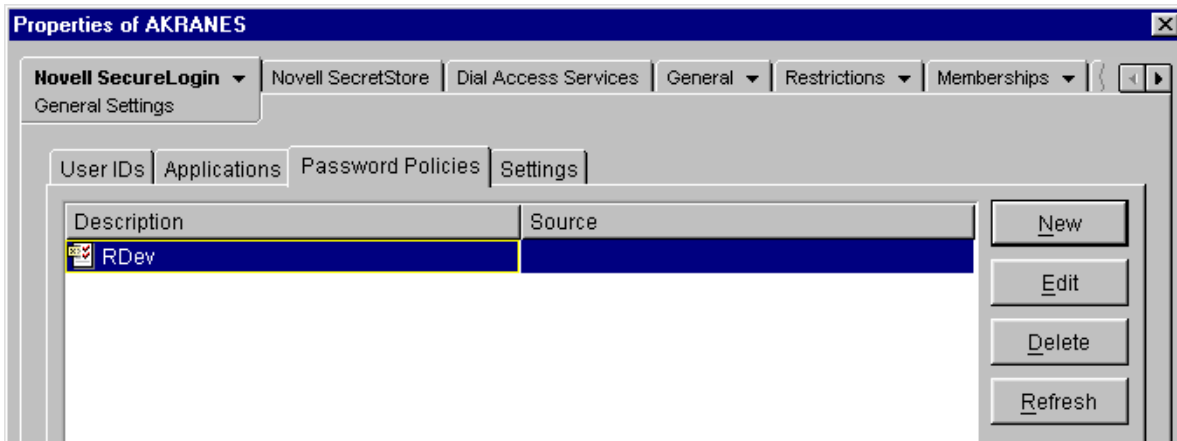
The Source column displays the distinguished name of the object that contains the password policy (the container that the policy is inherited from).

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.

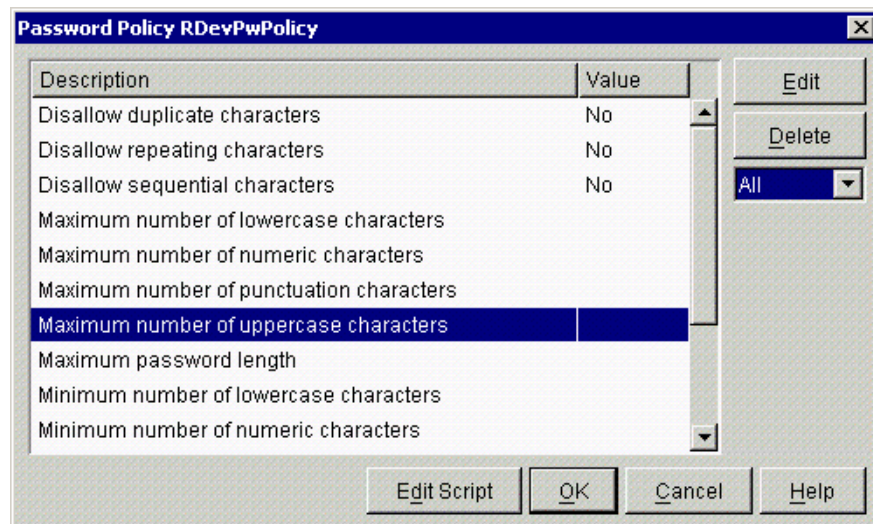
- 2 Click New, enter a descriptive name for the new policy, then click OK.



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



- 4** Edit settings, then click OK.

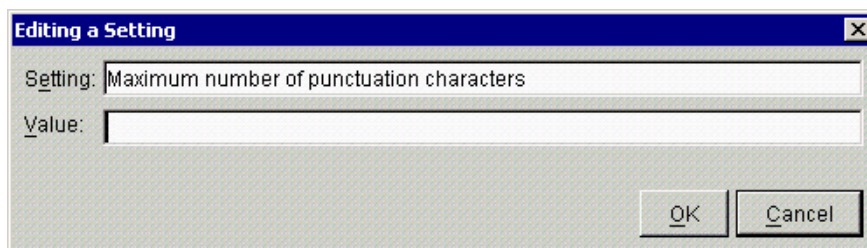


By default, several basic settings are displayed. To display all settings, select All from the drop-down list below the Delete button.

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 Editing a Setting text box.



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, this password AaBC is still accepted.

The following table lists default values for the settings:

Setting	Default Value
Disallow duplicate characters	No ABCA contains a duplicate character, but ABCD doesn't.
Disallow repeating characters	No AABC contains a repeating character, but ABCA doesn't.
Disallow sequential characters	No ABCD contains sequential characters, but BDAC doesn't.
Maximum number of lowercase characters	No value unless you set it.
Maximum number of numeric characters	No value unless you set it.
Maximum number of punctuation characters	No value unless you set it.
Maximum number of uppercase characters	No value unless you set it.
Maximum password length	No value unless you set it.
Minimum number of lowercase characters	No value unless you set it.
Minimum number of numeric characters	No value unless you set it.
Minimum number of punctuation characters	No value unless you set it. See "Allowable Punctuation Characters" on page 37.
Minimum number of uppercase characters	No value unless you set it.
Minimum password length	No value unless you set it.
Password must begin with an uppercase character	No

Setting	Default Value
Password must not contain any of these characters	No value unless you set it.

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:

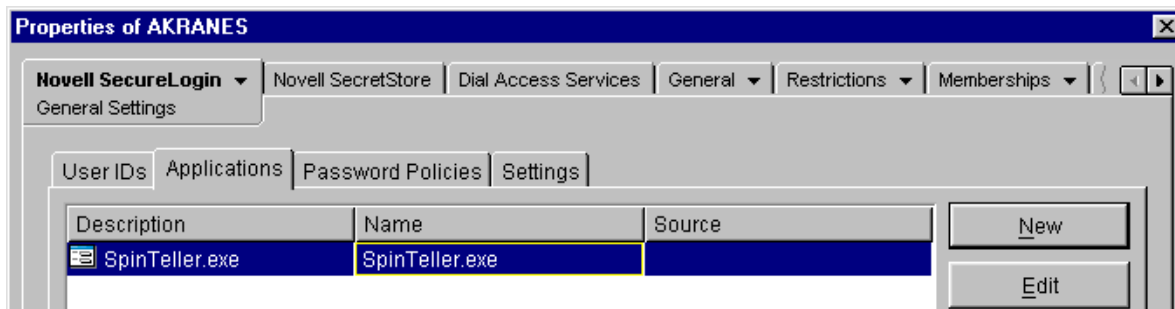
Character	Character Name
~	Tilde or swung dash
!	Exclamation mark
@	At
#	Hash or pound
\$	Dollar
%	Percent
^	Caret
&	Ampersand
*	Asterisk
	Space
()	Parentheses
_	Underscore
+	Plus
	Delimiter or delimiter bar
-	Hyphen
=	Equals
\	Backward slash or backward diagonal
{ }	Braces or curly brackets
[]	Brackets

Character	Character Name
:	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

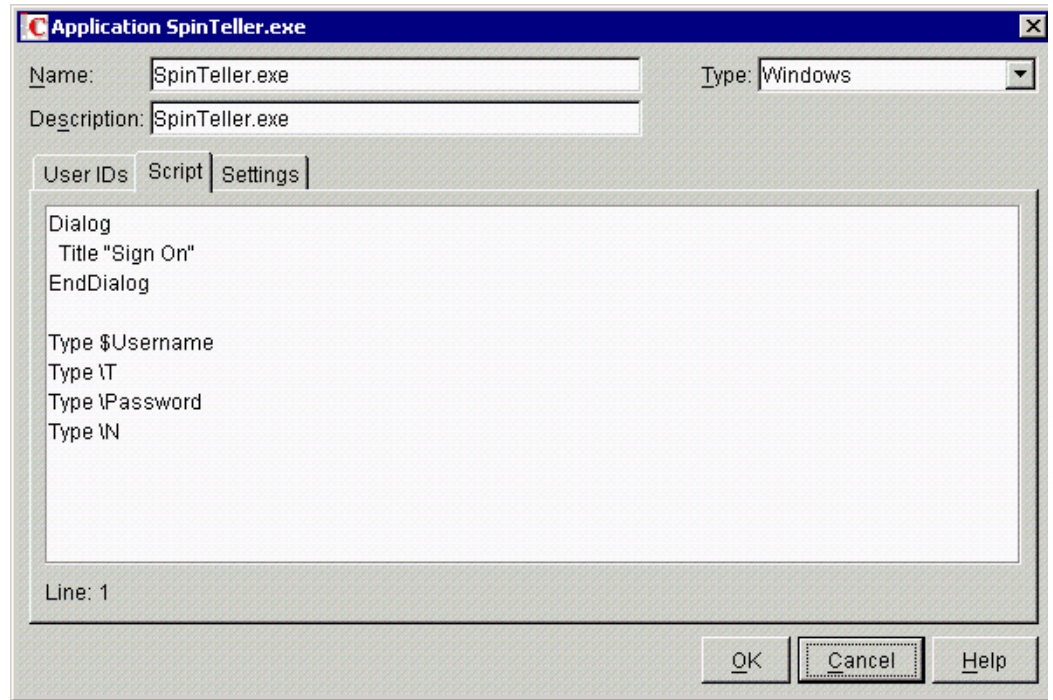
Using Password Policies in Scripts

You can use a password policy to restrict a variable within a script to the assigned security settings.

- 1 Click Applications.



- 2 Click the required application, then click Edit.



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 on the RestrictVariable and other commands, see the [Nsure SecureLogin 3.51 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. [“Managing Administrative and User Settings” on page 41](#)

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

Setting the Default Domain Policy

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

- 1** Expand Active Directory Users and Computers, right-click the domain name, then 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 41](#)
- ♦ [“Configuring SecureLogin Settings” on page 41](#)

Understanding the Configuration Hierarchy

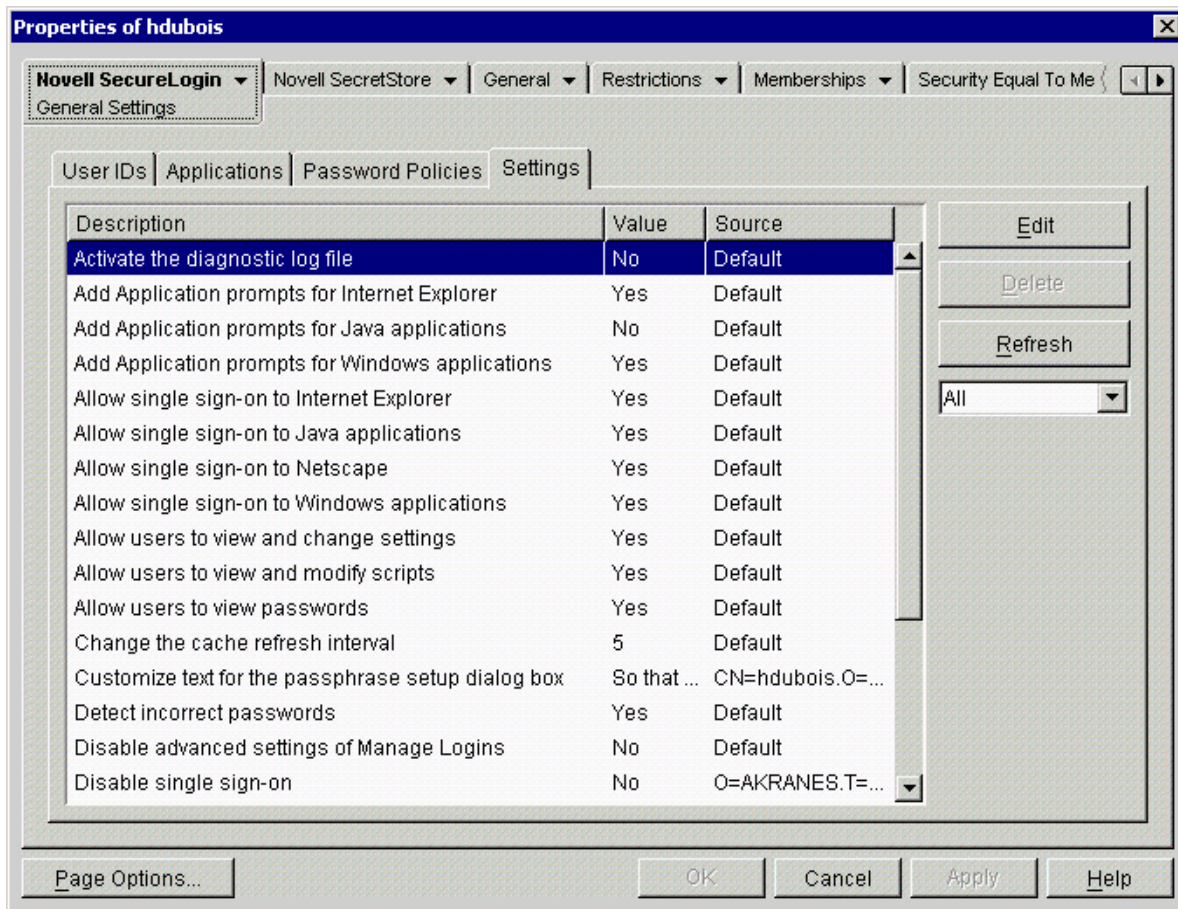
You can apply SecureLogin settings to a Container object, a User object, or a workstation.

- ♦ 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.

Configuring SecureLogin Settings

You can set up SecureLogin for users by changing default values on the Settings page. Some settings are user settings. Others are administrative settings. Users can change (override) user settings on their workstations. Even if an administrator makes a user setting, users can override it. However, users can't override administrative settings.

- 1 Click Settings.



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

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.

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.

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

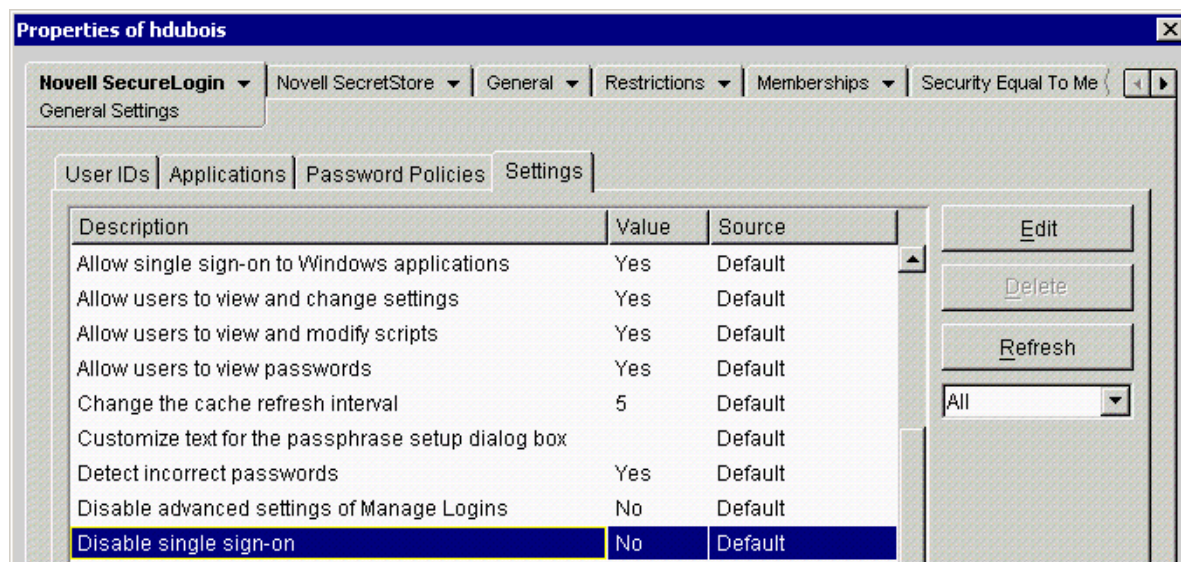
Configuration Option	Description
Activate the Diagnostic Log File	Logs the details of use to the hard drive. Because this preference is used for debugging and troubleshooting, the default is set to No. Don't change the value to Yes unless Novell Technical Services advises you to.
Add Application Prompts for Internet Explorer	Controls whether the Internet Explorer single sign-on component automatically detects Web application login panels and launches the Add Applications Wizard. To prevent a prompt, change the value to No.

Configuration Option	Description
Add Application Prompts for Java Applications.	Controls whether the Java single sign-on component automatically detects Java application login panels and launches the Add Applications Wizard. To allow prompts, change the value to Yes.
Add Application Prompts for Windows Applications	Controls whether the Windows single sign-on component automatically detects Windows application login panels and launches the Add Applications Wizard. To prevent a prompt, change the value to No.
Allow Single Sign-on to Internet Explorer	Enables the Internet Explorer single sign-on features of SecureLogin. To prevent users from being able to single sign-on to Internet Explorer applications, set the value to No.
Allow Single Sign-on to Java Applications	Enables the Java single sign-on features of SecureLogin. To prevent users from being able to single sign-on to Java applications, set the value to No.
Allow Single Sign-on to Netscape	Enables the Netscape single sign-on features of SecureLogin. To prevent users from being able to single sign-on to Netscape applications, set the value to No.
Allow Single Sign-on to Windows Applications	Enables the Windows single sign-on features of SecureLogin. To prevent users from being able to single sign-on to Windows applications, set the value to No.
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	<p>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.</p> <p>To prevent users from viewing and modifying scripts, set the value to No.</p>
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.
Change the Cache Refresh Interval	Controls the number of minutes that SecureLogin waits between synchronizing the information between the local cache and the Directory. The default is 5 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	Enables SecureLogin to attempt to detect whether you have given it an incorrect password. SecureLogin can then prompt you to change the password. To disable this feature, set the value to No.
Disable the Advanced Settings of Manage Logins	<p>The Advanced option that is available from the SecureLogin system tray icon enables users to change SecureLogin settings, change their passphrases, and refresh the local cache.</p> <p>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 system tray icon or Manage Logins.</p>

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.
Display the System Tray Icon	To prevent users from displaying and accessing the system tray icon, change the value to No.
Enable the File Cache	Enables SecureLogin to use cache files. Usernames and passwords 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 add logins by accessing the New Login Wizard from the system tray. To disable this feature, change the value to No.
Password Protect the System Tray Icon	Requires users to provide their passwords before they can access options on the system tray SecureLogin icon. The default is No. 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	By default, SecureLogin reads its information from the current user's context and then searches up the Directory tree. The default is No. To prevent searching upward, change the value to Yes.
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.

Preventing Users from Accessing SecureLogin

- 1 Click Settings.



- 2 Click Disable Single Sign-On, click Edit, then set the value to Yes.

Managing Passphrases

SecureLogin uses an underlying security mechanism, known as a passphrase. A passphrase is actually two parts:

- ♦ A passphrase question

The passphrase question should provide a good level of security for the actual answer. For example, a question of "What is 2 times 3?" would obviously not provide a secure passphrase answer. The same could be said for questions that pertain to a user's personal information, such as parents' names.

To apply an acceptable level of security, the SecureLogin administrator can set the passphrase question.

Passphrase questions can have 255 characters.

- ♦ A passphrase answer

The passphrase answer is a value that is unique to each user and should only be known by the account owner.

The figure in ["Entering a Passphrase Question and Answer" on page 45](#) illustrates the dialog box that collects your passphrase question and answer.

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

To prevent a rogue administrator from resetting a user's password and attempting to gain access to a user's single sign-on information, SecureLogin prompts for the passphrase whenever SecureLogin recognizes that tampering or an administrative password change has been performed on the user's account.

This passphrase is also used when the user accesses cached login data while not authenticated to the directory.

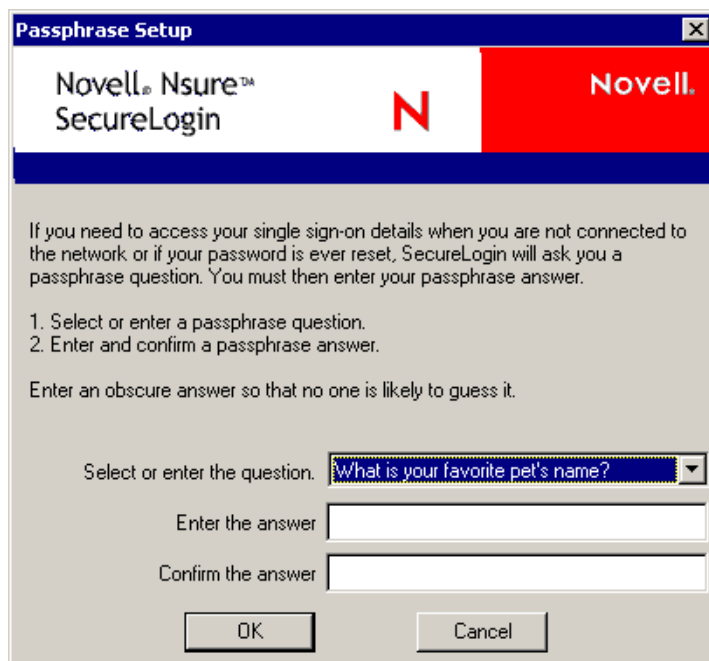
The passphrase question and answer help you access your login data in the following situations:

- ♦ You aren't authenticated to the directory.
- ♦ The network connection is lost.
- ♦ You are using a laptop computer and are out of contact with the network
- ♦ You forget your eDirectory password and have it reset for you.
- ♦ Your credential store was locked when an administrator inappropriately reset your eDirectory password.

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

Entering a Passphrase Question and Answer

As the following figure illustrates, a dialog box enables you to provide a passphrase question and answer. You encounter this dialog box after you install and first run SecureLogin.



SecureLogin uses the question and answer to ensure that no one else uses your login credentials to access your applications. Choose passphrase information that you'll be able to recall months or years from now.

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. When you next log in, you encounter a passphrase answer prompt. For more information, see [“Setting Up a SecretStore Administrator”](#) in the [Novell SecretStore 3.3.0 Administration Guide](#).

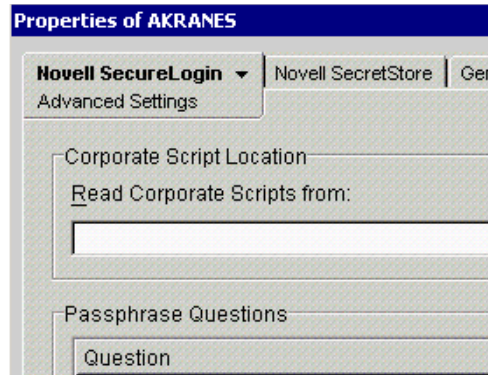
Providing Passphrase Questions

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

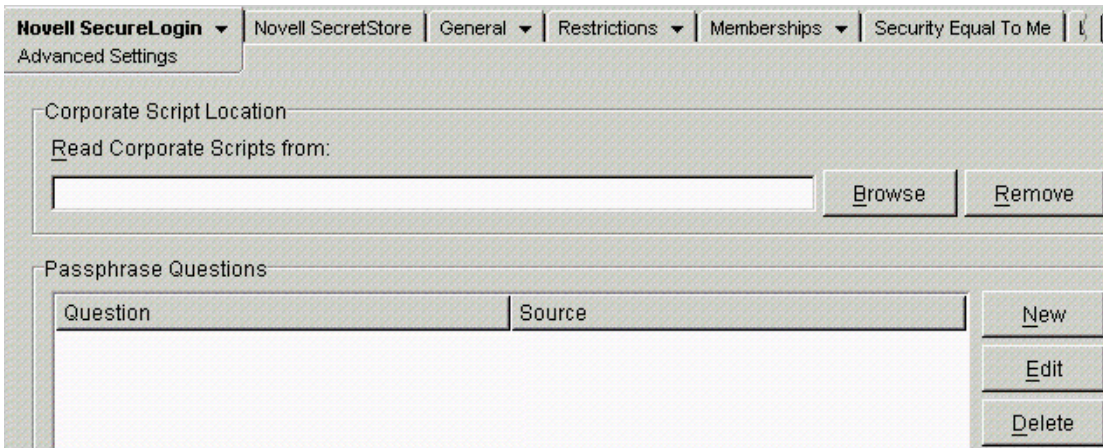
- 1 In ConsoleOne, right-click a Container object, then click Properties.

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

- 2 Click Novell SecureLogin, then select Advanced Settings.

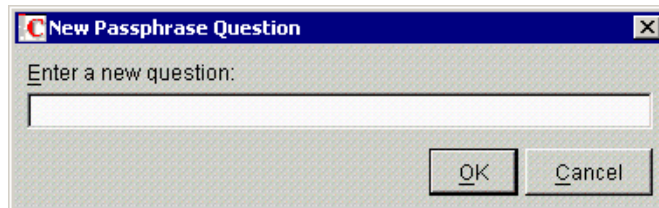


- 3 In the Passphrase Questions dialog box, click New.



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

- 4 Type a question, then click OK.

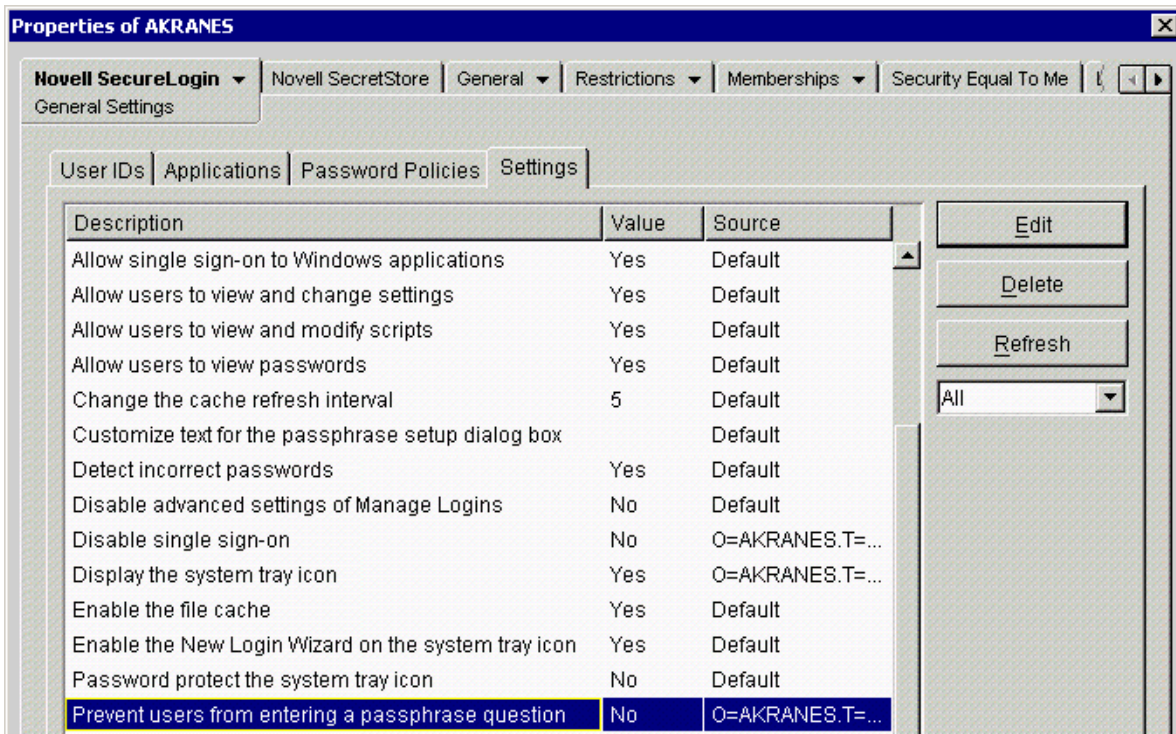


- 5 Click Apply.

Disabling User-Set Passphrase Questions

By default, users can enter their own passphrase questions. To disallow user-set questions and require users to select a preset question:

- 1 In an administrative tool, select Novell SecureLogin > General Settings, then click Settings.

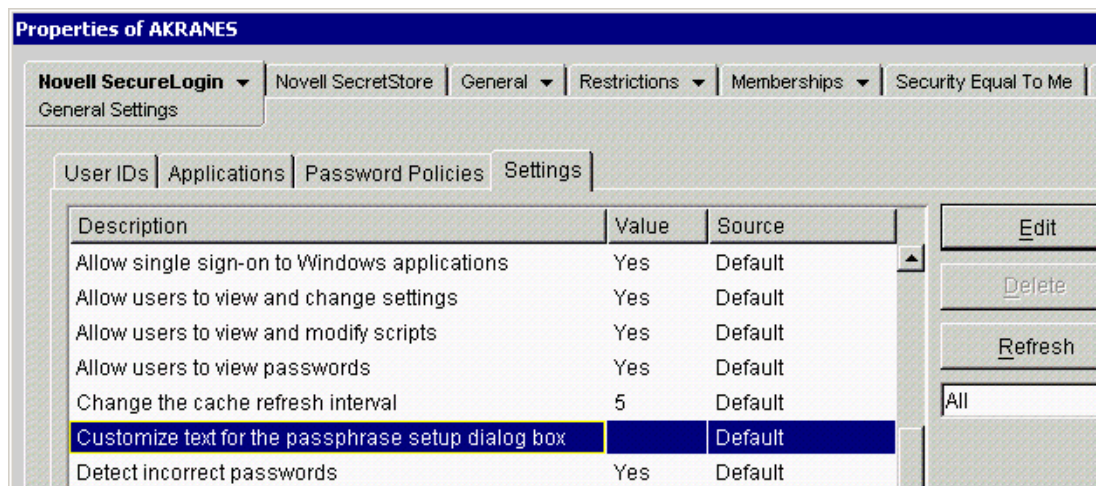


- 2 Click Prevent Users from Entering a Passphrase Question, click Edit, select Yes from the drop-down list, click OK, then click Apply.

Customizing Introductory Text

When users first encounter SecureLogin, SecureLogin prompts them to enter a passphrase question and answer. See [“Entering a Passphrase Question and Answer” on page 45](#). You can edit that text and provide customized instructions.

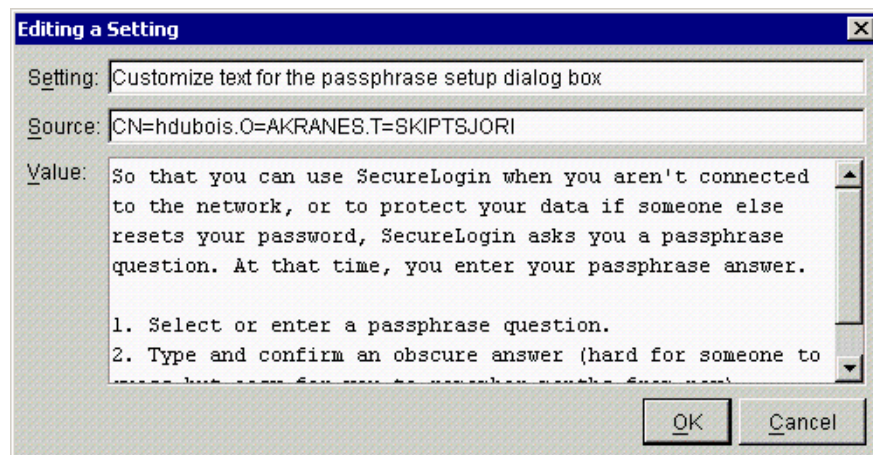
- 1 Click Settings.



- 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.



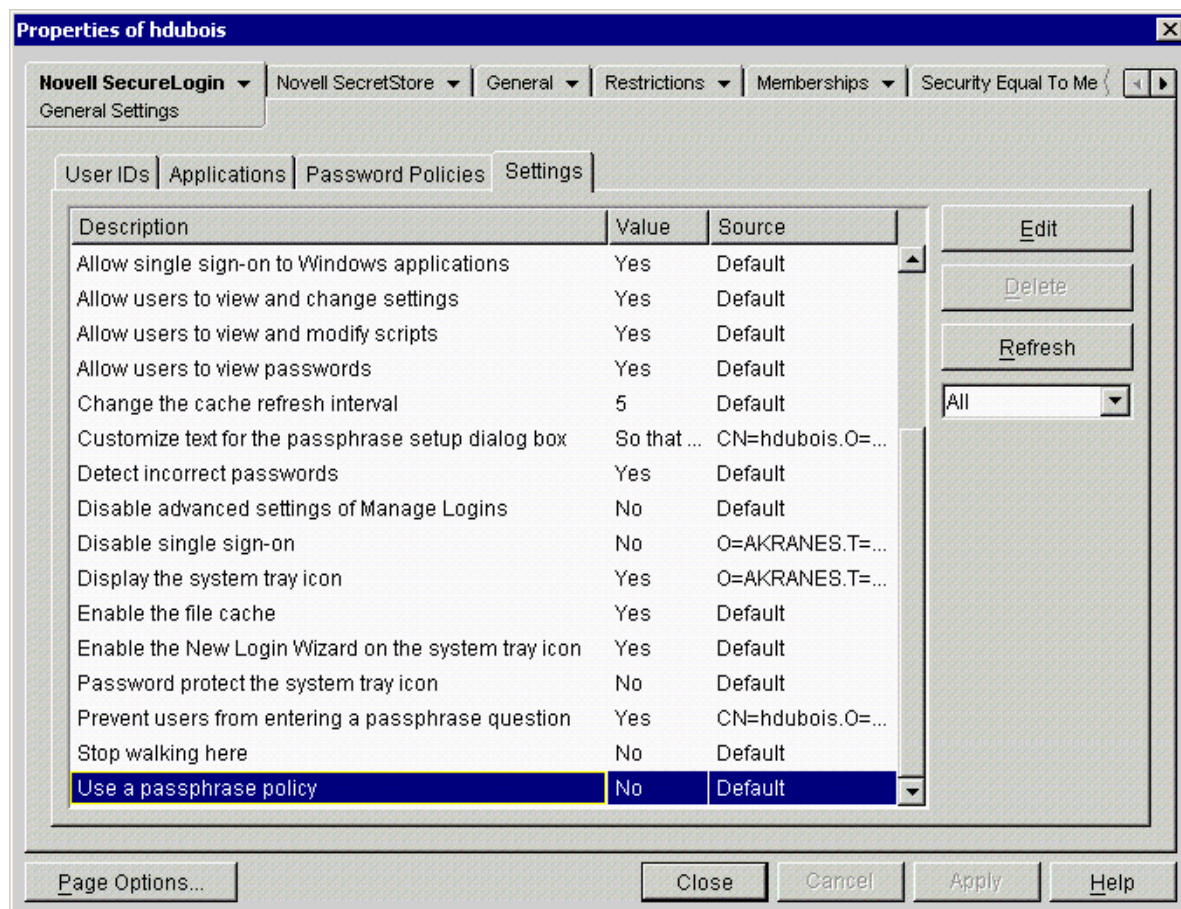
Although your introductory text can have 8 lines with 64 characters in each line, limit your text to 415 characters. If you type too many lines, the text boxes for the passphrase question and answer will hide them.

- 4 Click Apply.

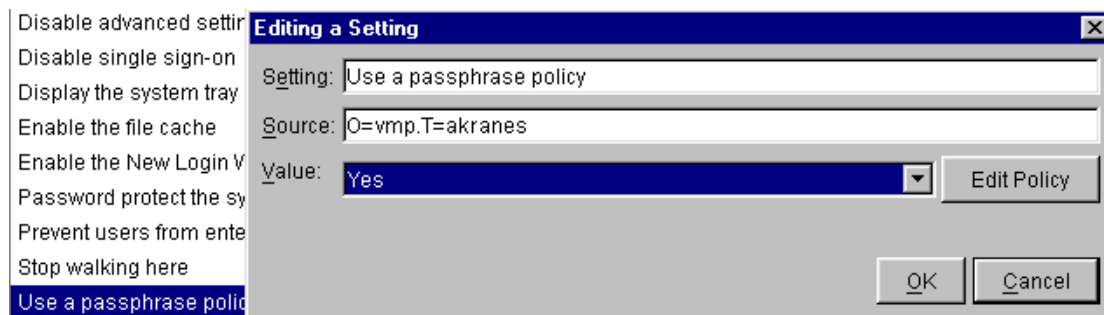
Using a Passphrase Policy

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

- 1 Click Settings.
- 2 Scroll to and select Use a Passphrase Policy.



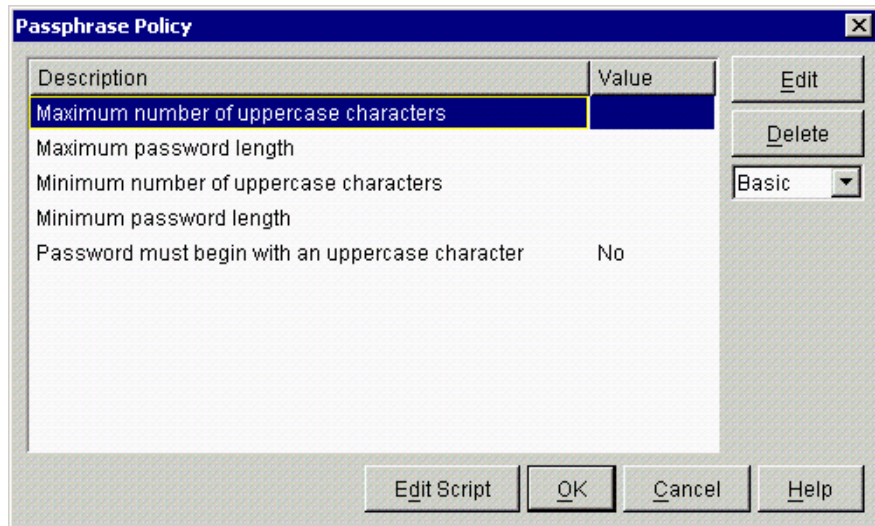
3 In the Editing a Setting dialog box, require a passphrase policy by changing the value to Yes.



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

4a Select a setting, then click Edit.

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



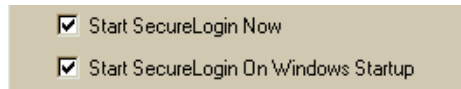
To view all the settings, select All from the drop-down list.

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

5 Save the setting by clicking OK twice.

Displaying the System Tray Icon

During installation, you encountered a Post-Install screen that displayed the following options:



If you checked the Start SecureLogin on Windows Startup check box, SecureLogin places the SecureLogin icon on the system tray whenever you start the computer.



To prevent users from displaying and accessing the system tray icon:

- 1** Click Settings.
- 2** Select Display the System Tray Icon, then click Edit.
- 3** Using the drop-down list, change the value to No.

If you turn off the SecureLogin icon on the system tray 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 system tray, 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.

Using SecureLogin with Client Software

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

- ♦ The Novell Client™ for Windows NT* or the Novell Client for Windows 9x
- ♦ The eDirectory option (selected during installation)
- ♦ The eDirectory with SecretStore 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 (NMASTM) client, using the eDirectory password method, no additional installation or configuration is required. By default, the NMASTM client hides the eDirectory password field on the Novell Client login dialog box in favor of a subsequent password prompt.

To re-enable the Login dialog's password field:

- 1** Right-click the N icon on the system tray.
- 2** Click Novell Client Properties > Location Profiles.
- 3** Click Default in the Location Profiles window, then click Properties.
- 4** In the Services page, click Properties.
- 5** In the Credentials page, check the Enable Password Field check box.
- 6** Close dialog boxes by clicking OK.

To enable use of eDirectory login data without the NMASTM client, install the SecureLogin client login extension (slina.dll) from the `\securelogin\terminalserver\citrix\srv\nw` directory.

- 1** Without replacing newer files, copy `slina.dll` and `unicows.dll` to the Windows system directory (`c:\winnt\system32` or `c:\windows\system`).
- 2** Register the login extension by double-clicking the appropriately-named .reg file.
 - ♦ On Windows NT, Windows 2000, or Windows XP workstations, register the login extension by opening `Register NT LoginExt.reg`.
 - ♦ On Windows 98 workstations, open `Register 98 LoginExt.reg`.

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. 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:

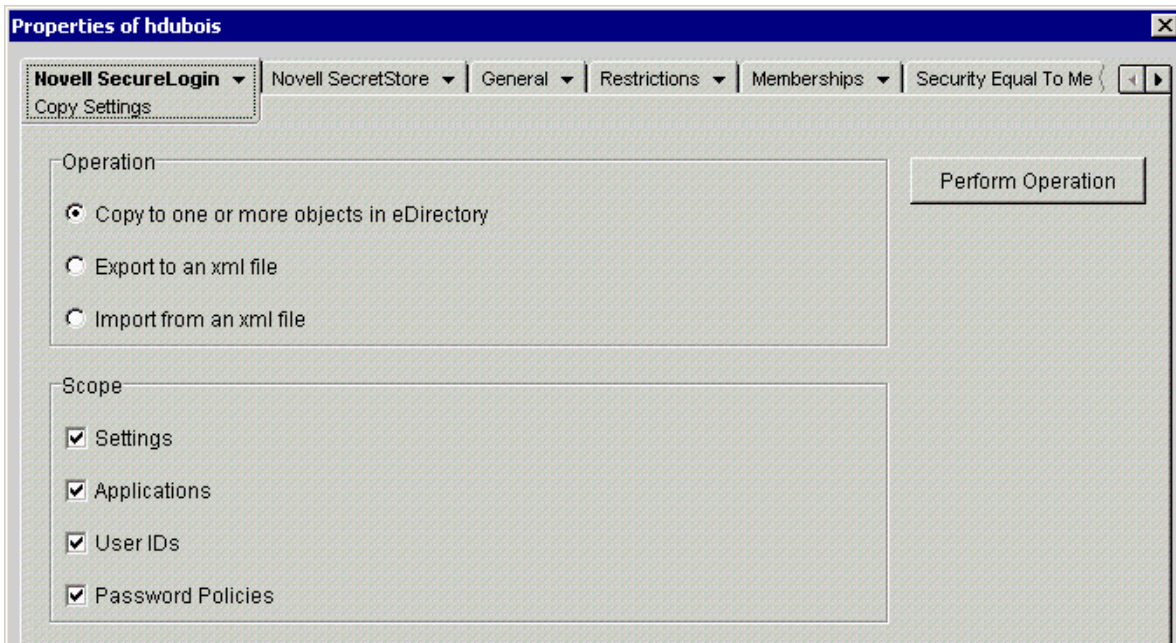
- ♦ Typically, copy from a User object to a User object and from a Container object to a Container object.
- ♦ Copy settings to an object in the same context, a parallel context, or a subordinate context. Don't copy settings from an object in a subordinate context to an object in a superior (higher in 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.

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.



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

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

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

- 4** Click Perform Operation.
- 5** At 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

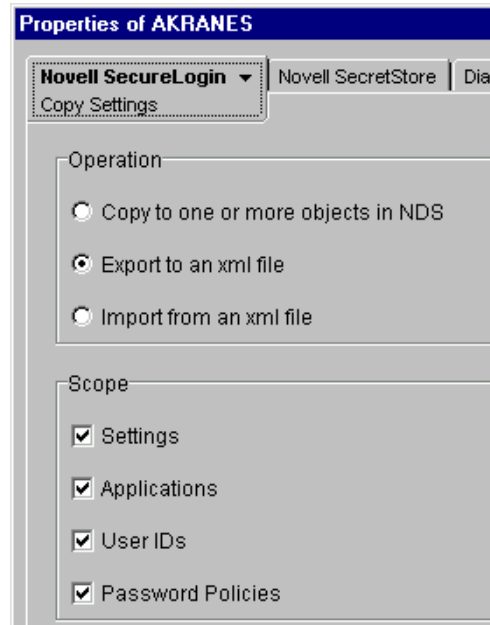
You can export settings from one tree and import them into the same tree or a different tree. The Export and Import options operate on the same settings as Copy Settings.

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.



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

To limit the scope, uncheck 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 check all check boxes (in the Scope pane) for settings that you want to import.

To limit the scope, uncheck 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.

Setting Up Multiple IDs for an 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 identity for each role. SecureLogin automatically logs Henri in to deskup.exe according to the role that he uses to log in.

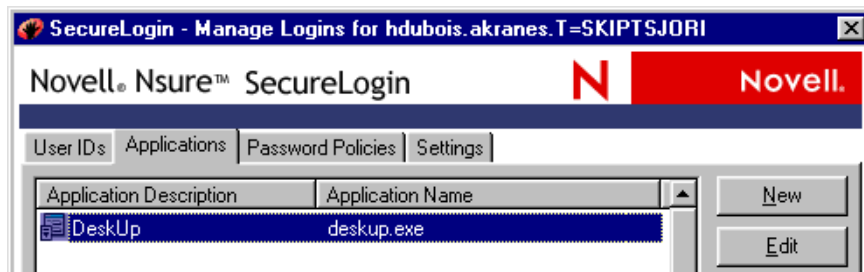
To set up multiple IDs for an application:

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

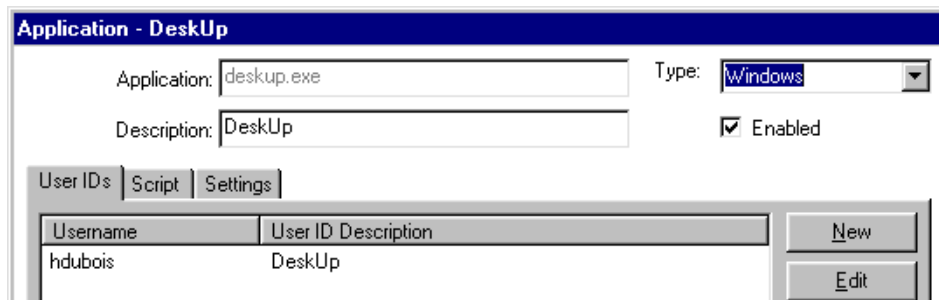
If a user ID already exists for the application that you need multiple IDs for, skip this step.

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

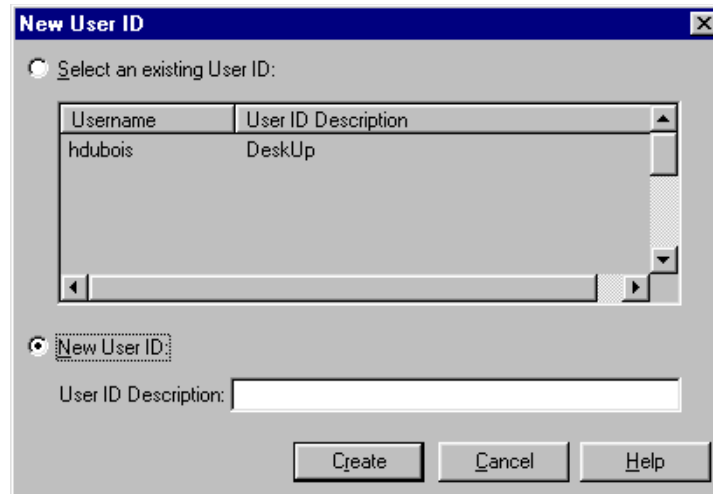
- 2 Click Applications, select the application that you want to create the multiple user ID for, then click Edit.



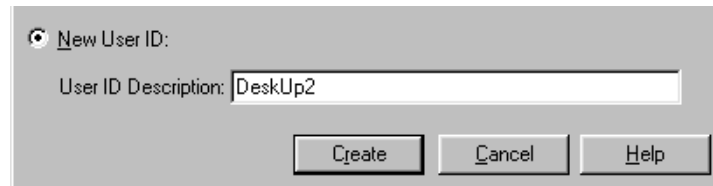
- 3 In the User IDs dialog box, click New.



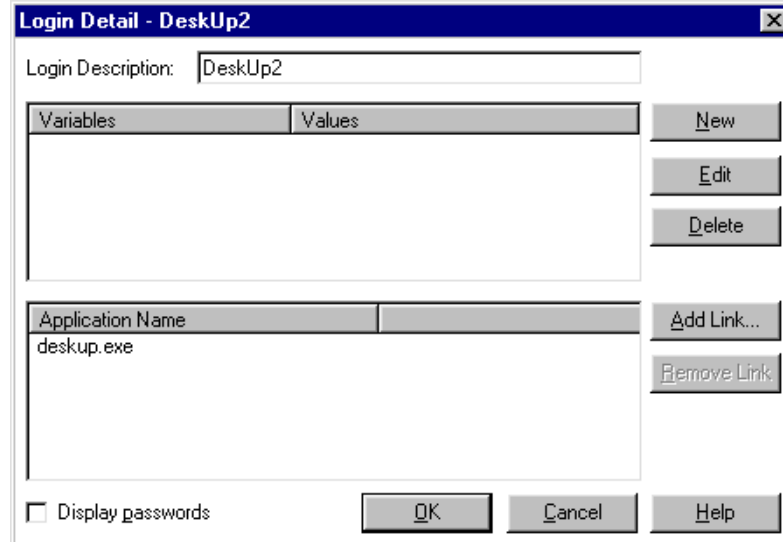
- 4 In the New User ID dialog box, click New User ID.



- 5** Type a description for the multiple-ID login that you are creating, then click Create.

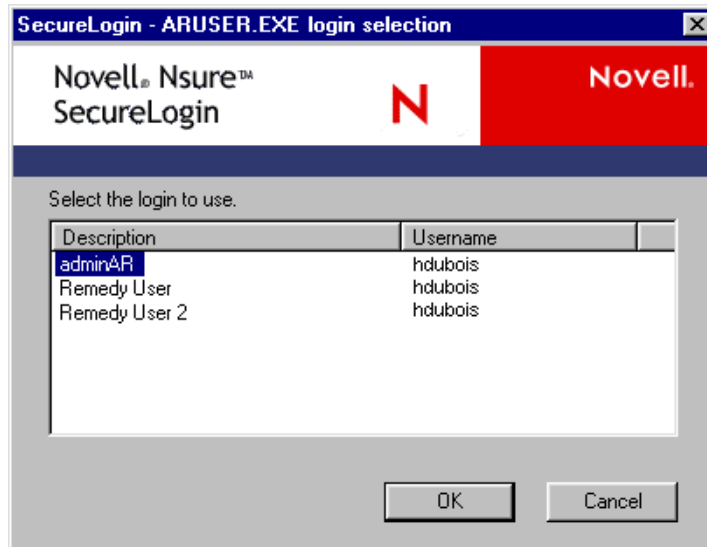


- 6** Enter variables and values for the new user ID, then save changes.



- 7** 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.



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.

Defining Applications That SecureLogin Detects

SecureLogin automatically detects applications that require users to log in. You or the user can set the preferences to have SecureLogin detect or ignore Windows Applications, Internet Explorer, or Netscape logins. 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.

By default, SecureLogin doesn't provide or use an `exclude.ini` file. The applications that SecureLogin ignores are hard-coded into SecureLogin. The following table lists applications that SecureLogin ignores:

loginw32.exe	nwadm95.exe	slmanager.exe
loginw95.exe	nwadm95.exe	slproto.exe
mmc.exe	nwtray.exe	slwinsso.exe
msdev.exe	scrnlock.scr	tlaunch.exe
notes.exe	setup.exe	wfica32.exe
nswebsso.exe	slbroker.exe	
nwadm32.exe	sllock.scr	

Ignoring Additional Applications

- 1 Create an `exclude.ini` file in the SecureLogin installation directory.

Typically, the directory is `c:\program files\novell\securelogin`.

You can use a standard text editor to create the file.

- 2 List the executable names for applications that you want SecureLogin to ignore.

Add one executable name per line. For example, to prevent SecureLogin from detecting weblog.exe, enter the following line in the exclude.ini file:

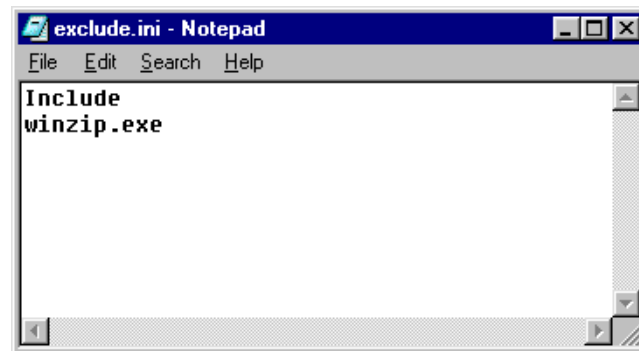
```
weblog.exe
```

- 3 Save the exclude.ini file.

Detecting Specific Applications

By using an exclude.ini file, you can specify and limit the programs that SecureLogin detects.

- 1 Create an exclude.ini file.
- 2 Place the Include command as the first entry in the file.



- 3 List the applications that you want SecureLogin to detect.
- 4 Save exclude.ini on the workstation in the SecureLogin installation directory.

Typically, the directory is c:\program files\novell\securelogin.

When using the Include command in the exclude.ini file, you must list every application you want SecureLogin to detect. Using the Include command in the exclude.ini file does the following:

- ♦ Increases performance
- ♦ Stops the auto detection of new applications
- ♦ Stops the auto detection of single sign-on to any applications not listed in the file
- ♦ Increases security

NOTE: You can't simultaneously use Exclude and Include modes.

If an application has been hard-coded to be ignored, you can have SecureLogin detect it.

- 1 Create an exclude.ini file.
- 2 Place the Nodefault command as the first entry in the file.

This command causes SecureLogin to ignore the hardcoded list.

- 3 Rebuild the hard-coded list in the exclude.ini file, including all the applications in the list except the application that you want SecureLogin to detect.
- 4 Save exclude.ini on the workstation in the SecureLogin installation directory.

Typically, the directory is c:\program files\novell\securelogin.

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 autostart:

- ♦ “Using the Startup Group” on page 60
- ♦ “Using Startup Scripts” on page 60
- ♦ “Using Novell Application Launcher to Start Applications” on page 61

Using the Startup Group

You can move application start commands from Registry Run to the Startup group. 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.

Using Startup Scripts

Startup scripts are scripts that are executed during SecureLogin’s startup. You can move application start commands from Run or the Startup group to a SecureLogin startup script. This option has the following possible drawbacks:

- ♦ Application paths might be different on each computer.
To resolve this issue, place a .ini file on each computer. This file would list the applications that are to start after SecureLogin has initialized.
- ♦ This option is not automated.
To resolve this issue:
 1. Check the list of applications in the Run key against the applications defined in SecureLogin.
 2. Prompt the user to automatically delete the list from the Run key.
 3. Add the list to the .ini file.

After users have added the list to the .ini file, they must restart the application, or log out and log back in to the workstation. (This is a one-time task.)

If for some reason SecureLogin doesn't detect an application when it is launched from the startup script, you can modify the startup script to call a batch file. The following example startup script launches Novell iFolder:

```
Run "c:\Documents and Settings\administrator\Desktop\ifolderlaunch.bat"
```

The batch file contains the following lines:

```
Sleep 1
Start "ifolder" /MIN /B "c:\Program Files\novell\ifolder\trayapp.exe"
Exit
```

Using Novell Application Launcher to Start Applications

Use the Icon Order and Wait on Force Run options in Novell Application Launcher™ (NAL). These options enable you to use NAL 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 NAL launches.

3

Using SecureLogin

This section contains information on the following:

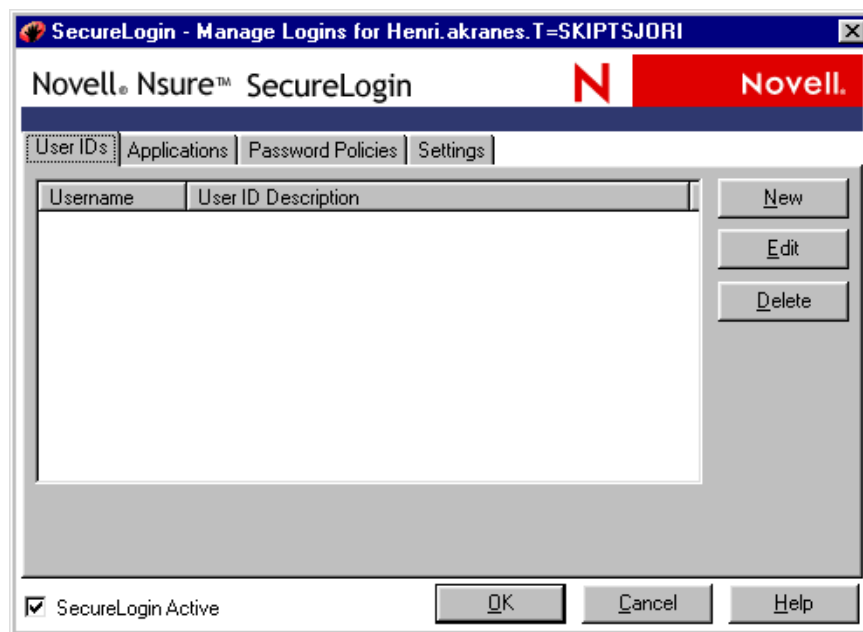
- ♦ “Accessing SecureLogin’s Main Window” on page 63
- ♦ “Using the SecureLogin Icon” on page 64
- ♦ “Adding Applications” on page 65
- ♦ “Linking User IDs to Applications” on page 78
- ♦ “Changing Settings” on page 79

Accessing SecureLogin’s Main Window

The SecureLogin client runs on workstations. To access SecureLogin’s main window, do one of the following:

- ♦ Click Start > Programs > Novell SecureLogin > Novell SecureLogin.
- ♦ Double-click the SecureLogin icon on the system tray.
- ♦ Right-click the SecureLogin icon on the system tray, then select Manage Logins.

The following figure illustrates SecureLogin’s main window.



NOTE: If the administrator has set the value for Display the System Tray Icon to No, this window won't display on user's workstations. SecureLogin will run, add applications, and manage credentials on behalf of the users, but users won't have access to management options that SecureLogin's main window provides.

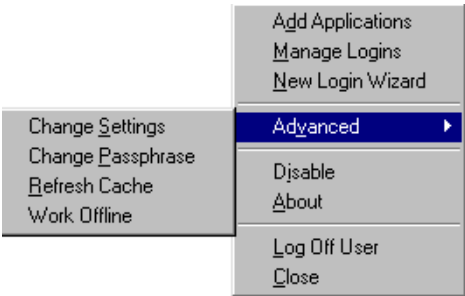
Using the SecureLogin Icon

By default, the installation program places the SecureLogin icon on the system tray.



This icon is a shortcut to SecureLogin functionality on workstations. To use the shortcut:

- 1 Right-click the SecureLogin icon on the system tray.
- 2 Select the task that you want to complete.



The following table provides information on the tasks:

Option	Description
Add Applications	Adds Windows, Web, Advanced Web, and Java applications. Enables you to have applications launch as soon as Windows starts up. See "Adding Applications" on page 65
Manage Logins	Brings up SecureLogin's main window. Adds user IDs (login credentials), links user IDs to applications, manages password policies, and manages SecureLogin settings.
New Login Wizard	Creates a new user ID for an application that you select.
Advanced > Change Settings	Applies a subset of settings to a workstation. For a complete list of settings, see "Configuring SecureLogin Settings" on page 41 .
Advanced > Change Passphrase	Changes a user's passphrase question or passphrase answer. See "Managing Passphrases" on page 45 .
Advanced > Refresh Cache	Refreshes the contents of the local cache.
Advanced > Work Online/Offline	Toggles between SecureLogin's online and offline states. When you work offline, SecureLogin uses the local (secondary) cache rather than the directory.
Active	Determines whether SecureLogin is enabled (active) or disabled.

Option	Description
About	Displays the SecureLogin version number and the status of the data stores. The primary data store is the directory. The secondary is the local cache.
Log User Off Windows	Logs you off from your Windows session.
Close	Closes SecureLogin.

This list of tasks is also available by clicking Start > Programs > Novell SecureLogin > Display Menu. If SecureLogin is running, Display Menu provides an alternative for opening the task bar menu. If SecureLogin isn't running, Display Menu starts SecureLogin. If a new user, who hasn't run SecureLogin yet, clicks Display Menu, SecureLogin prompts the user to set up a passphrase.

Adding Applications

To add applications, use the Add Applications Wizard. Pop-up prompts enable you to launch the wizard as you log in to new Windows, Web, Advanced Web, or Java applications, or you can manually launch the wizard.

The Add Applications Wizard helps you generate login scripts and store variables (for example, usernames and passwords). The Wizard captures login data to use in SecureLogin prebuilt scripts or creates new scripts for Windows, Web, and Java applications.

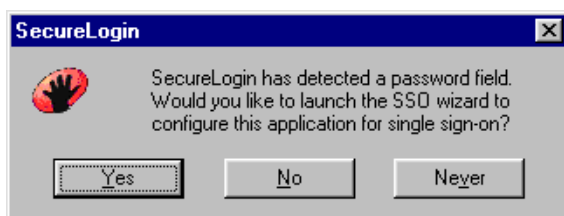
The wizard-generated login scripts store your login name, password, and any other information required for authentication. Scripts are stored in the local database and in the directory. The wizard is only available from the workstation. It isn't available in the SecureLogin snap-in to ConsoleOne® or in Active Directory Users and Computers.

Responding to Pop-Up prompts

After SecureLogin is installed on your desktop, SecureLogin watches for applications that aren't enabled for single sign-on. Upon detecting such an application, SecureLogin prompts you to use SecureLogin wizards that enable those applications for single sign-on and thereby simplify future logins.

Prompts for Windows Applications

After detecting a Windows login panel, SecureLogin displays the following dialog box. (If the application has a prebuilt script, the initial text varies.)

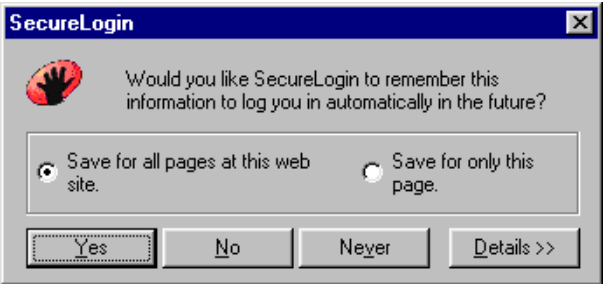


You can choose not to enable single sign-on for this application. If you select to not be prompted during future encounters, SecureLogin generates a blank script for this application and doesn't prompt you again.

If you click Yes, SecureLogin launches the Add Applications wizard, which guides you through the setup and creates a script for the login panel. The next time you open the application, SecureLogin authenticates for you.

Prompts for Web Pages

When you navigate to a Web page that has a login field and then submit your login information, SecureLogin prompts you whether to enable single sign-on for the site, for only the current page, or not at all.

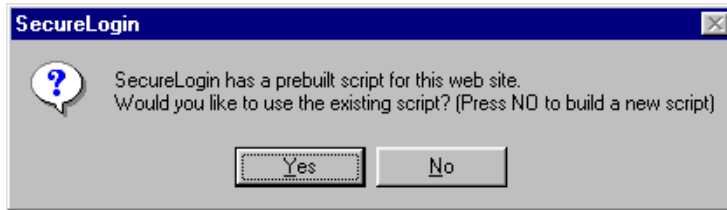


If you click Yes, SecureLogin extracts the login information from the Web page and stores it for future single sign-on authentication.

Option	Description
Save for All Pages at This Web Site	Saves the script against the base URL of the page (for example, mail.yahoo.com).
Save for Only This Page	Saves the script against the exact URL of the page (for example, http://login.yahoo.com/config/mail?.intl=au).
Yes	Creates a script, automatically reads the credentials entered into the browser, and stores the credentials against suitable variables. The next time the Web page is loaded, SecureLogin enters your credentials.
No	Doesn't create a script. The next time the Web page is loaded, SecureLogin displays the prompt again.
Never	Creates a blank script with no variables. The next time the Web page is loaded, you aren't automatically logged in or prompted to enable the Web page for single sign-on.
Details	Changes the URL that is saved with the script. Select a URL suggestion from the drop-down list or enter a URL. See the following figure.

Prompts for Applications That Have Prebuilt Scripts

When SecureLogin detects a login panel for an application that has a prebuilt script, SecureLogin prompts you with the option to implement that script. The following figure illustrates a prompt for a Web site:



To enable the script, click Yes, then enter the required credentials. SecureLogin logs you into the application whenever the application is launched.

To ignore the prompt, click No. The next time SecureLogin detects the application's login panel, SecureLogin displays this prompt again.

Manually Adding Applications

If the Add Application Wizard doesn't run automatically, you can launch it:

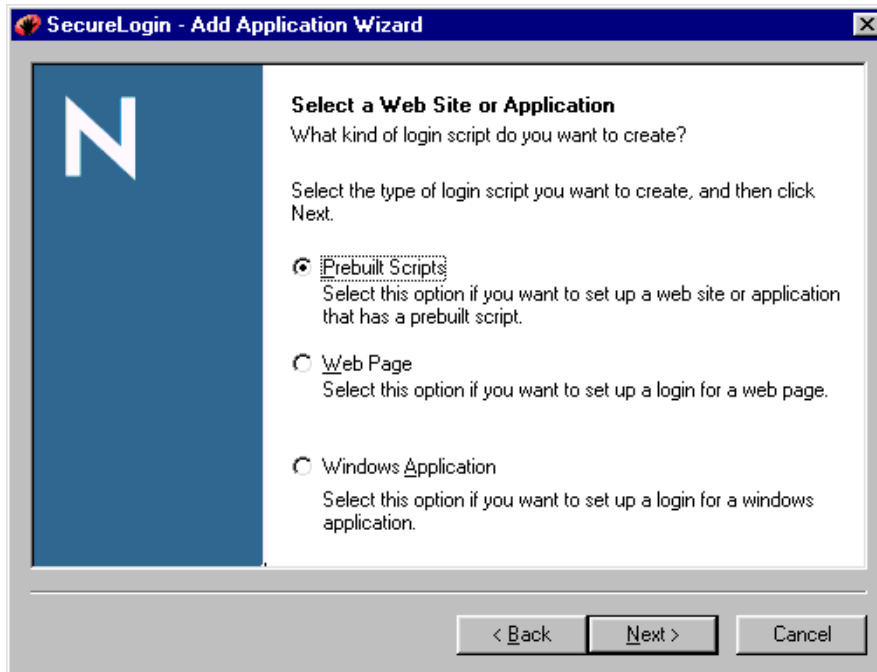
- 1** Right-click the system tray icon.
- 2** Click Add Applications.
You can also click Start > Programs > Novell SecureLogin > Novell SecureLogin > Applications.
- 3** At the Welcome dialog box, click Next.
- 4** Add an application that has a prebuilt script, add a Web application, or add a Windows application.

Using Prebuilt Scripts

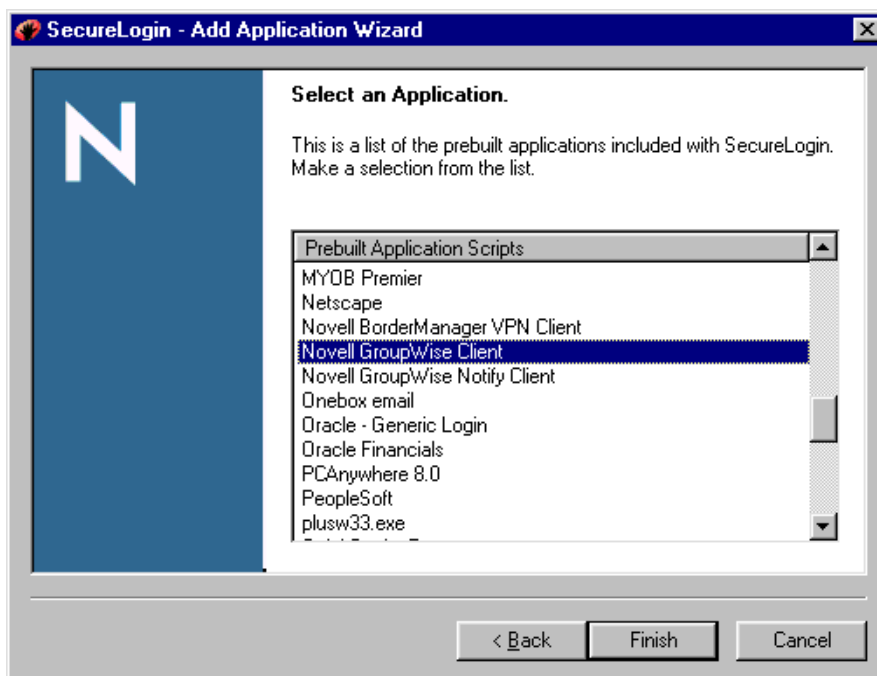
Scripts store certain login information so that it can be used again and again. To save you the time and trouble of setting up scripts, SecureLogin provides prebuilt scripts for many applications.

To add an application that has a prebuilt script:

- 1** Right-click the SecureLogin icon on the system tray, then click Add Applications.
- 2** At the Welcome window, click Next.
- 3** Click Prebuilt Scripts, then click Next.

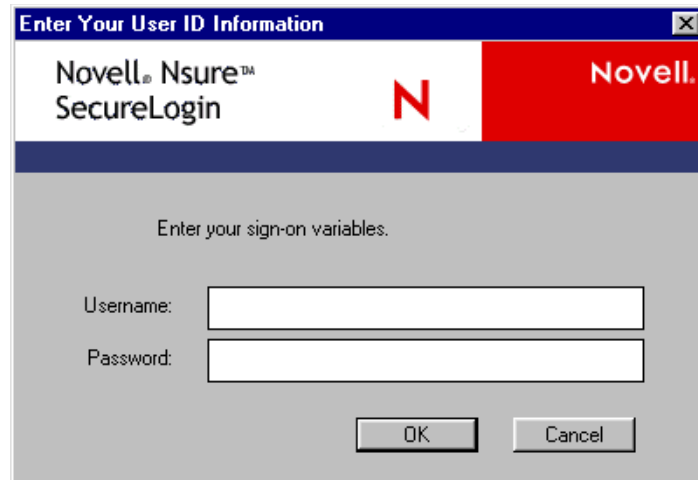


- 4 Select the application from the list, then click Finish.



- 5 Provide a login.

As the following figure illustrates, when you next launch the application, SecureLogin prompts you to enter login variables.

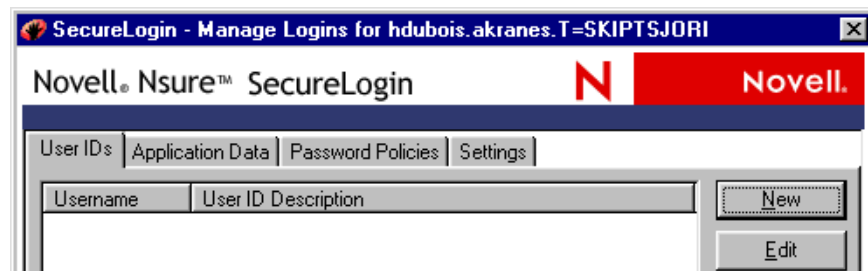


After you type the variables and click OK, SecureLogin saves this data and logs you in. For subsequent launches, SecureLogin automatically logs you in.

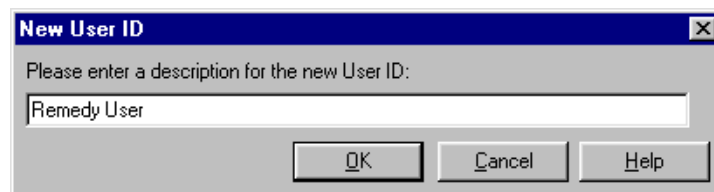
You can also provide login data manually:

5a Right-click the SecureLogin icon on the system tray, then click Manage Logins.

5b Click User IDs > New.

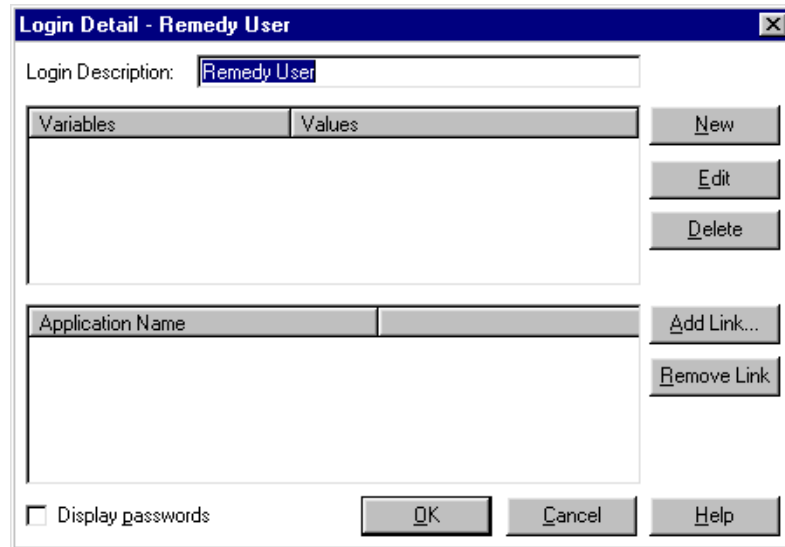


5c Type a description for the user ID, then click OK.



Typically, enter the application name.

5d Type login variables.



Login Detail - Remedy User

Login Description:

Variables	Values

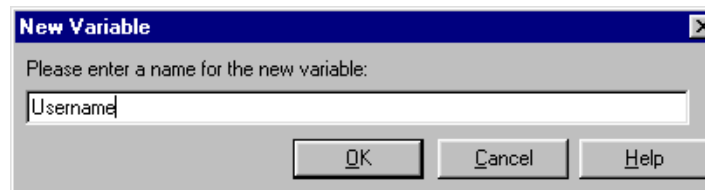
Application Name:

☐ Display passwords

Buttons: New, Edit, Delete, Add Link..., Remove Link, OK, Cancel, Help

Entering a Name in the Variables Column

To enter a name in the Variables column, click New, type a name (for example, Username), then click OK.



New Variable

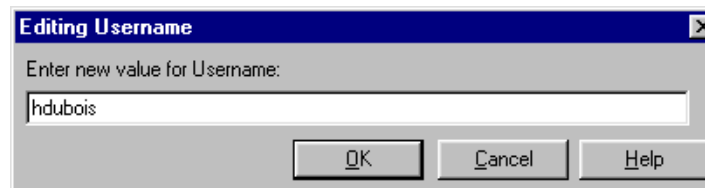
Please enter a name for the new variable:

Buttons: OK, Cancel, Help

"Username" is a typical entry. However, it's a good idea to use the text that appears on the login panel. For example, text for a Windows application might be User Name or User ID, but text for a Web page that logs you in to a bank might be Account.

Entering a Value

The entry in the Variables column requires a matching value. In the Editing Username dialog box, type the value (for example, the actual username), then click OK.

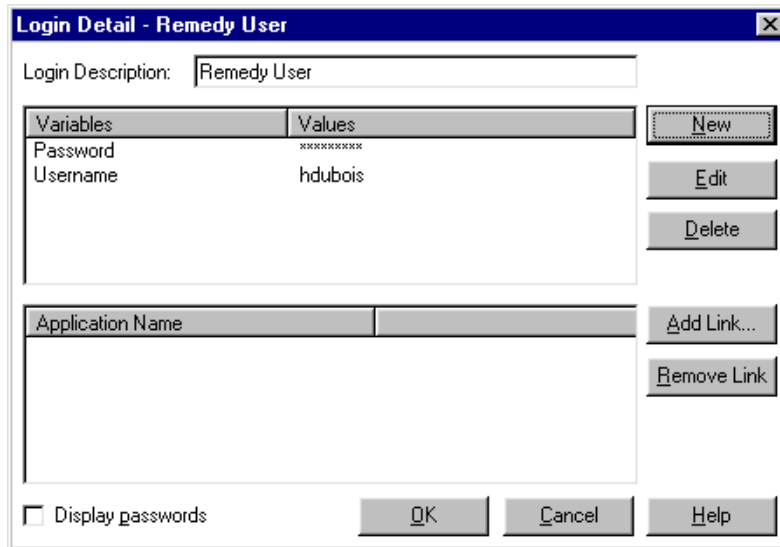


Editing Username

Enter new value for Username:

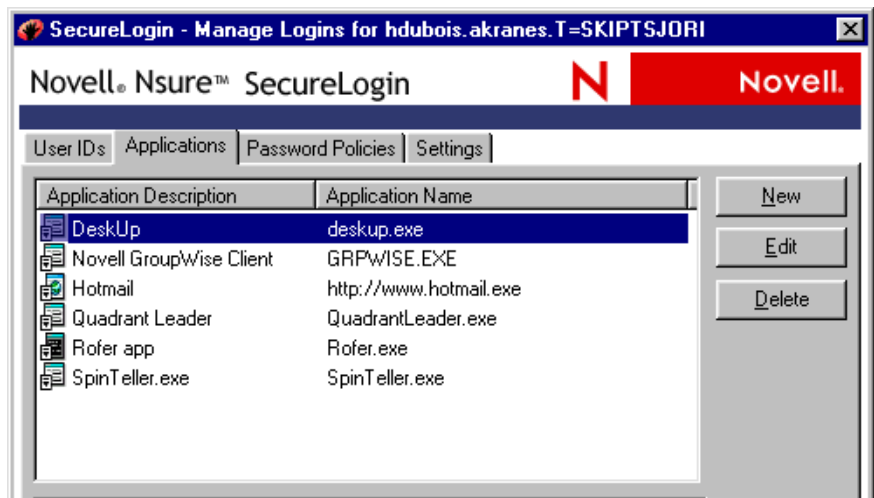
Buttons: OK, Cancel, Help

Add other variables (for example, Password) and matching values (for example, the actual password) as required in the login panel.



If you have already saved values, you can edit them. For example, to change a password, click the Password variable, click Edit, then type and confirm the new password.

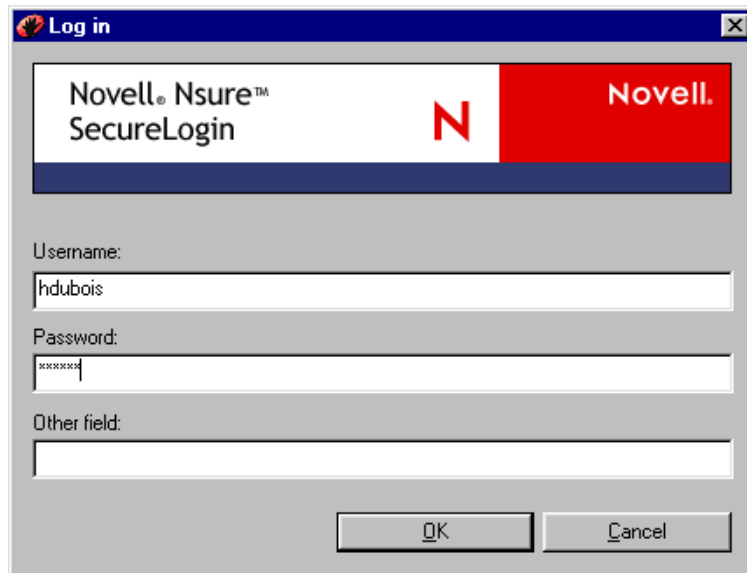
Save the variables and values for the login by clicking OK, then save the data to cache by clicking OK.



Adding a Windows Application

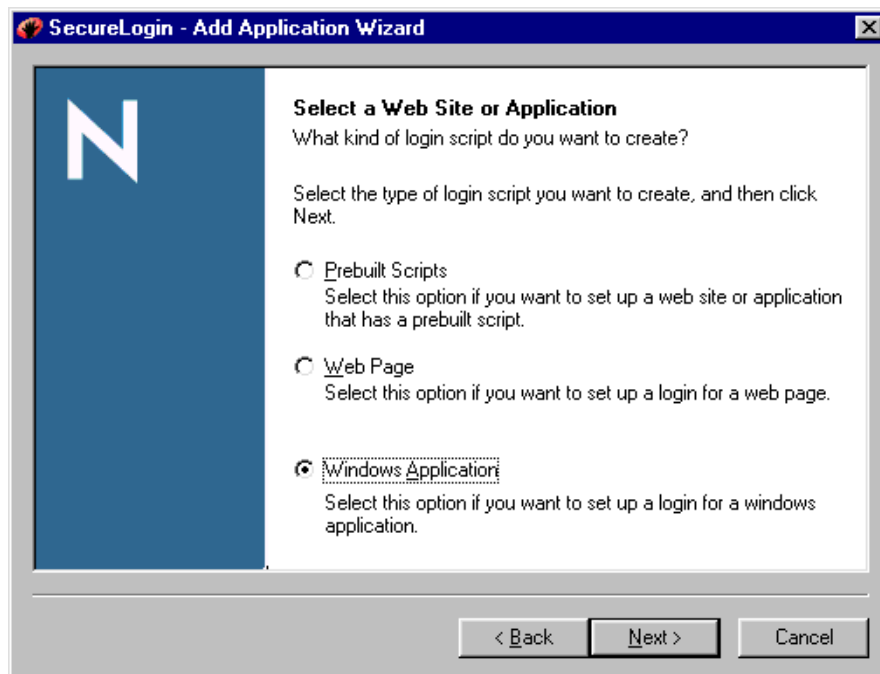
The following steps apply when SecureLogin doesn't automatically detect a new application. If SecureLogin detects a new application and launches the Add Application Wizard, go to Step 6. For information on SecureLogin's pop-up prompt, see ["Responding to Pop-Up prompts" on page 65](#).

- 1** Launch the application and drag the login panel to one side of the screen.
- 2** Type login information (for example, username and password), but don't click OK, Next, or Finish.

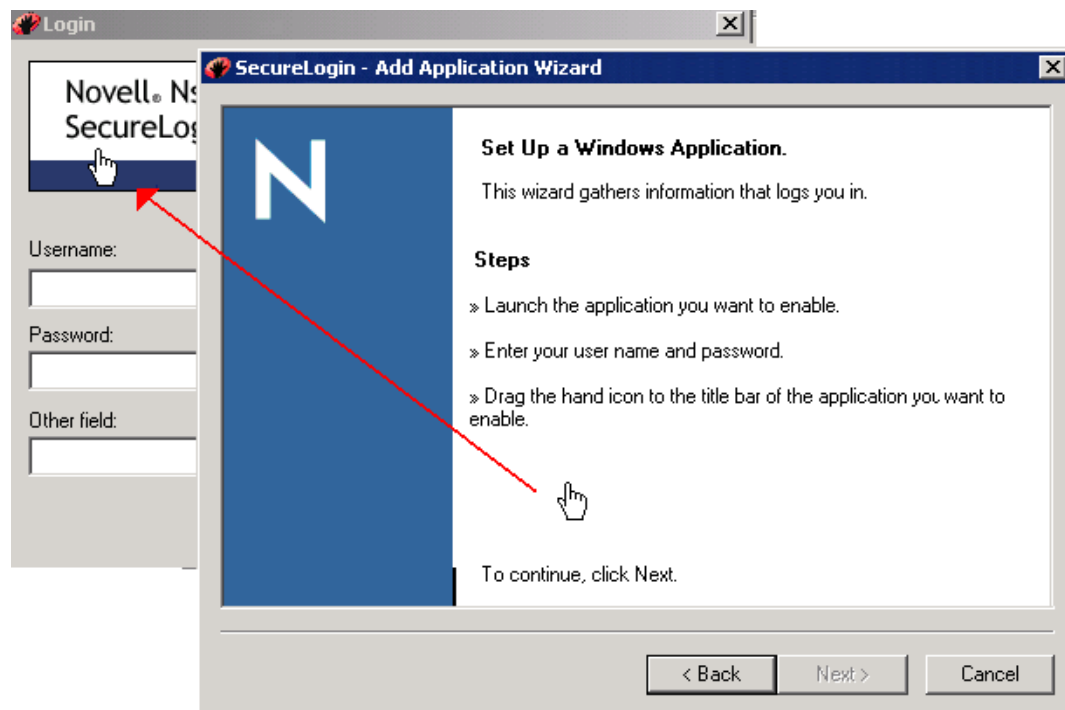


The login panel needs to remain so that SecureLogin can capture the information on the panel.

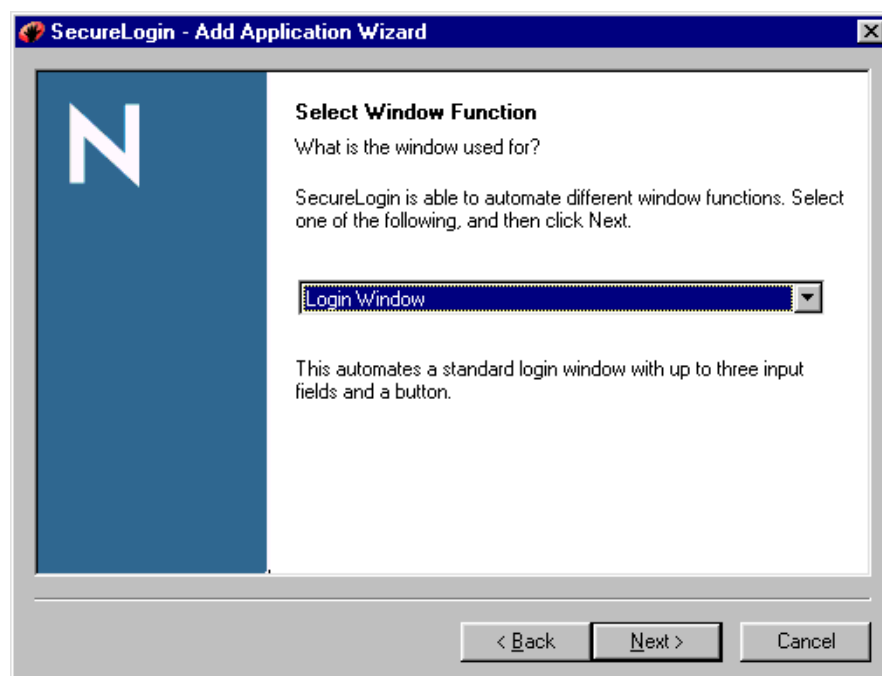
- 3** Right-click the SecureLogin icon on the system tray, then click Add Applications.
- 4** Click Next > Windows Application > Next.



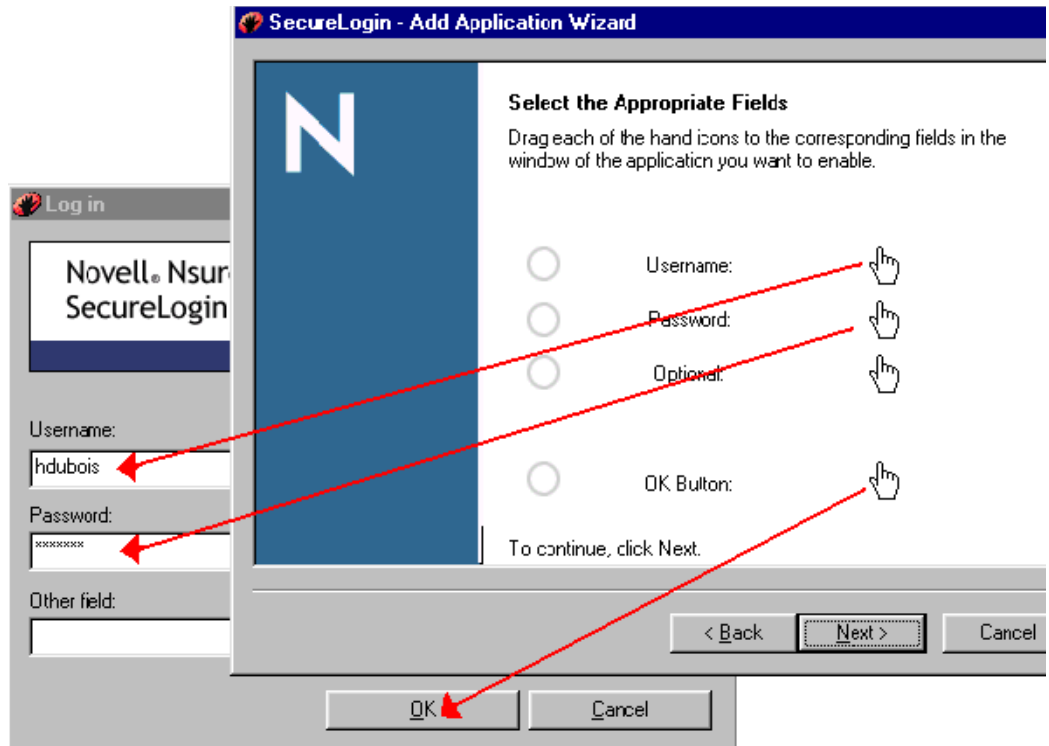
- 5** At the Set Up a Windows Application window, drag the hand to the title bar.



- 6 At the Select Window Function window, select Login Window from the drop-down list, then click Next.



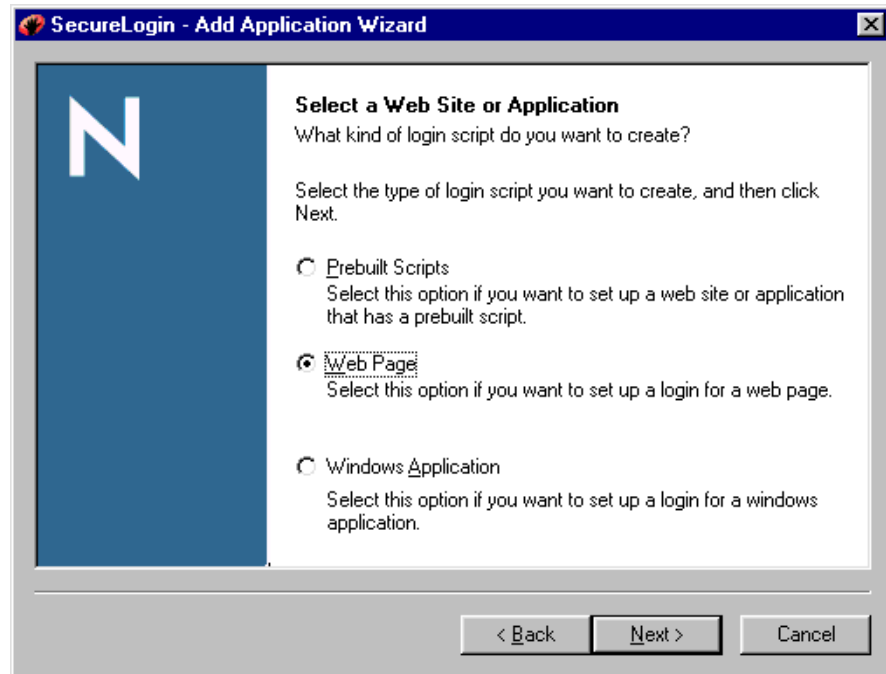
- 7 Select the login fields.



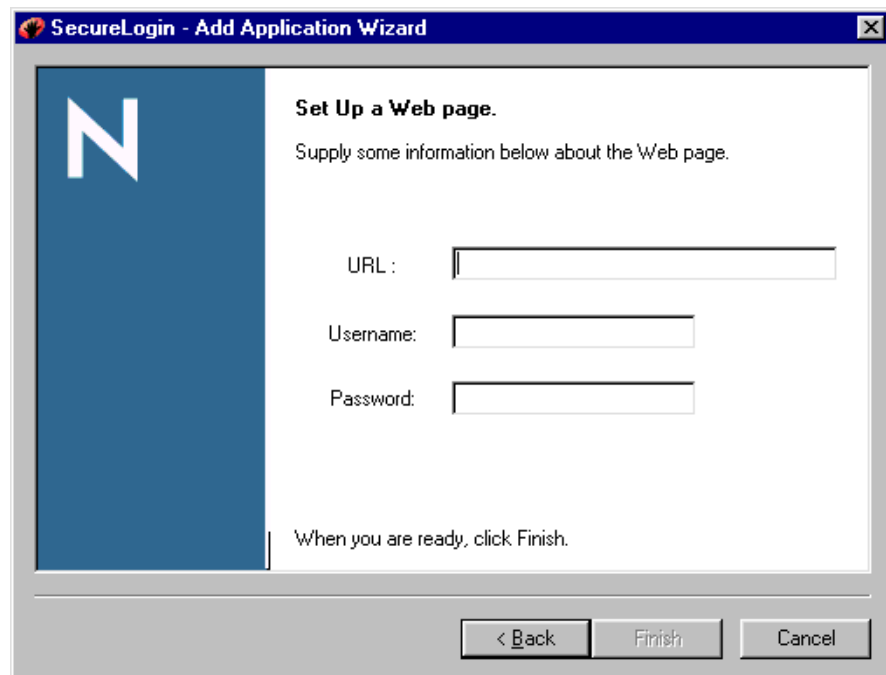
- 7a** Drag the hand icons and drop them onto the corresponding Username, Password, and (if appropriate) Optional fields on the login panel.
- 7b** Drag the hand icon for the OK Button and drop it onto the OK, Next, Continue, or similar button.
- 7c** Click Next.
- 8** At the Confirm Details dialog box, verify that your username is correct and that a password exists, then click Next.
- 9** At the Name the Script window, accept the default name (or select a name from the drop-down list or type a new name) for the application, then click Finish.

Adding a Web Application

- 1** From a browser, go to the URL of the Web page that you want to log in to.
- 2** Right-click the SecureLogin icon on the system tray, then click Add Applications.
- 3** Click Next > Web Page > Next.



- 4 At the Set Up a Web Page dialog box, copy and paste the URL, type your username and password, then click Finish.



If you have difficulty logging in to a Web site, see “Why is SecureLogin unable to log me in to some Web sites?” on page 119.

Adding a Java Application

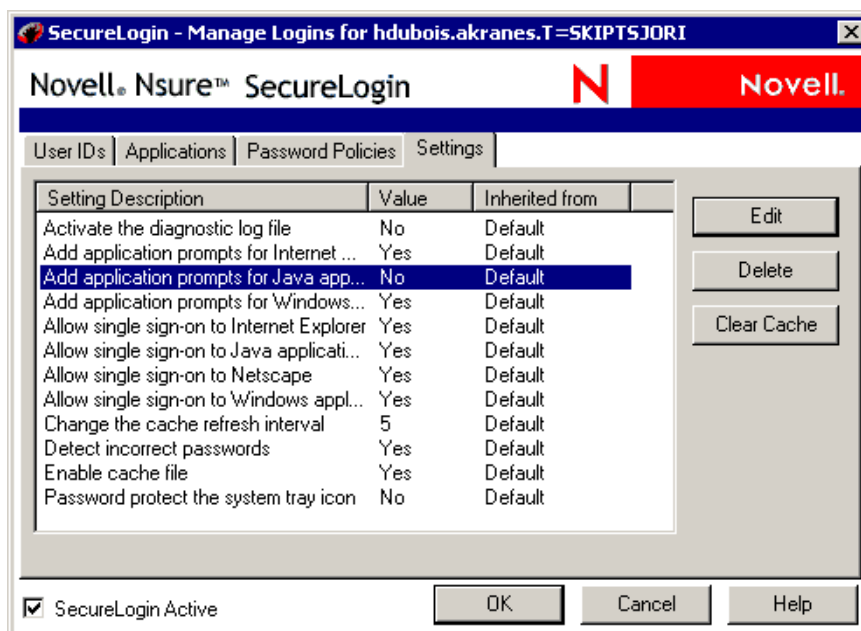
Prerequisites

- ♦ Sun Microsystems Java Runtime Environment (JRE) 1.4.2 or later is installed on the workstation.
- ♦ Following installation of the JRE, SecureLogin 3.51 is installed on the workstation.
- ♦ You have advanced knowledge of scripting.

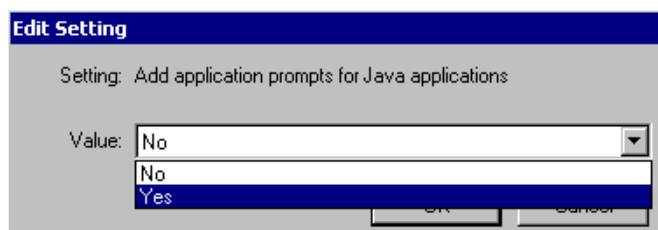
Enabling the Add Applications Wizard for Java

When the JRE is installed, the SecureLogin installation program installs Java support by default. However, when SecureLogin first launches, the Add Application Wizard for Java is disabled. To use Java applications, you must enable the Add Applications Wizard for Java.

- 1 Right-click the SecureLogin icon on the system tray, select Manage Logins, then click Settings.



- 2 Select Add Application Prompts for Java Applications, then click Edit.
- 3 Change the value to Yes, then click OK.



- 4 Save the data by clicking OK.

Adding the Java Application to the List of Applications

1 Launch the Java application.

The Java application can be an applet or an executable file.

SecureLogin displays the following message:

```
Java SSO has detected a new platform. Would you like to generate a script
for it?
```

NOTE: The script will only contain the list of controls in this Java program. It will need to be modified to achieve full functionality.

2 (Conditional) If the dialog box that appears isn't the one that you want SecureLogin to learn for the Java application, click No.

3 Navigate to the dialog box that you want SecureLogin to learn, then click Yes.

Multiple instances of the "Java SSO" message appear for every instantiation of the Java application.

4 Close the application.

5 On the Setting tab, set the Add Application Prompts for Java Applications to No, then save the data.

6 Verify that the application has been added.

View the applications listed on the Applications page. SecureLogin displays a new icon and application type.

However, the user IDs are blank and several lines in the Description column are commented out. The number of lines depends on the application.

Also, the number of control boxes (edit, OK, Cancel) depends on the application. For example, an application might have three edit boxes. Control #1 might be the Username field, defined with its Java class. Control #2 might be the Password field, with its Java class. Control #3 might be an Other field, also defined by its Java class. The control numbers might be as follows:

Control	Field	Control ID Number
Edit box 1	Username field, defined with its Java class	1
Edit box 2	Password field, defined with its Java class	2
Edit box 3	Other field, defined with its Java class	3
Button	OK	4
Button	Cancel	5

7 Provide a script for the Java application.

To provide a script for a Java application, you need advanced scripting knowledge. We recommend that a consultant help you with advanced Java applications.

A basic script follows:

```
Dialog
Type $Password
Type Control #2
```

```

Type $Username
Type Control #1
Type Control #3
Delay 1000
Click #1
EndDialog

```

Many Java applications require a Delay command, so that user ID information can be entered before the OK button is clicked. This script types the password, types the username, types the Other field, waits 1,000 milliseconds, moves the mouse to the OK button, then clicks the OK button.

With Java applications, Raw submits (as found in scripts for Windows and Web applications) are not supported.

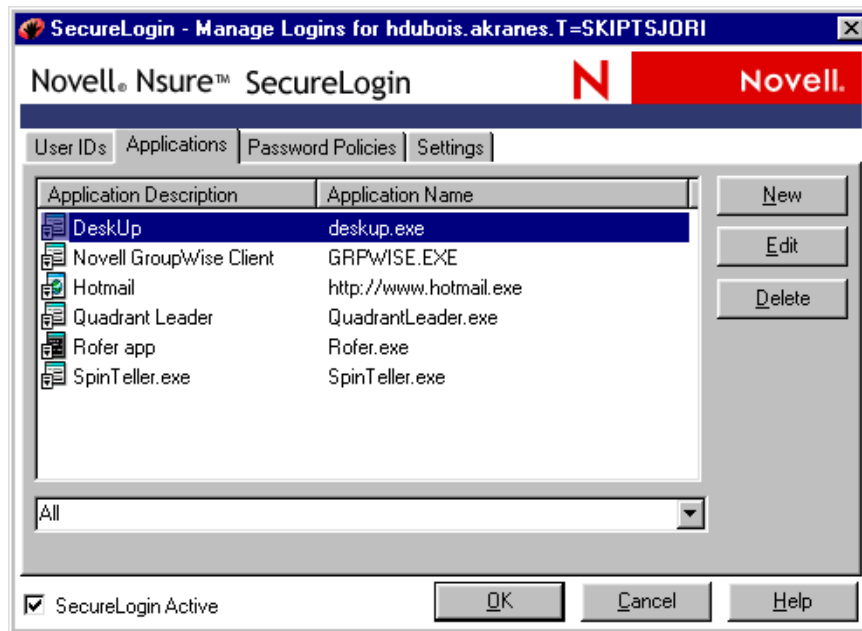
- 8 Launch the Java application, then enter user information.

SecureLogin collects the information that you enter, executes, and logs you in.

Linking User IDs to Applications

You use applications to do your work. If an application is password protected, you must log in to it. So that you can use SecureLogin to automatically log you in to an application, you create a user ID that you can link to that application.

The following figure illustrates SecureLogin's main window:



If you added an application that has a prebuilt script, you need to link a user ID to it. However, you don't need to add or create user IDs for applications that you enabled for single sign-on in the following ways:

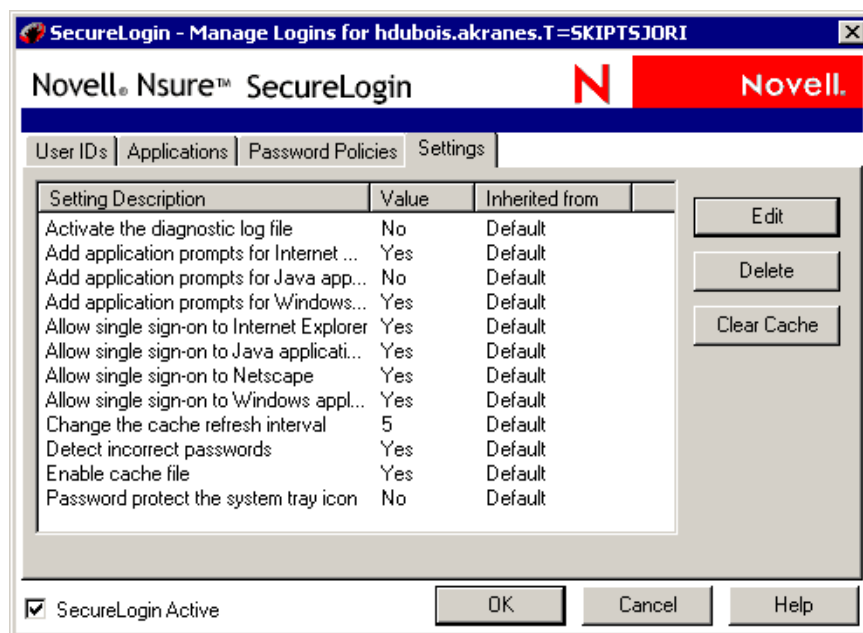
- ◆ You encountered a new application through a pop-up prompt and then used the Add Applications wizard to enable the application.
- ◆ You ran the Add Applications wizard and selected a Web Page or Windows Application option as the script type.

In these two cases, SecureLogin's Add Application wizard created the user ID while you were adding the application to SecureLogin's single sign-on functionality.

For information on managing user IDs, applications, and password policies, refer to the help system.

Changing Settings

As the following figure illustrates, users with access to the SecureLogin icon on the system tray can apply settings to a workstation:



The list in the Setting Description column is a subset of settings you control through ConsoleOne. For information on these and the complete list, see [“Configuring SecureLogin Settings” on page 41](#).

To clear the entries in the local cache, click Clear Cache. The cache file is updated at the next refresh. You might want to clear the cache if SecureLogin behaves strangely (for example, loss of sync with passwords, or having multiple credential sets when only one should exist).

Disabling the Workstation's Cache

So that you can use login data when you work offline (for example, on a disconnected laptop), you can store login data in encrypted files on your workstation.

If you forget the passphrase answer password and are not able to log in using your directory password, you will have to delete and recreate the cache files. SecureLogin automatically re-creates cache files, provided you are authenticated to the network.

The only time a user needs to delete a local cache is when the user is locked out of both the directory and the local cache. This would happen if you as administrator reset the user's password and the user can't remember the passphrase answer. You would then go to the User object in ConsoleOne and clear user data. The user would then need to delete the local cache files and add login information again.

To disable the cache:

- 1 Double-click the SecureLogin icon on the system tray.
- 2 Click Settings > Enable Cache File.
- 3 Set the value to No, then click OK.

Toggling the Active Setting

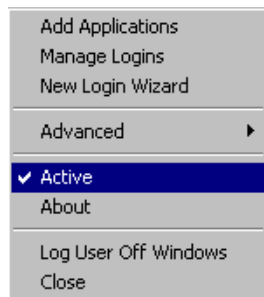
You can use the Active setting to override all the settings and disable SecureLogin.

Scenario: Writing a New Script. You have started writing a script for an application. Because you need to inspect some control IDs with Window Finder, you do not want the script to run at this time. You disable the Active setting. SecureLogin doesn't run while you fine-tune the script. After troubleshooting, you click Active. SecureLogin is functional again.

Scenario: Troubleshooting an Existing Script. You have a script already written for an application. You open the application to get more information from it, so that you can put the information in your script. Because the Active setting is used, the script for the application runs.

You don't want to wait for the script to run while you look for control IDs. Therefore, you close the application, click Active to disable SecureLogin, then open the application. You then get the information that you need, return to your script, enter the information into the script, toggle to Enable, then run the script.

The Active setting can also be useful for the help desk to use in troubleshooting, so that a technician can manually step through a login.



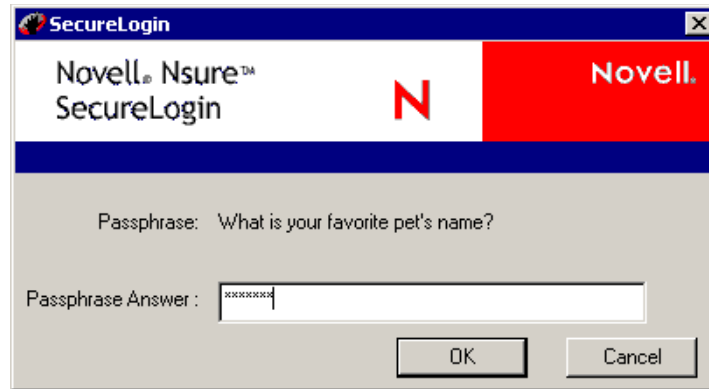
To toggle the Active setting:

- 1 Right-click the SecureLogin icon on the system tray.
- 2 Click Active.

Changing Your Passphrase

If the network administrator allows you to, you can change a passphrase question and answer:

- 1 Right-click the SecureLogin icon on the system tray.
- 2 Click Advanced > Change Passphrase.
- 3 Type your existing passphrase answer.



- 4 Edit the passphrase question, passphrase answer, or both, then click OK.

4

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.).



Include the filename extension.

- 4 Click Start.

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



- 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 || || ComboBox || 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.

5

Working with Terminal Emulators

This section provides information on the following:

- ♦ “Terminal Launcher” on page 85
- ♦ “Setting Up Terminal Emulation” on page 86
- ♦ “Setting Up a Shortcut” on page 104
- ♦ “Configuring Backup Sessions” on page 106
- ♦ “Determining Which Session File To Automatically Use” on page 106
- ♦ “Using Terminal Launcher With Non-HLLAPI-Compliant Emulators” on page 107

Terminal Launcher

Terminal Launcher, a component of SecureLogin, enables users to log in to any type of host that requires a login using an emulator (for example, ACF2 or RACF mainframe, a UNIX host, or a Cisco router).

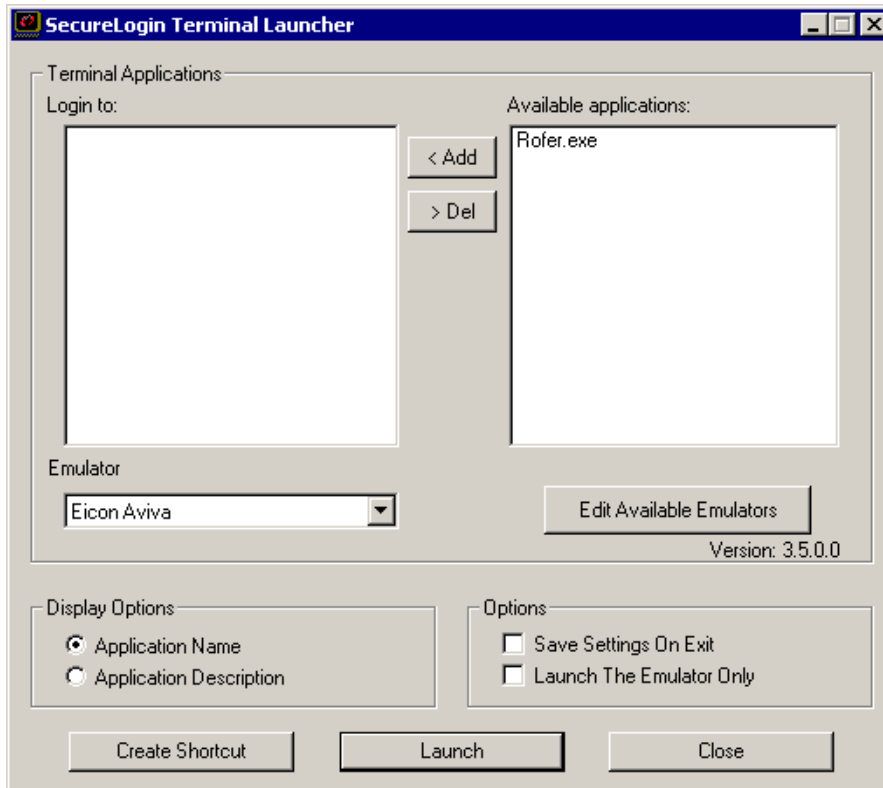
Terminal Launcher supports the following emulator types:

- ♦ HLLAPI
- ♦ DDE
- ♦ VBA
- ♦ Generic
- ♦ Advanced Generic

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.

The following figure illustrates Terminal Launcher’s main window.



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 Scripting Guide](#).

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

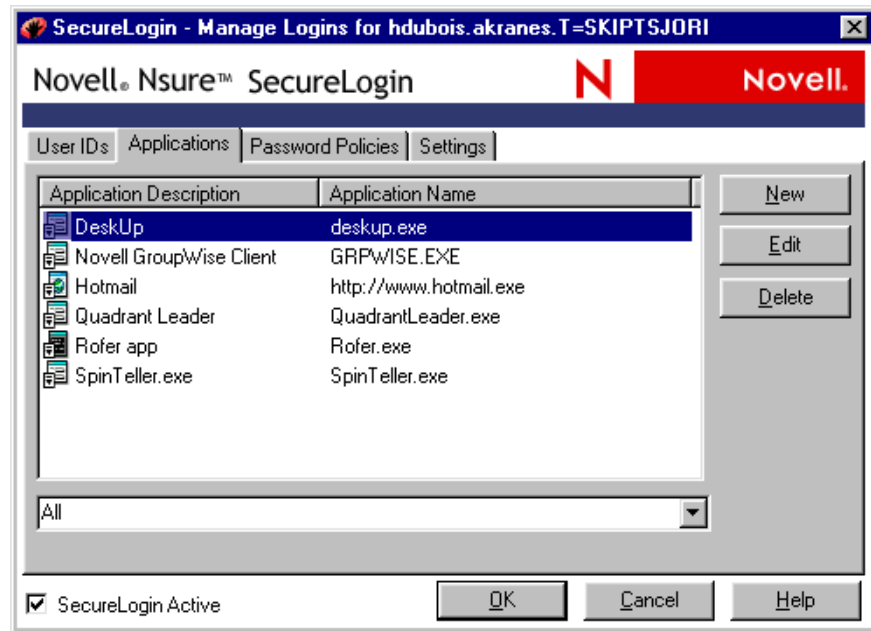
Setting Up Terminal Emulation

To set up terminal emulation, create a script for the emulator, specifying Terminal Launcher as the script type. Then configure the emulator and create a login.

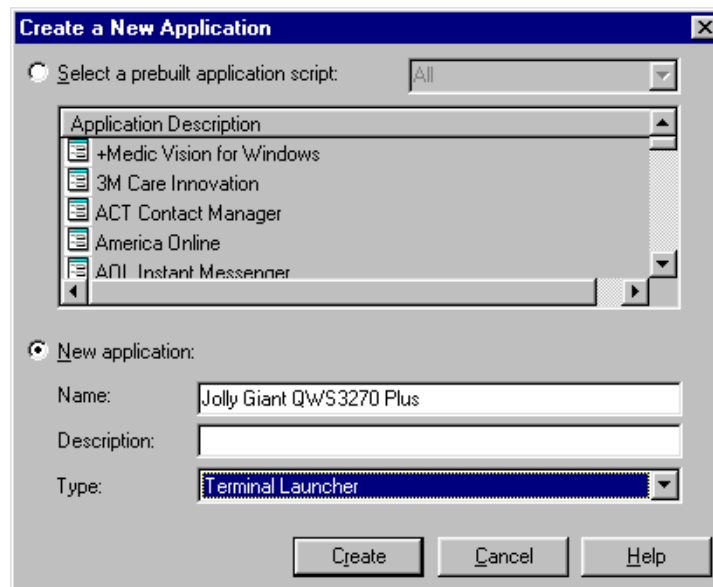
Creating a SecureLogin Script

The following example sets up SecureLogin Terminal Launcher to single sign-on to a session using Jolly Giant QWS3270 Plus.

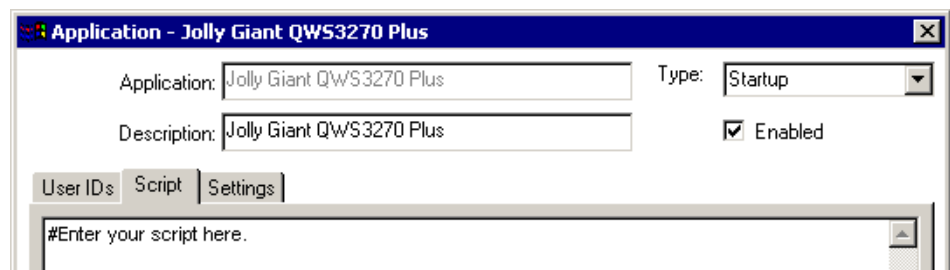
- 1 Double-click the SecureLogin icon on the system tray, click Applications, then click New.



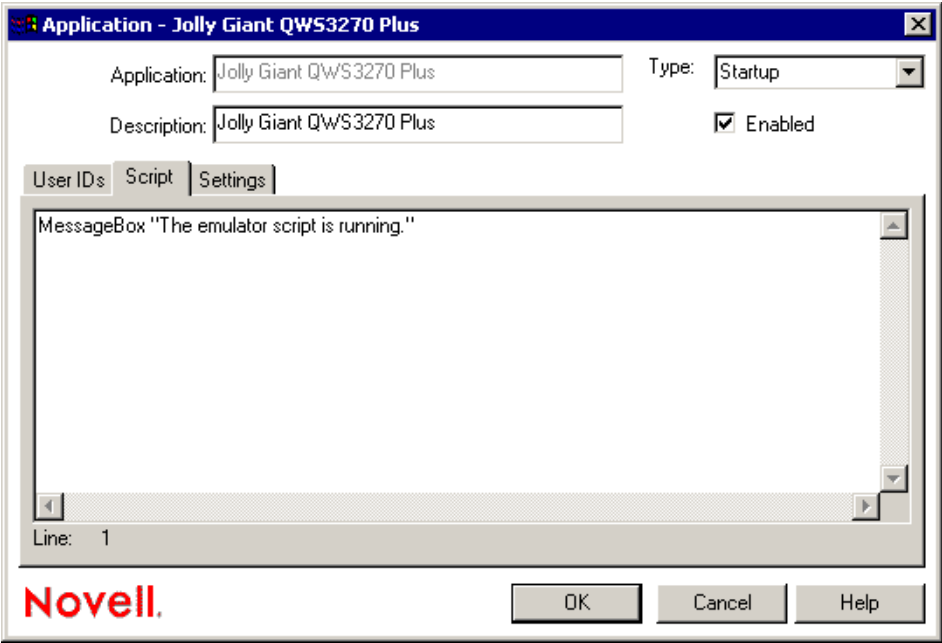
- 2 Select New Application, type a name in the Name text box, select Terminal Launcher as the type, then click Create.



- 3 Click Script.



4 Type a single command, then click OK.



For example, type a MessageBox command. By entering one command, you can find out the following:

- ◆ Terminal Launcher is working as expected.
- ◆ The script is ready for you to enter the appropriate commands.

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

Configuring Terminal Launcher

SecureLogin Terminal Launcher includes configurations for the following emulators:

Emulator	Emulator
Attachmate* Extra*	NetTerm v4.2
Attachmate Extra 2000	NS/Elite
Attachmate KEA!	PASSPORT* TN 3270E
Chameleon* Hostlink	QVT
Eicon* Aviva*	QWS3270 Plus
GLink	SDI* TN3270
HBO Star Navigator	TeraTermPro
IBM* Personal Communications	TLaunch Options
IDXTerm Healthcare	ViewNow
Info Connect	Wall Data RUMBA*

Emulator	Emulator
Microsoft* Telnet 2000	Wall Data RUMBA 2000
Microsoft Telnet NT	Wall Data RUMBA Web To Host
Microsoft Telnet Win 9x	Windows Telnet VT
Mocha W32 Telnet	WRQ* Reflection*

If an emulator doesn't have a predefined script, you can configure Terminal Launcher to do the following:

- ♦ Connect to the mainframe or host, wait for the login sequence, then enter usernames and passwords.
- ♦ Work with a range of different terminal emulators.
- ♦ Navigate to a particular subsystem or menu within an application.
- ♦ Incorporate into SecureLogin scripts any keystrokes that an application accepts, so that Terminal Launcher can send the keystrokes to the host.

At the corporate level, one script can accommodate all users. SecureLogin applies user-specific variables.

To configure Terminal Launcher you must specify any required mainframe session file and the path to the emulator executable.

Configuring WinHLLAPI, HLLAPI, or 16-Bit HLLAPI Emulators

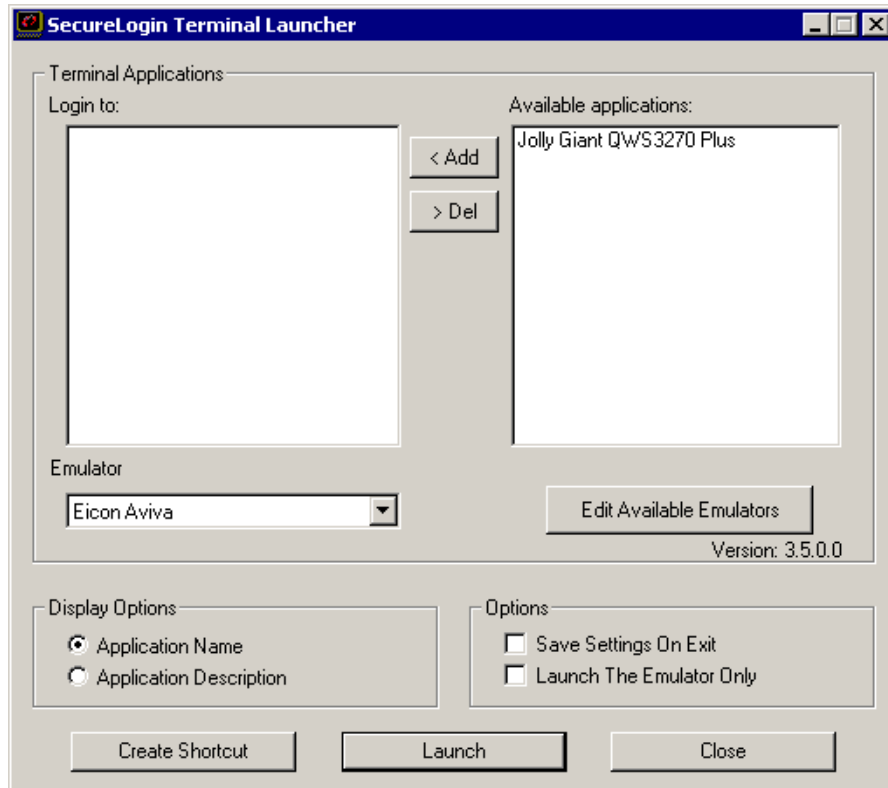
This section can help you configure WinHLLAPI, HLLAPI, or 16-bit HLLAPI emulators. If you select the wrong HLLAPI type, however, Terminal Launcher will fail. To find out the HLLAPI type, do one of the following:

- ♦ 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.

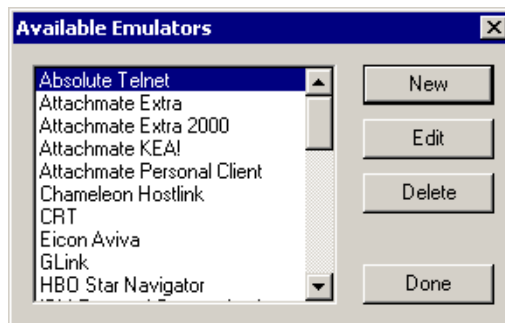
TIP: Most HLLAPI-based emulators require you to configure HLLAPI short session names (normally A-Z) and link them with the session files or the main application. Otherwise, SecureLogin won't be able to determine which HLLAPI session to send responses to, and it will appear that SecureLogin isn't working.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

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

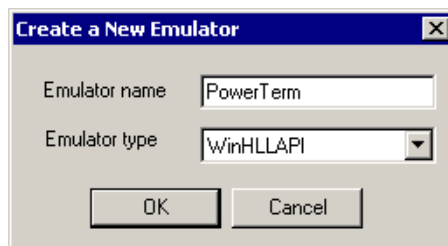
As the following figure illustrates, Terminal Launcher displays the application that you created the script for:



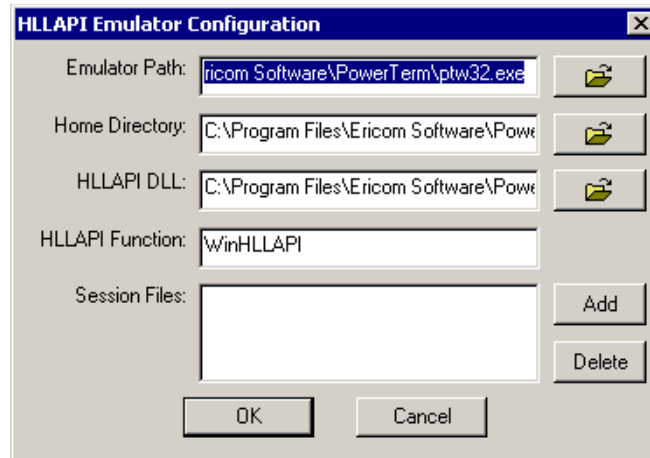
2 Click Edit Available Emulators > New.



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



4 Type values, then click OK.



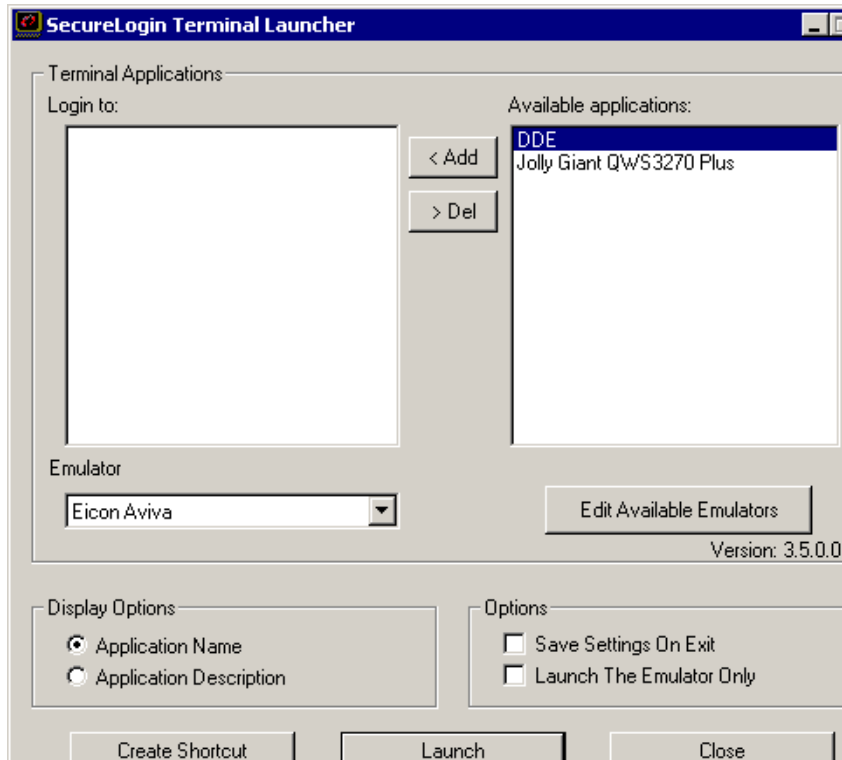
Field	Description
Emulator Path	The directory path and executable filename of the emulator. Either type the path or use the Browse button located to the right of the text box. You can type short (8.3 format) or long filenames. Enclose long filenames in quotes (for example, "c:\Program Files\emulator").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

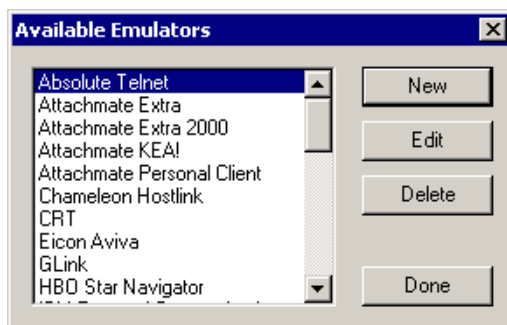
Configuring a DDE Emulator

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

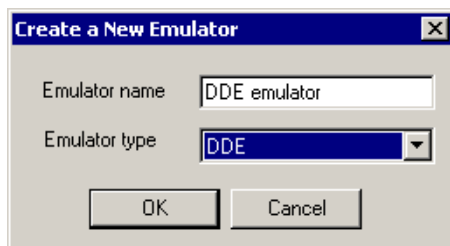
As the following figure illustrates, Terminal Launcher displays the application that you created the script for:



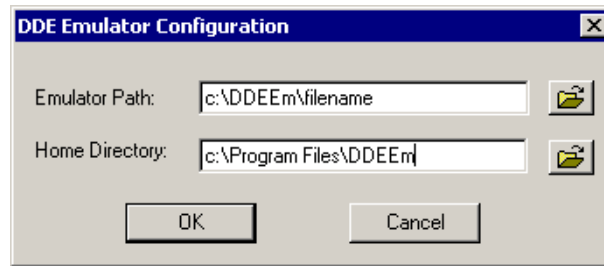
2 Click Edit Available Emulators > New.



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



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").
Home Directory	The directory path to where the executable is located.

- 5 In the Available Emulators dialog box, click Done.

Configuring a VBA Emulator

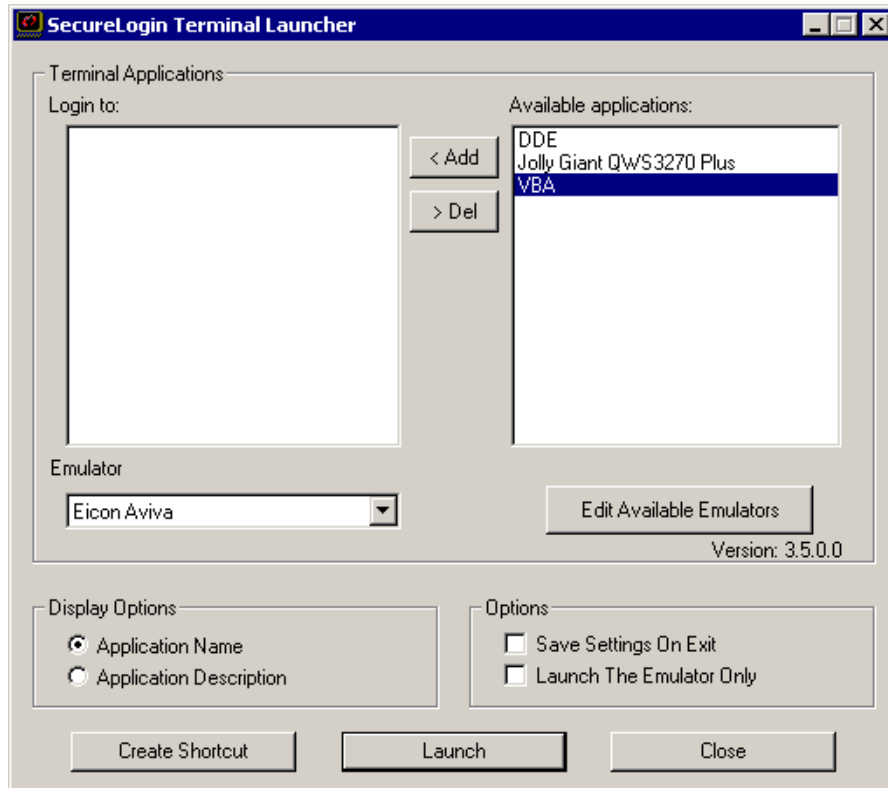
VBA emulators support the Visual Basic* scripting language. In most cases, it is possible to write a macro for the emulator. The macro prompts SecureLogin to enter credentials.

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

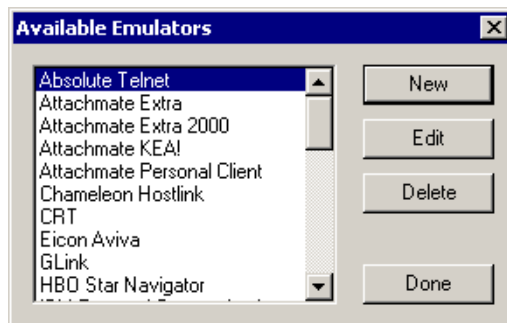
VBA emulators can often be configured as Generic emulators. However, generic configuration offers limited functionality.

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

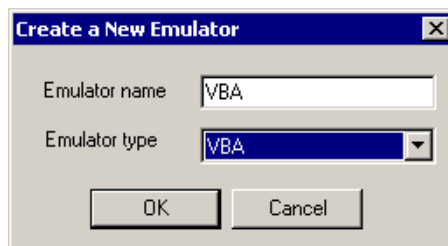
As the following figure illustrates, Terminal Launcher displays the application that you created the script for:



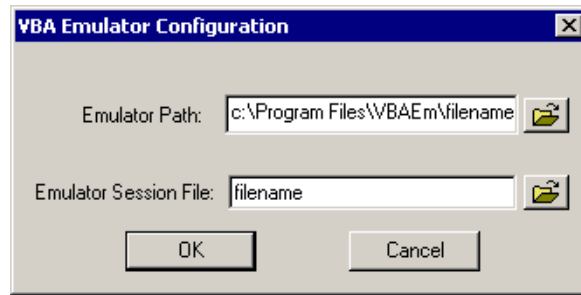
2 Click Edit Available Emulators > New.



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



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").
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 through 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 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.

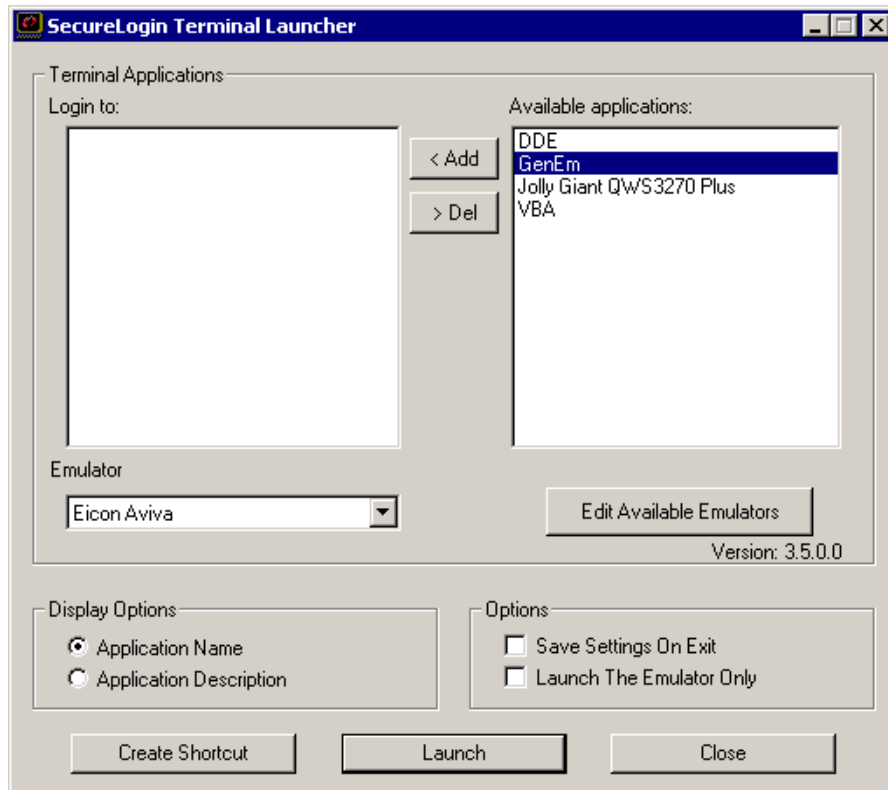
When using the Clipboard, Terminal Launcher copies the text (for example, a username) to the Clipboard and then simulates the selection of the Paste function of the emulator. This procedure

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.

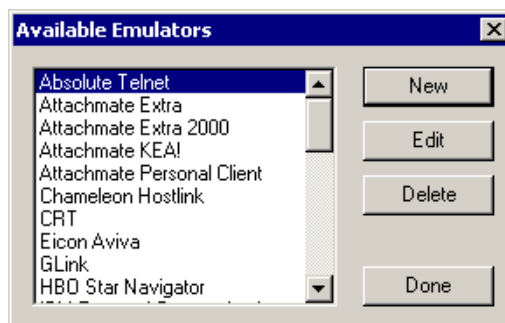
The process is then repeated for the password, and the user's login to the mainframe session is complete.

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

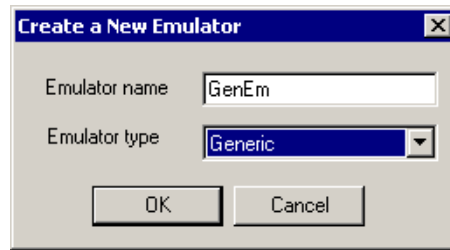
As the following figure illustrates, Terminal Launcher displays the application that you created the script for:



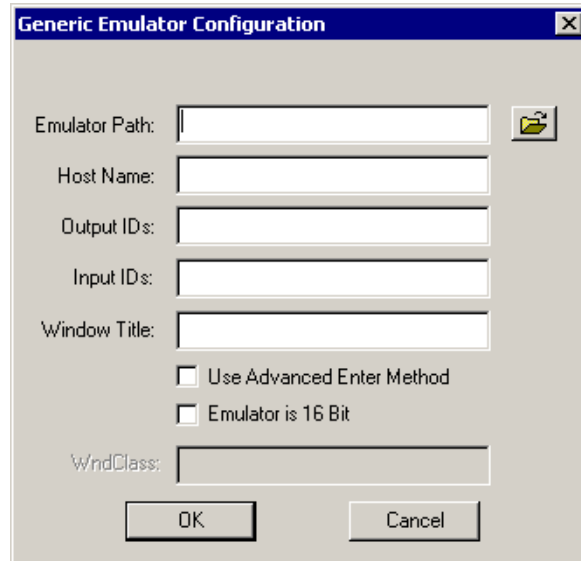
- 2 Click Edit Available Emulators > New.



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



- 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	<p>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.</p> <p>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.</p>
Output IDs	<p>The Control ID for the Copy function of the emulator. For information on finding Output IDs, see Appendix C, "Finding Control IDs and Offsets of an Emulator," on page 129.</p> <p>Some emulators allow a keyboard simulation alternative (for example, CTRL+C) instead.</p>

Field	Description
Input IDs	<p>The Control ID for the Paste function of the emulator. For information on finding Input IDs, see Appendix C, "Finding Control IDs and Offsets of an Emulator," on page 129.</p> <p>Some emulators allow a keyboard simulation alternative (for example, CTRL+C) instead.</p>
Window Title	<p>Assists Terminal Launcher in detecting the emulator window. If no Window Title is specified, Terminal Launcher might not detect the emulator opening.</p> <p>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.</p> <p>Some emulators hide the real Window Title.</p> <p>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.</p>
Use Advanced Enter Method	<p>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.</p>

- 5** In the Available Emulators dialog box, click Done.

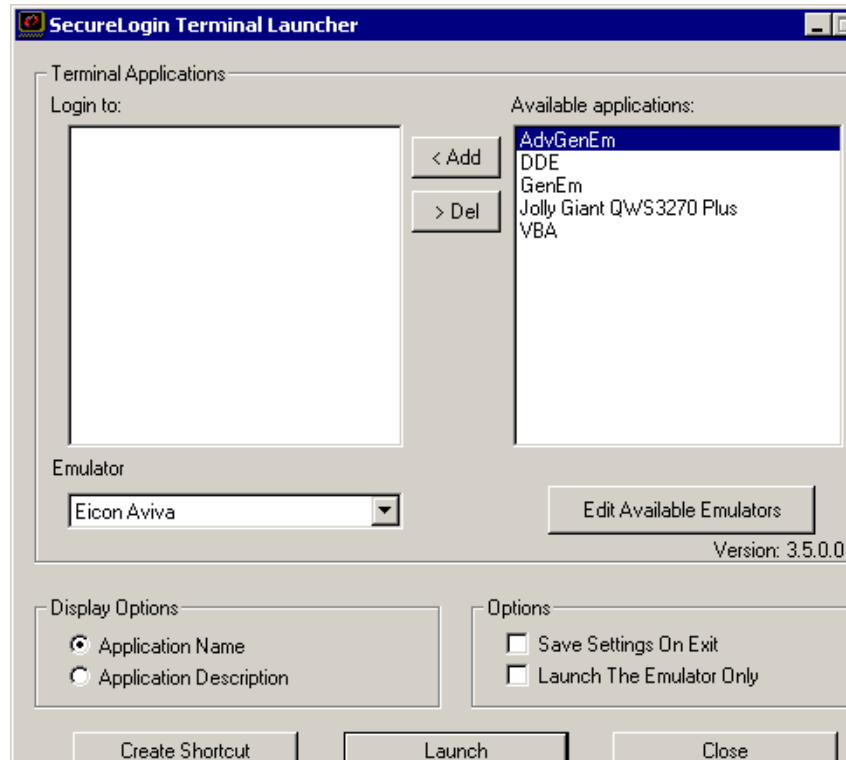
Configuring an Advanced Generic Emulator

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

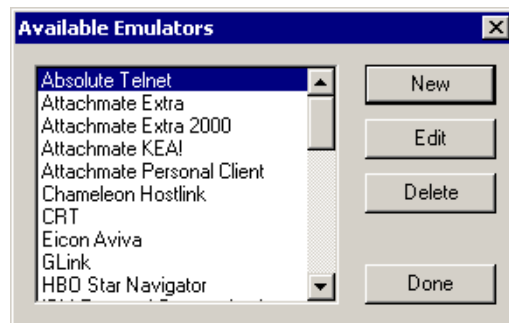
For advanced generic emulators, Terminal Launcher follows the same process as for generic emulators, except for one difference. Instead of simulating the selection of Select All, Terminal Launcher clicks and drags the mouse cursor over the emulator screen. This procedure selects all the text that the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

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

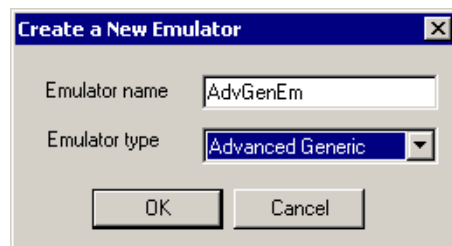
As the following figure illustrates, Terminal Launcher displays the application that you created the script for:



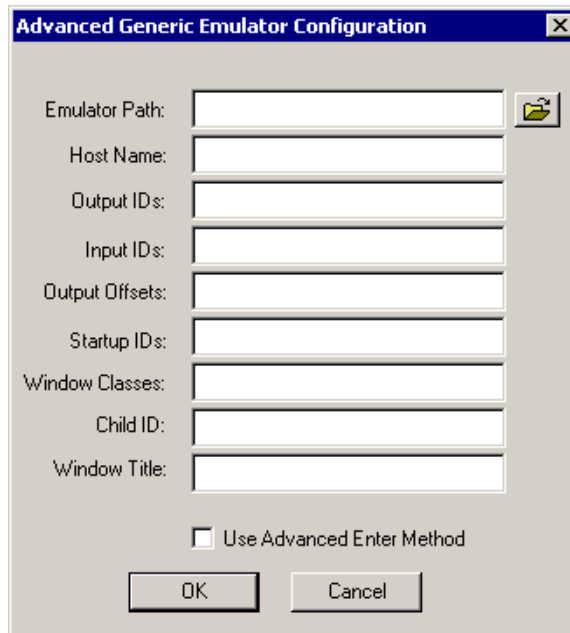
- 2** Click Edit Available Emulators > New.



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



- 4** Type values, then click OK.



The image shows a Windows-style dialog box titled "Advanced Generic Emulator Configuration". It contains several text input fields for configuration: "Emulator Path:" (with a browse button icon to its right), "Host Name:", "Output IDs:", "Input IDs:", "Output Offsets:", "Startup IDs:", "Window Classes:", "Child ID:", and "Window Title:". At the bottom, there is a checkbox labeled "Use Advanced Enter Method" and two buttons, "OK" and "Cancel".

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	<p>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.</p> <p>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.</p>
Output IDs	<p>The Control ID for the Copy function of the emulator.</p> <p>Some emulators allow a keyboard simulation alternative (for example, CTRL+C) instead. For information on finding Output IDs, see Appendix C, "Finding Control IDs and Offsets of an Emulator," on page 129.</p>
Input IDs	<p>The Control ID for the Paste function of the emulator.</p> <p>Some emulators allow a keyboard simulation alternative (for example, CTRL+C) instead. For information on finding Input IDs, see Appendix C, "Finding Control IDs and Offsets of an Emulator," on page 129.</p>

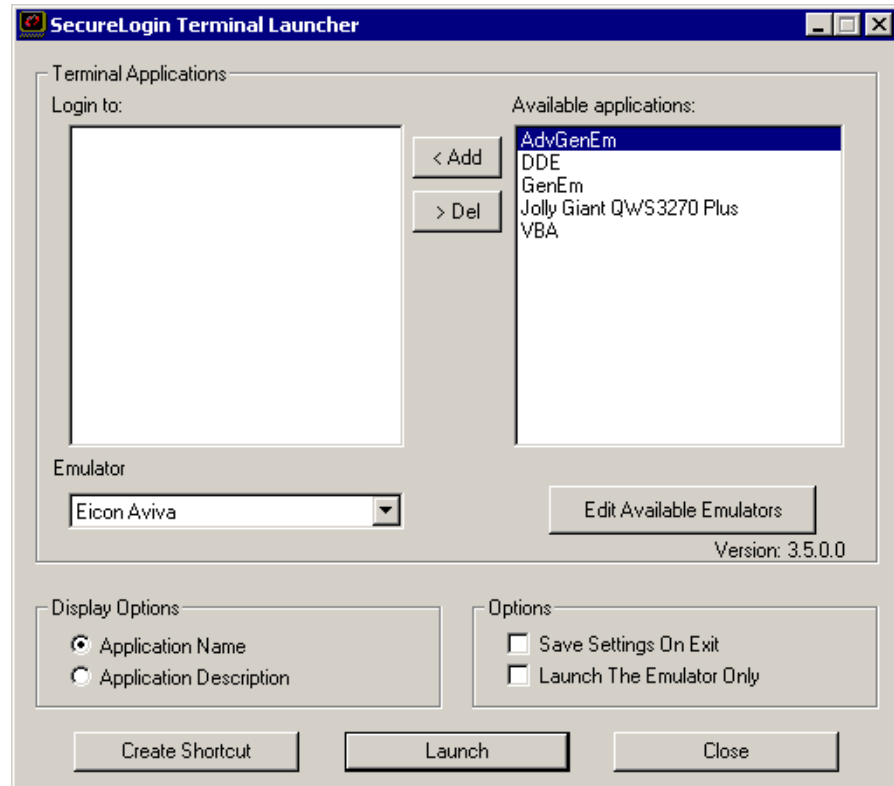
Field	Description
Output Offsets	<p>For Terminal Launcher to select the text on the screen without a Select All function, Terminal Launcher needs to use the mouse to copy from the screen. Select all the text by clicking and dragging the cursor over the entire emulator screen.</p> <p>For Terminal Launcher 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.</p> <p>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.</p> <p>To find the Output Offsets, you can use nsfinder.exe or trial and error.</p> <p>To use nsfinder.exe, download the utility from Novell's Support Web site (http://support.novell.com/servlet/filefinder?name=nsfinder.exe). A text file that explains how to use nsfinder is downloaded along with the utility. TID 2965468 provides the download. Also see "Finding Offsets" on page 137.</p> <p>To use the trial-and-error method, start with high numbers (for example: 10000,10000) and work your way down.</p> <p>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.</p> <p>Normally, the Output Offset number is around 500,7000 or lower.</p> <p>Trial and error becomes easier with experience.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Startup IDs	<p>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</p> <p>If several functions or buttons are needed, separate them with a comma.</p>

Field	Description
Windows Classes	<p>Assist Terminal Launcher in detecting the emulator window. If no Window Class is specified, Terminal Launcher might not detect the emulator opening.</p> <p>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.</p>
Child ID	<p>A Child ID is given to each child window that the main application launches.</p> <p>Only enter a Child ID into the TLaunch configuration if it is necessary to interact with a child window.</p>
Window Title	<p>Assists Terminal Launcher in detecting the emulator window. If no Window Title is specified, Terminal Launcher might not detect the emulator opening.</p> <p>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.</p> <p>Some emulators hide the real Window Title.</p> <p>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.</p>
Use Advanced Enter Method	<p>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.</p>

- 5** In the Available Emulators dialog box, click Done.

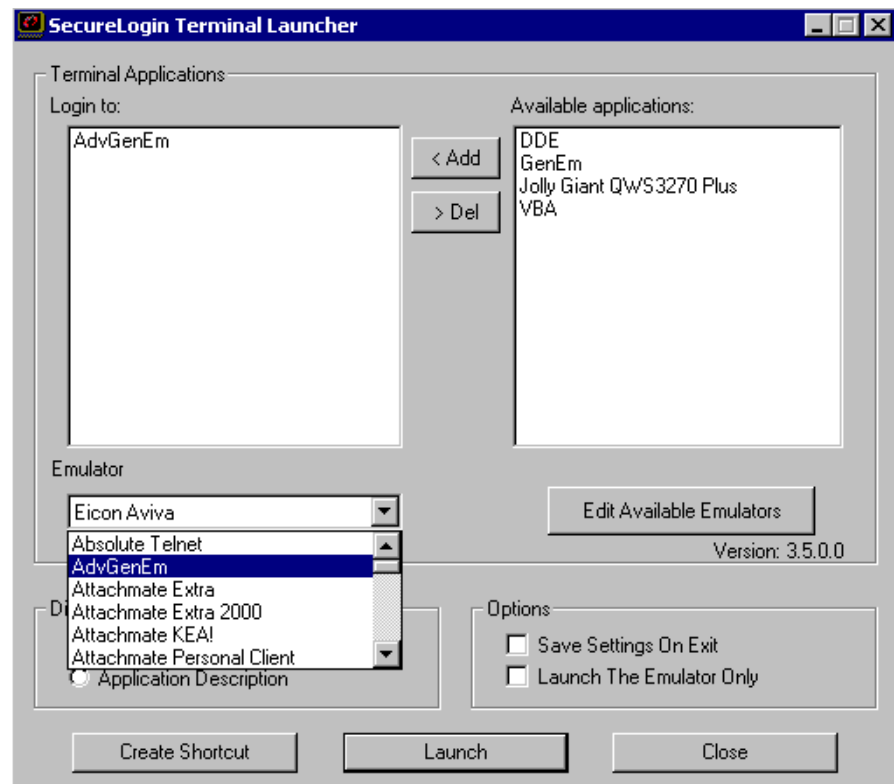
Creating a Login for an Emulator

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



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.



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

You can set up a shortcut for terminal launcher application scripts. 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 Right-click the desktop, then click New > Shortcut.

2 Enter (or browse to) the path for tlaunch.exe.

For example, enter "c:\Program Files\novell\securelogin\tlaunch.exe". Include quotation marks.

3 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 104](#).

The shortcut box contains this shortcut line:

```
"C:\Program Files\Novell\Securelogin\Tlaunch.exe" "/auto/pSimple Login/eJolly Giant"
```

4 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	Enables the command line facility of Terminal Launcher. This parameter must be in the command line for the other command line options to work.
/b	Specifies background authentication mode.
/leemulator_name	Launches the specified emulator. You must enter the emulator name exactly as it is listed in the Emulator drop-down list.
/lhllapi_short_name	Forces Terminal Launcher to connect to the specified HLLAPI session.
/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.

Parameter	Description
<i>/kexecutable_name</i>	Kills the specified executable before launching an emulator.
<i>/m</i>	Allows multiple (sequential) connections to particular sessions.
<i>/n</i>	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.
<i>/nnumber_1-15</i>	Launches the specified number of sessions without running scripts.
<i>/papplication_name</i>	<p>Runs the specified application. Type the application script name exactly as it is listed in the Terminal Launcher Available Applications list.</p> <p>To run several applications scripts from a shortcut at once, add <i>/panother application name</i> 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.</p>
<i>/q</i>	Specifies Quiet Mode (no cancel dialog).
<i>/s</i>	Suppresses errors.
<i>/t</i>	Enables unlimited timeout when connecting to an emulator.
<i>/wprocess name</i>	Waits until the specified process name is running before running the script.
<i>/xparameters</i>	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.

When an emulator or application is not specified on the command line, Terminal Launcher uses the settings stored in the `tlaunch.ini` file. You can modify these settings.

- 1** Check the Save Settings on Exit check box.
- 2** Click Close.

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.

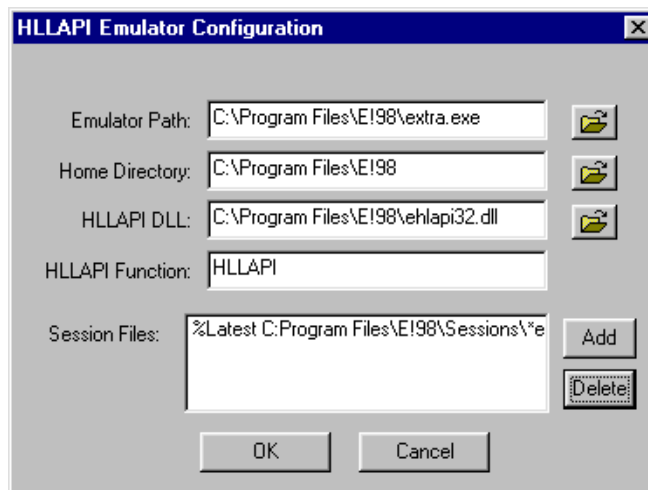
NOTE: After the emulator is launched, these session files are executed as a command line parameter. Some emulators (such as QWS3270 Plus) do not have session files. Instead, these emulators have individual sessions stored in the registry. Think of these session files as command line parameters that are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



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 \(http://support.novell.com\)](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.

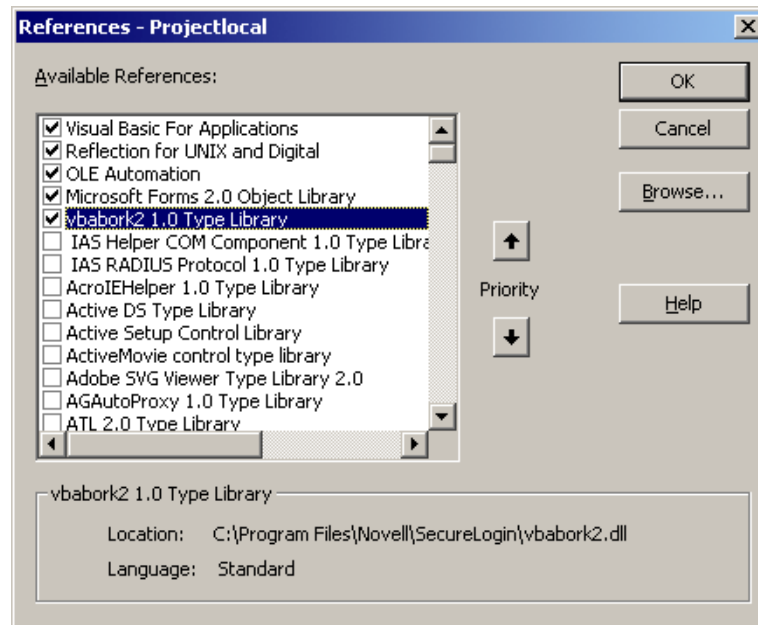
By doing this procedure, the SecureLogin script macro will run every time the session is opened. Without this procedure, you will need to manually run the script macro when you want to run the script.

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

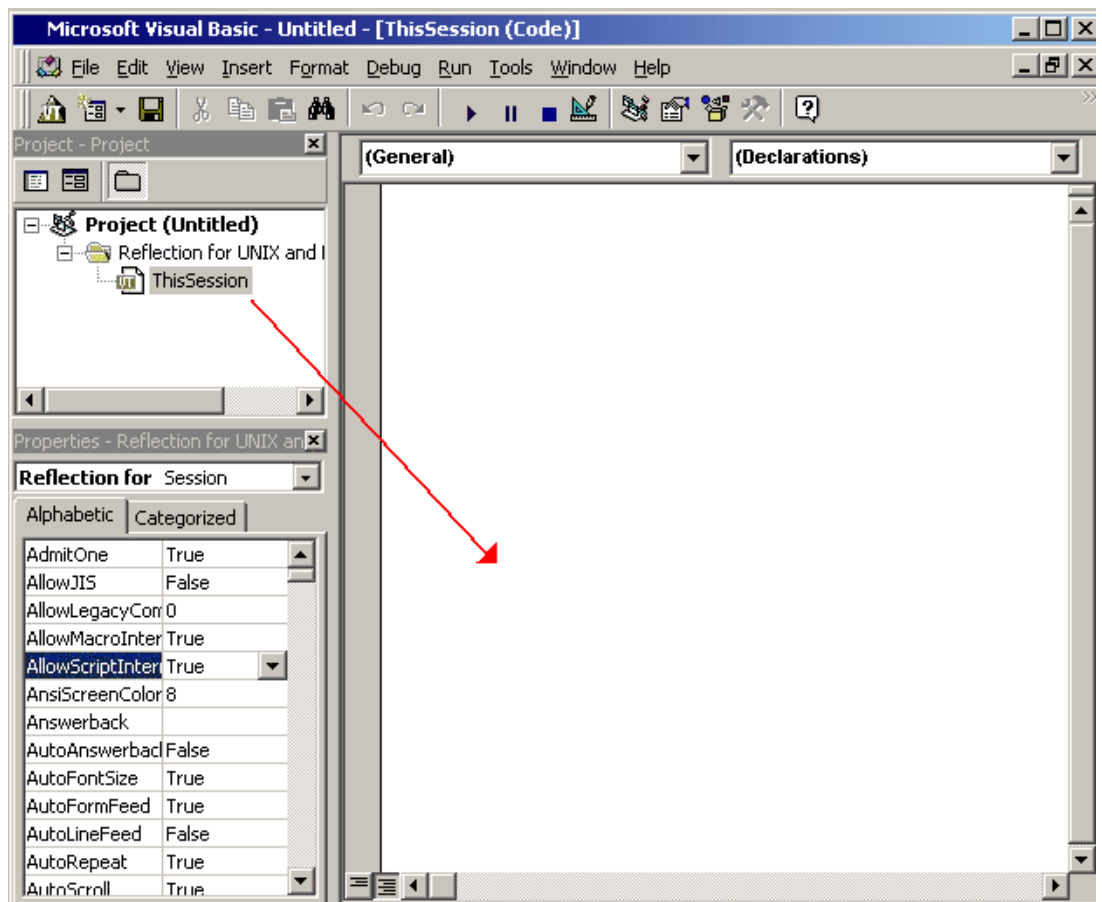
- 1** Launch Terminal Launcher, then click Edit Available Emulators. Set up the emulators as usual, but set the HLLAPI type to None.
- 2** Select the emulator.
- 3** Type anything in the hllapi dll and HLLAPI Function boxes.
- 4** Click OK, then click Done.

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 vbabork2 1.0 Type Library, then check the check box.



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



- 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.

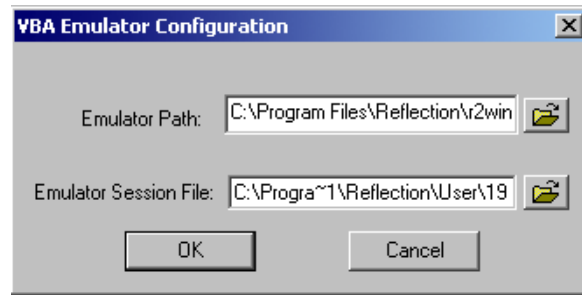
This is where you set up the host name and protocol that you are connecting to the mainframe.

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.



12 Create a script for the emulator to use.

6

Troubleshooting SecureLogin

This section contains information on the following:

- ♦ “Interoperability Issues” on page 113
- ♦ “Clearing Object Data” on page 115
- ♦ “Frequently Asked Questions” on page 118
- ♦ “Useful TIDs” on page 123

For information on error codes, see [Appendix E, “Error Codes,” on page 145](#).

Interoperability Issues

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 [“Adding a Java Application” on page 76](#).

- 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.

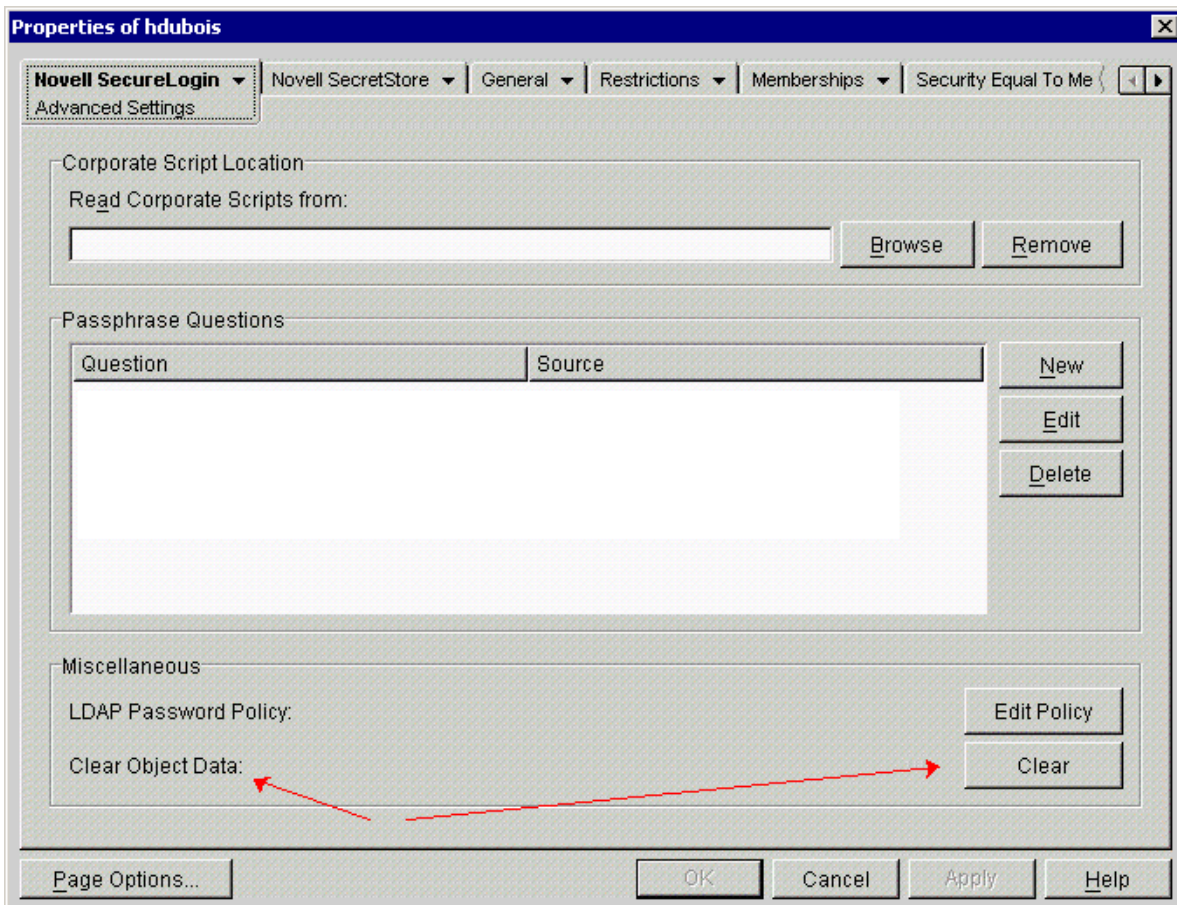
Clearing Object Data

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 cache files.

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

- 1** Right-click an object, then click Novell SecureLogin > Advanced Settings.
- 2** At the Clear Object Data label, click Clear.

The following figure illustrates this option:



Clearing object data does not clear all of the object's data. It only clears the object data stored in the directory. The data stored in the SecureLogin cache files on the workstation remain. Therefore, if you reboot the workstation or resync between the workstation and the directory, the data store in the directory will be repopulated with the information.

To clear all object data from a specific user, clear object data within the directory and then also delete the cache files located on the workstation.

The directory will be repopulated with the old information in the cache files only if the user sets up a passphrase that matches the old passphrase.

Disabling the offline cache does not disable SecureLogin's cache files. It just disables the use of the cache files for offline access. To completely remove or clear object data, delete the cache files on the workstation.

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 ProtAuthMethods, 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 [“Troubleshooting SecureLogin”](#) in the [Nsure SecureLogin 3.51 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.nsrld.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 ProtAuthMethods, 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.nsrld.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 [“Changing the Startup Order of Applications” on page 60](#).

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.

System Tray Icon Stays Active

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

Answer: This setting is only read at startup. After you restart your workstation, the system tray 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 \(http://download.novell.com/pages/PublicSearch.jsp\)](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.

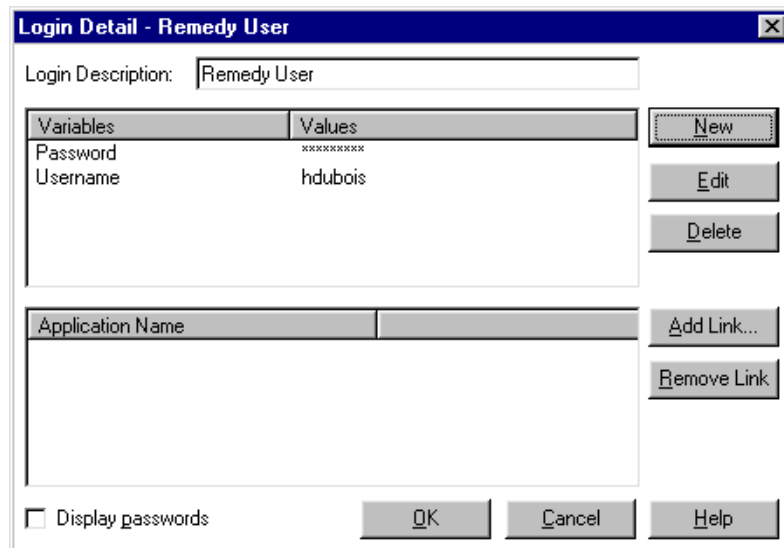
Use Dependency Walker to find the HLLAPI function export name, then enter it exactly.

Can't View Shadow Variables

What can't I view shadow variables?

Answer: You are probably running SecureLogin in a mixed SecureLogin 3.51 and SecureLogin 3.0.x environment. When you run SecureLogin in a mixed environment, you lose some SecureLogin 3.51 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.



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 \(http://developer.novell.com/ndk/doc/ldapover/index.html?page=/ndk/doc/ldapover/ldap_enu/data/a3wyu4m.html\)](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 slina.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, use \$Username and \$Password.

If you encounter this issue with a Citrix* or Terminal Server installation, verify that you registered the slina.dll while you were in install mode. Otherwise, the new slina.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 \(http://support.novell.com/search/kb_index.jsp\)](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 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

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)

A

Prebuilt Scripts

SecureLogin provides prebuilt login scripts for the following applications:

Application	Application	Application
ActiveSync*	iPlanet*	QuickBooks* Pro
America Online*	Lotus Notes (Win script)	Remedy* AR User
BorderManager®	MSN Messenger	SAP* R/3
Citrix Management Console	myNovell	SecureRemote
Entrust*	myRealBox SM	Tivoli* Helpdesk
Google*	MYOB Client	Trillian
GroupWise® Client	Nomad	Visual SourceSafe*
GroupWise Notify	Oracle* Financials	VNC
Hotmail*	OutLook*	Win95 /98 DialUp
I.E Proxy Authentication	pcANYWHERE	Yahoo* Messenger
iFolder® (JavaSSO)	PeopleSoft*	
iFolder (Win)	Qualcomm* Eudora*	

B

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 Terminal Services”](#) in the [Nsure SecureLogin 3.51 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 Citrix/Terminal Server module for whenever single sign-on through the Initial Citrix/Terminal Server GINA is required. This module automates the initial login to the Citrix/Terminal Server GINA by providing the user's details from the local machine. This process requires the installation of a login extension on both the client and the Terminal and MetaFrame servers. See the [Nsure SecureLogin 3.51 Terminal Services Guide](#).

C

Finding Control IDs and Offsets of an Emulator

This section provides information on the following:

- ♦ “Finding Input and Output IDs” on page 129
- ♦ “Finding Offsets” on page 137

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 \(http://www.gipsysoft.com/articles/winspector/\)](http://www.gipsysoft.com/articles/winspector/), or Spy++, available from Microsoft’s developer Web site.

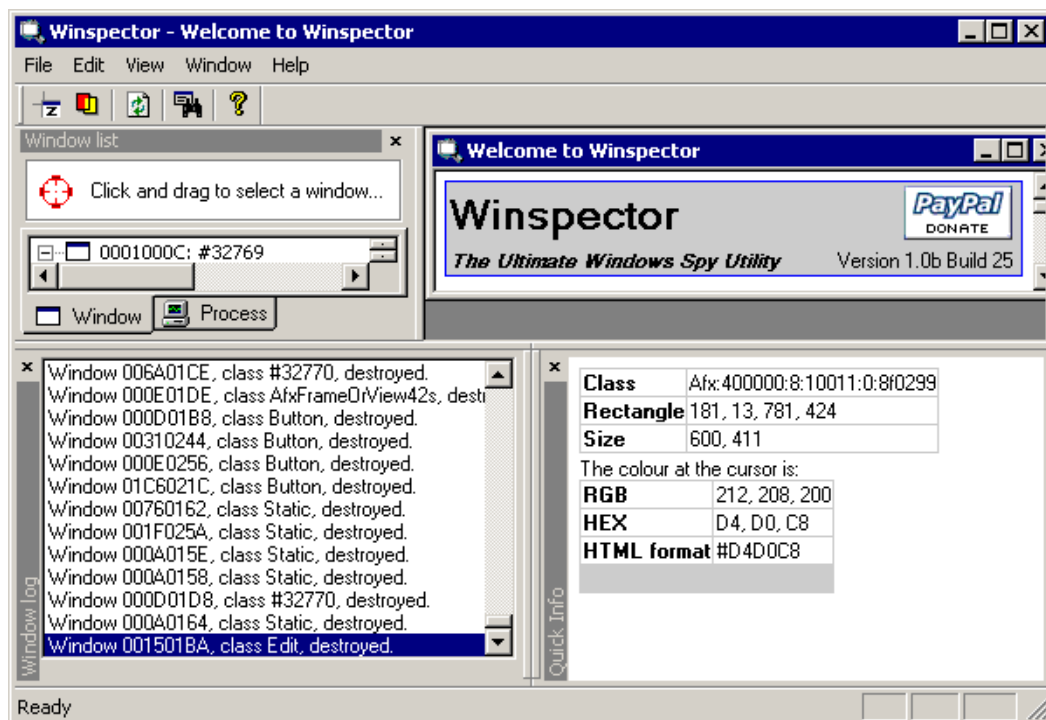
This section explains how to use Winspector.

Setting Up Winspector

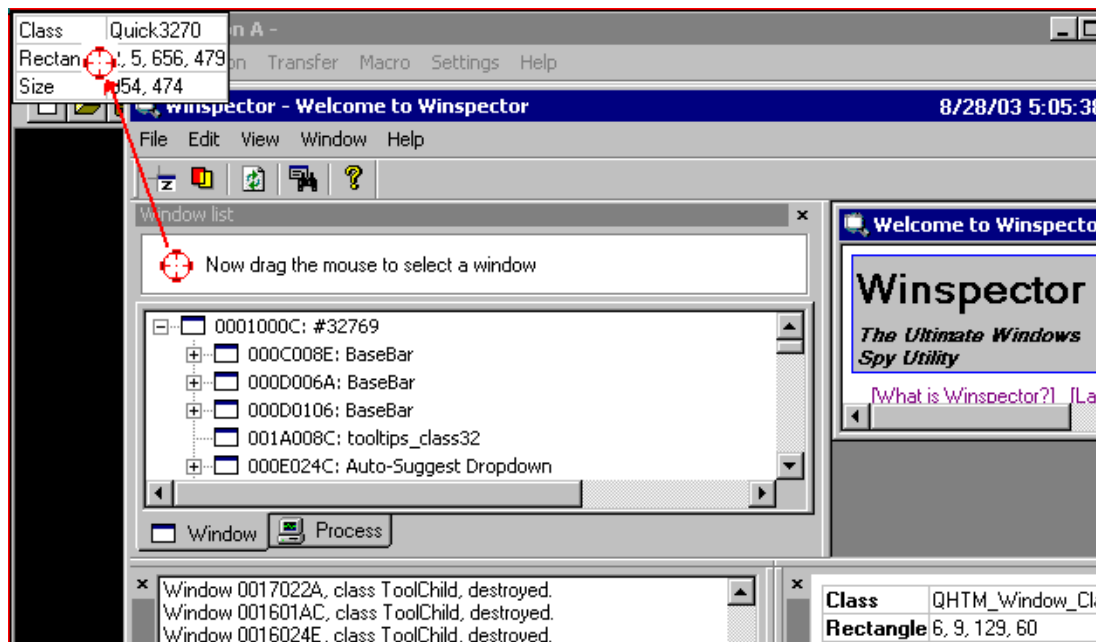
- 1** Run the emulator. Don’t close it.

In this example, the emulator is Quick32.

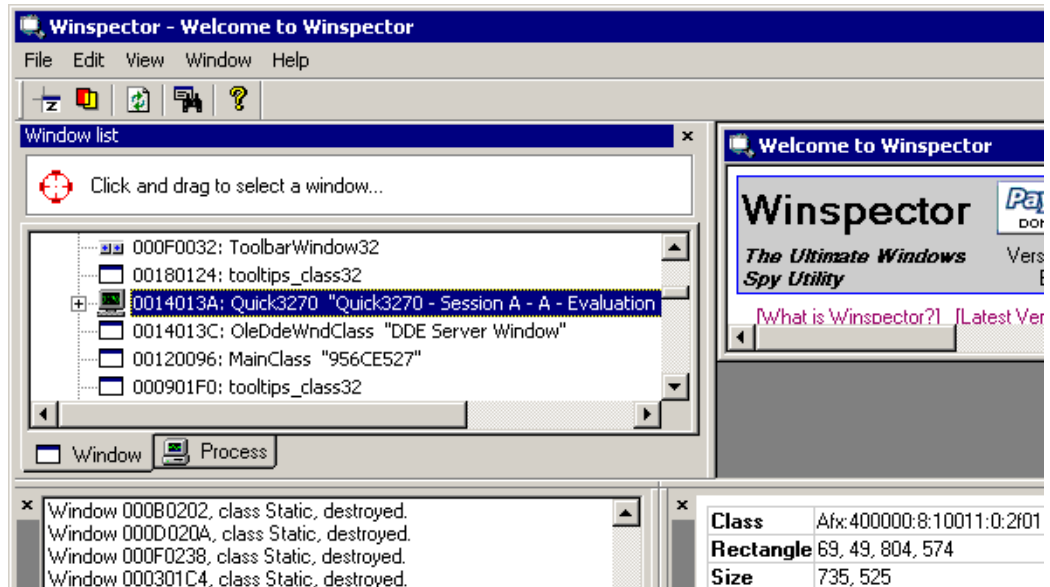
- 2** Run Winspector.



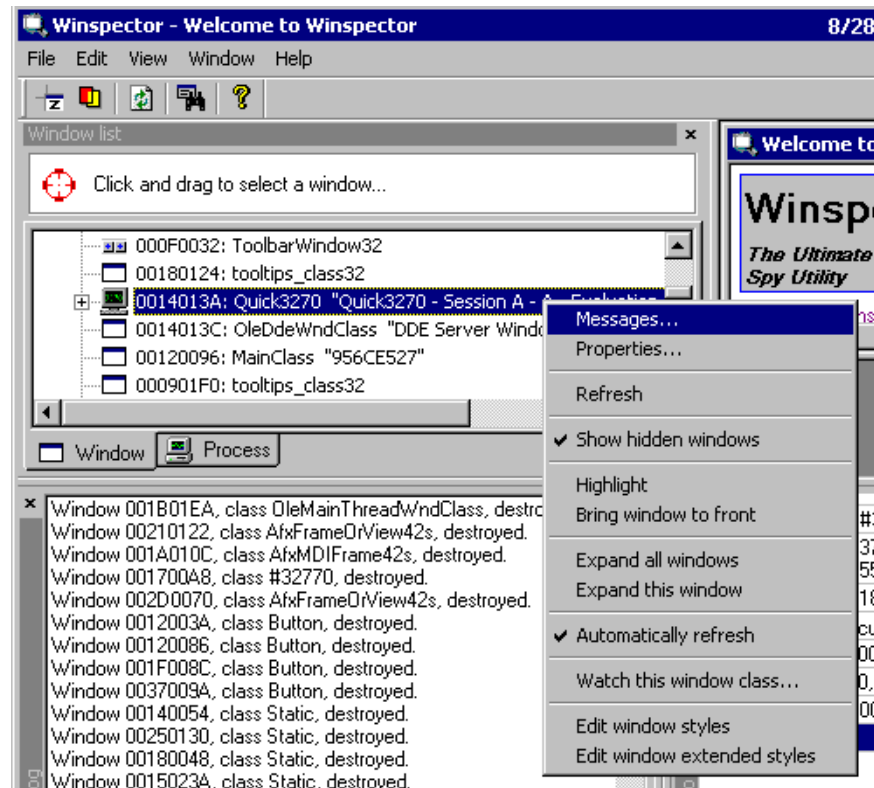
- 3 Arrange the windows so that emulator window and Winspector window are both visible on the screen.
- 4 Click and drag the Winspector icon to the title bar of the emulator, then release the mouse.



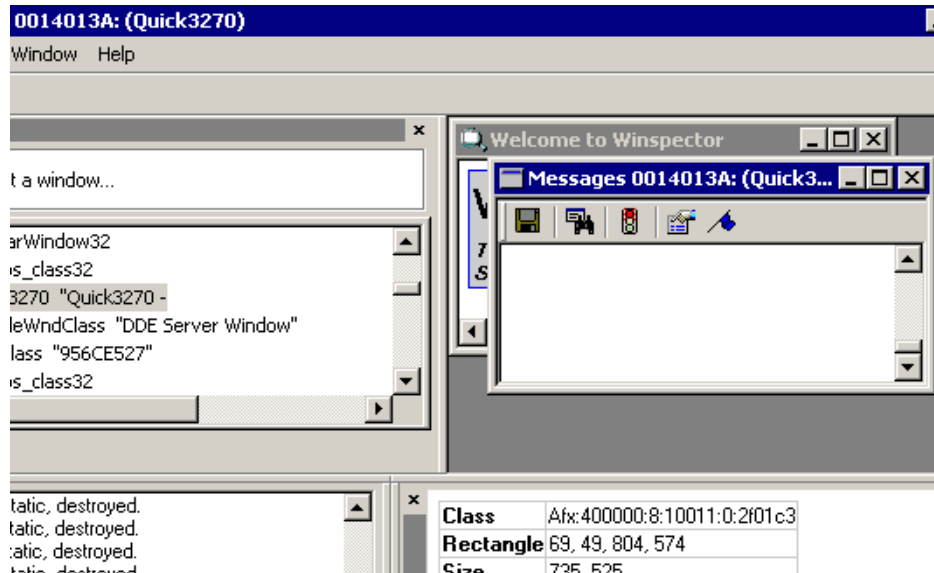
- 5 Verify that the title displayed on the emulator's title bar is listed among applications in Winspector's Click and Drag To Select a Window pane.



- 6 Right-click the emulator name, then click Messages.

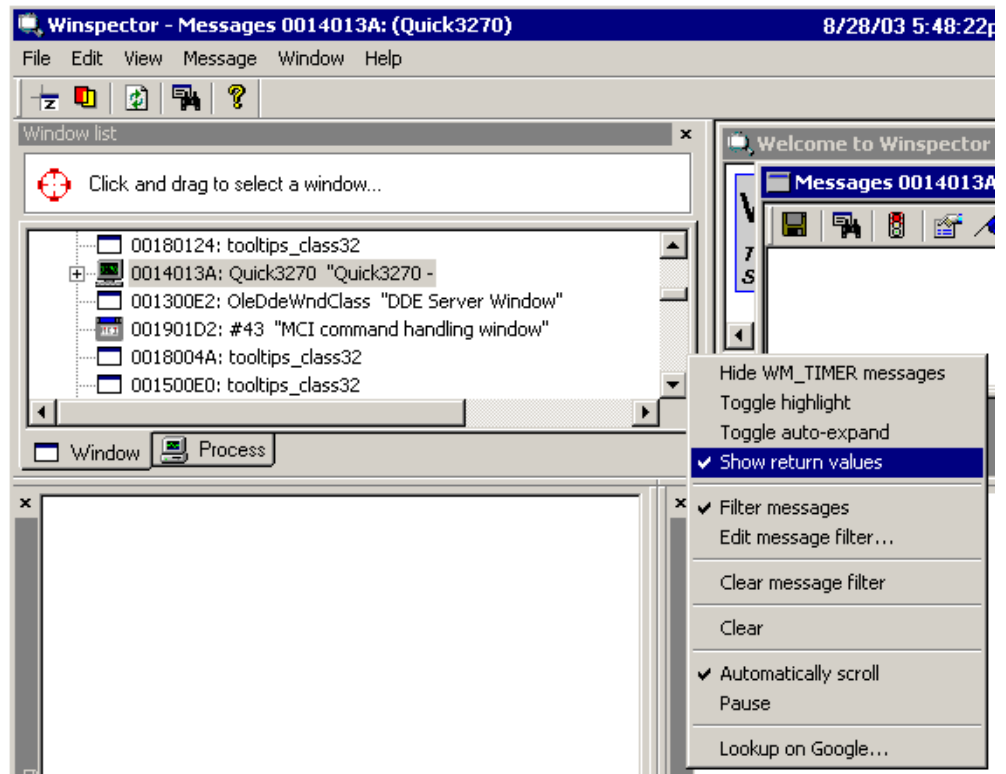


With the Messages window open, Winspector is ready to capture and log messages.

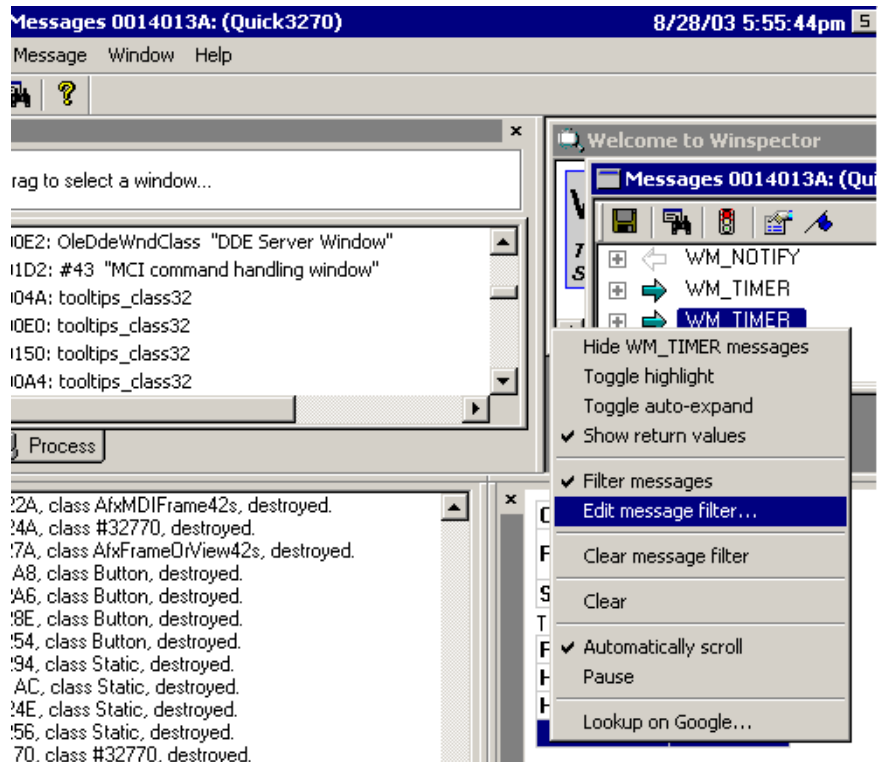


7 Limit what Winspector captures and logs.

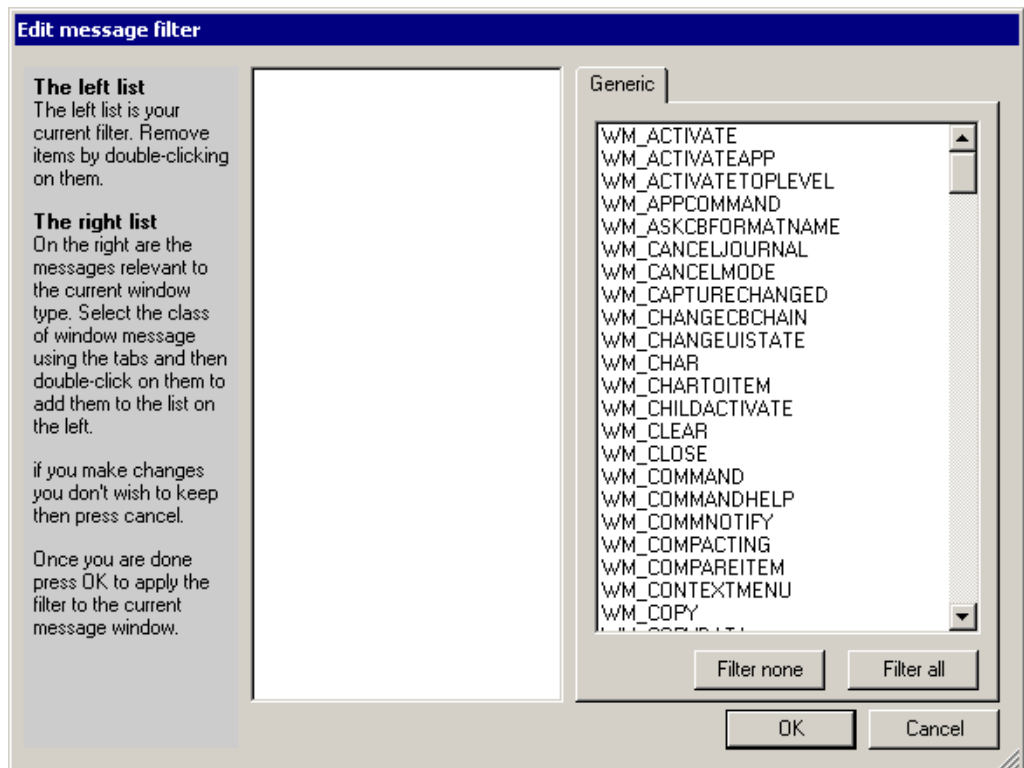
7a Right-click in the Messages window, then uncheck Show Return Values.



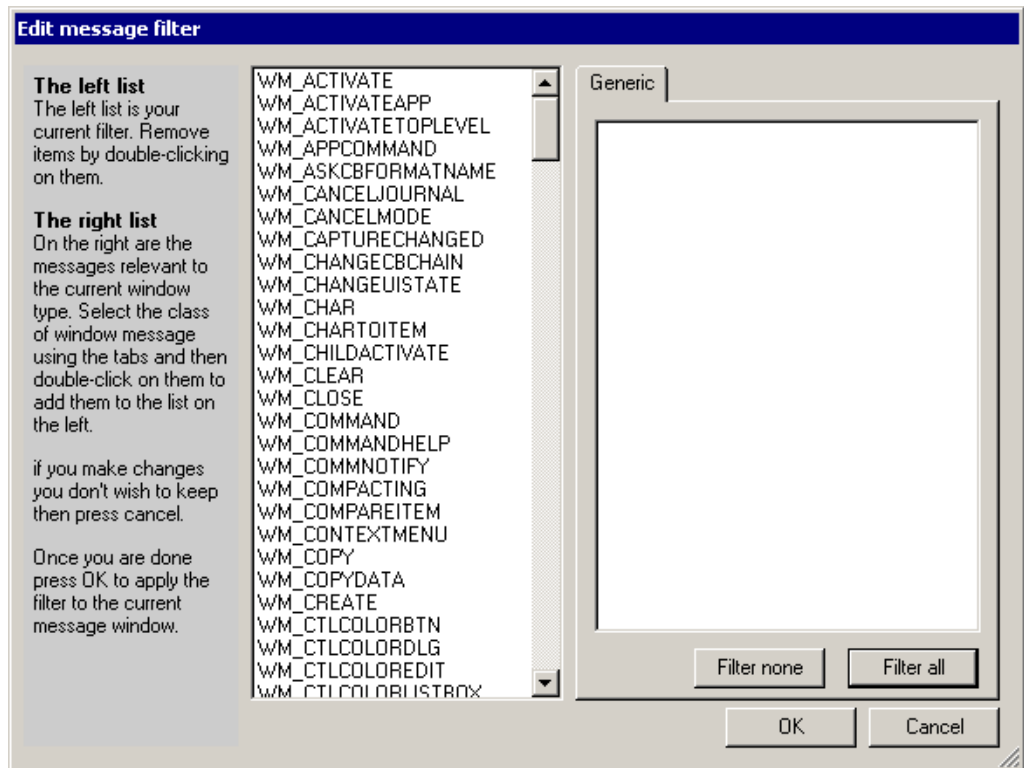
7b Right-click in the Messages window, then click Edit Message Filter.



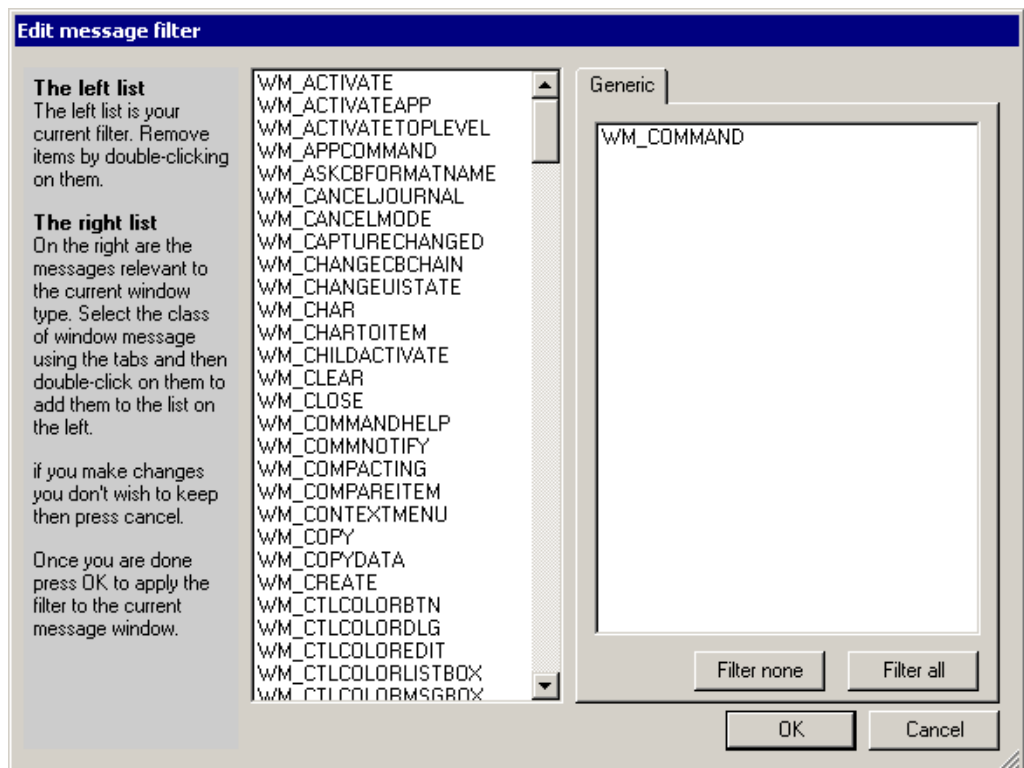
7c From the Edit Message Filter Window, click Filter All.



When all messages are filtered, Winspector rejects all messages. The Messages window won't be cluttered with unwanted messages.

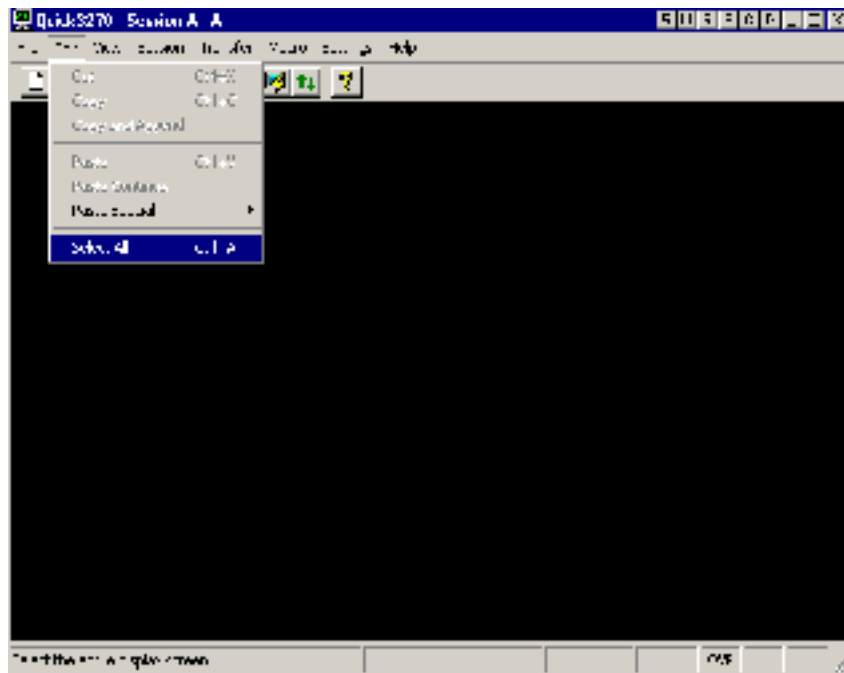


7d Scroll to and double-click WM_COMMAND, then click OK.

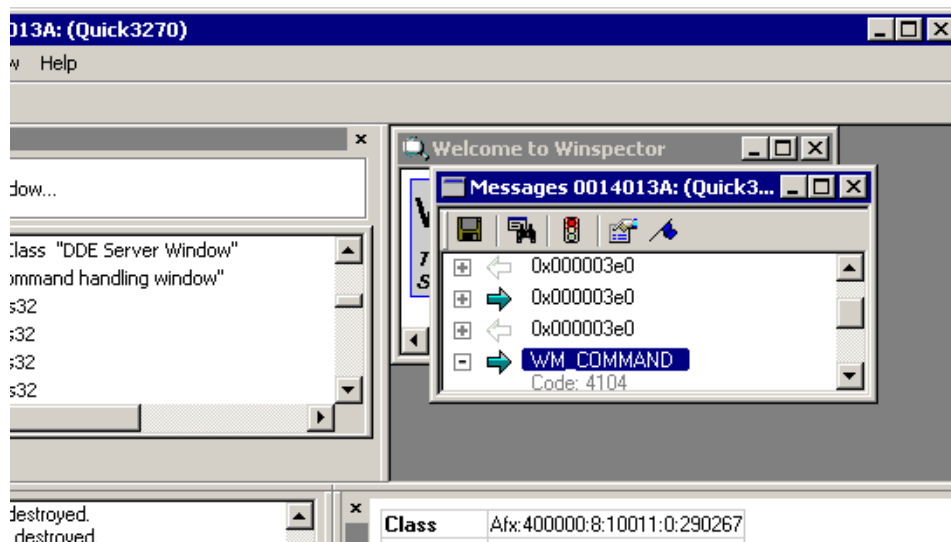


Viewing Control ID Numbers

- 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.



- 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.

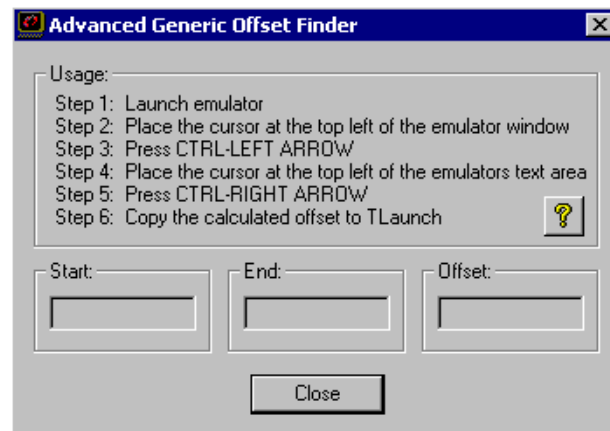
Finding Offsets

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...).

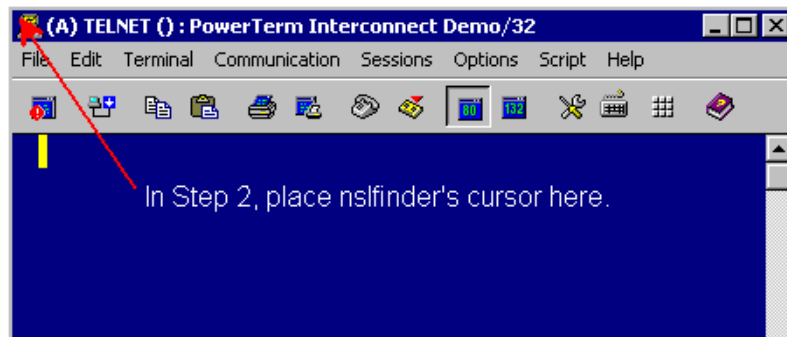
You can easily find offsets required for Advanced Generic emulators by using `nslfinder.exe`. Download this utility from [Novell's Support Web site \(http://support.novell.com/servlet/filefinder?name=nslfinder.exe\)](http://support.novell.com/servlet/filefinder?name=nslfinder.exe).

To find offsets:

- 1 Open the emulator, then open `nslfinder.exe`.



- 2 Place `nslfinder`'s cursor in the top left corner of the emulator's window.

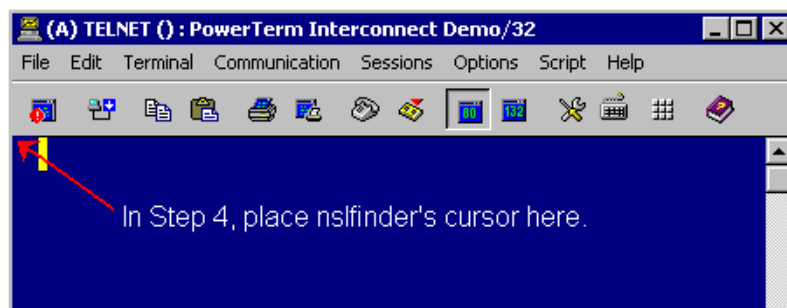


- 3** Type Ctrl+Left-arrow.

Nsfinder pastes the value into the Start text box.

Start: 3583,5973	End: 	Offset:
Close		

- 4** Place nsfinder's cursor in the upper left corner of the emulator's text pane.

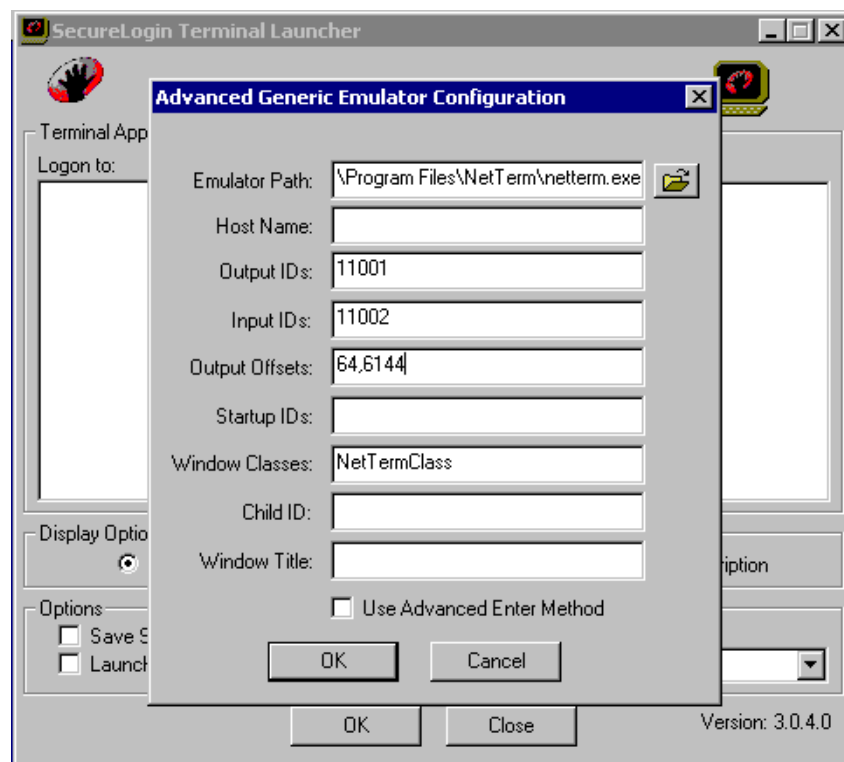


- 5** Type Ctrl+Right-arrow.

Nsfinder 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
Close		

- 6** Copy the offset values into Terminal Launcher's Output Offsets text box.



D

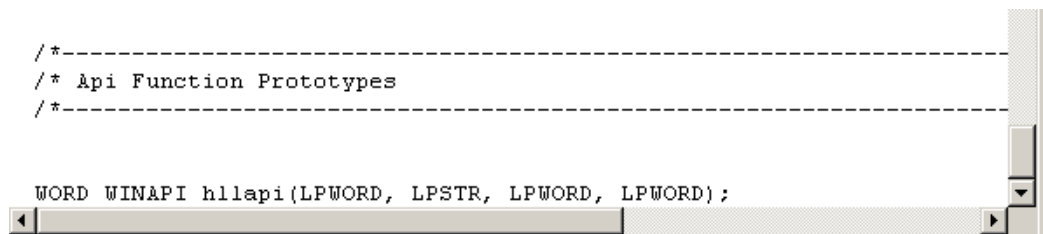
Finding HLLAPI Types

This section provides information on the following:

- ♦ “Using Header Files” on page 141
- ♦ “Using Dependency Walker” on page 141

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:



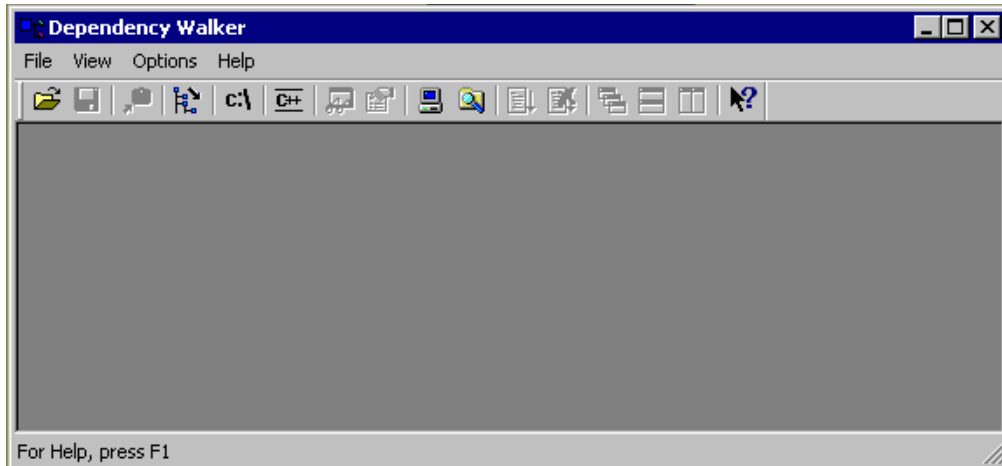
Using Dependency Walker

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.

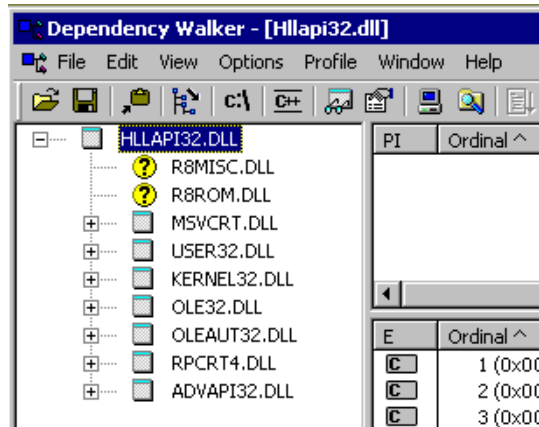
Dependency Walker is available from the [Dependency Walker Web site \(http://www.dependencywalker.com\)](http://www.dependencywalker.com).

- 1 Run depends.exe.



- 2** Click File > Open, then navigate to and open the hllapi.dll file.

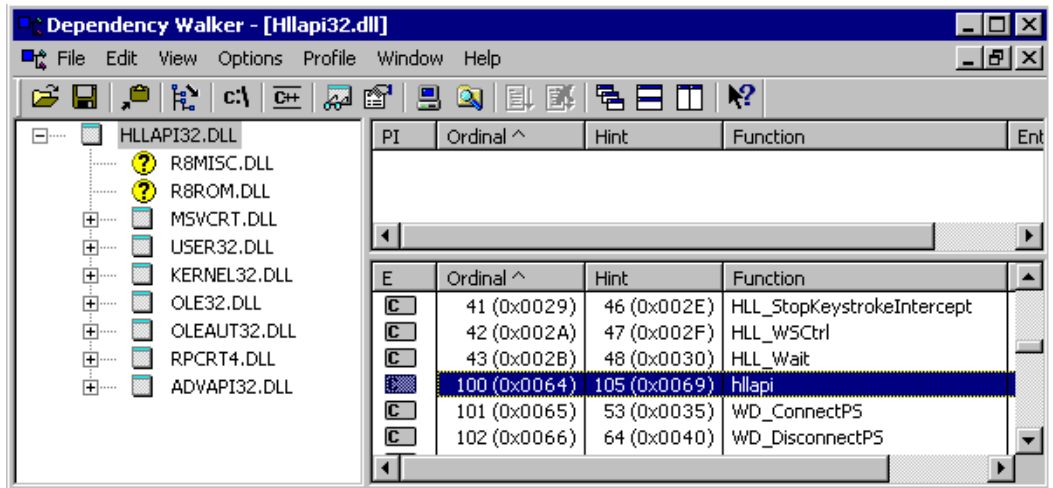
Look for a .dll file with the name "HLLAPI" (or some variation) in it. For example, the file for Quick3270 is QHLLAPI.DLL, found in the c:\Program Files\Quick3270 directory.



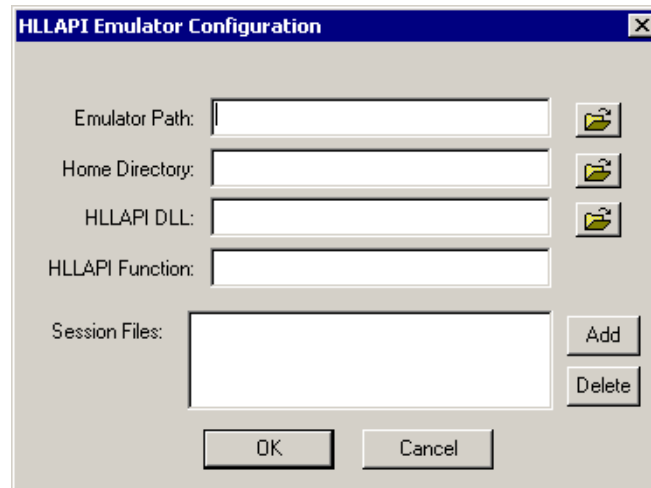
- 3** In the function exports window, scroll through the exports until you locate "hllapi".

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.



- 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.

E

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 145.

For a list of error codes that require help from Novell® Technical Services, see “[Getting Help from Novell Technical Services](#)” on page 163.

For information on error codes for LDAP, see [LDAP and NDS Integration \(http://developer.novell.com/ndk/doc_jldapunx.htm\)](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 in 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 in 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: Delete the local cache file 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 NMASTM 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: Delete the local cache file 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: Delete the local cache file and try again.

Action: Call Novell Technical Services.

-140 BROKER_SCRIPT_DATA_CORRUPT

Possible Cause: SecureLogin is unable to use data in scripts.

Action: Delete the local cache file 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: Delete the cache file.

-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 the Combroker 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: You used an incorrect function when you defined the emulator. 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: Using the [Nsure SecureLogin 3.51 Configuration Guide for Terminal Emulation](#), check the configuration for the emulator. Make sure that you typed the HLLAPI function correctly.

-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: Using the [Nsure SecureLogin 3.51 Configuration Guide for Terminal Emulation](#), check the configuration for the emulator. Specify the correct emulator type.

-226 BROKER_ERROR_DURING_WINHLLAPISTARTUP

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 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

Action: Refer to the vendor's documentation.

-266 BROKER_NT_FILE_STORAGE_SAVE_FAILED

Possible Cause: Using NT 4 Domains mode, the user was unable to save to the equivalent of a cache file in the Home directory.

Action: Grant the user 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.

-320 BROKER_GOTO_LIST_ASSERTION

Possible Cause: The software is not working as intended.

Action: Call Novell Technical Services.

-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 system tray. 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.

-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 couldn't find the function name and was therefore unable to connect to the emulator. The function name is probably wrong.

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: You haven't configured your emulator for an HLLAPI session. 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: Terminal Launcher was able to initialize the emulator but was unable to read the contents of the screen. 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, 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, 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 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 “[SecureLogin on LDAP](#)” in the [Nsure SecureLogin 3.51 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 do not 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. Slina.dll or slnmas.dll must be correctly installed for these variables to function.
- Action: Make sure that either slina.dll 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 Scripting Guide](#).

Getting Help from Novell Technical Services

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_UNINITIALIZED
- ◆ -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

F

Documentation Updates

This section contains new or updated information on installing and managing Novell® SecureLogin. The information is new since SecureLogin 3.5.

This documentation is also provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

If you need to know whether a copy of the PDF documentation you are using is the most recent, check the date that the PDF file was published. The date is in the Legal Notices section, which immediately follows the title page.

New or updated documentation was published on the following dates:

- ♦ “December 11, 2003” on page 167
- ♦ “February 10, 2004” on page 167

December 11, 2003

Location	Change
“Configuring an Advanced Generic Emulator” on page 98	Changed nsfinder.exe to nsfindera.exe.
“Finding Offsets” on page 137	

February 10, 2004

Location	Change
“Configuring WinHLLAPI, HLLAPI, or 16-Bit HLLAPI Emulators” on page 89	Revised the Tip note to include information about short session names.

April 22, 2004

Location	Change
Chapter 2, "Managing SecureLogin," on page 19	Corrected several doc defects in procedures throughout the chapter.
"Using SecureLogin with Client Software" on page 52	Corrected inaccurate steps to re-enable the Login dialog's password field.