Novell SecureLogin

6.0

www.novell.com

OVERVIEW

March 24, 2006

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.

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

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

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

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

Novell Trademarks

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

Third-Party Materials

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

About This Guide

This document contains the following information

Feedback

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

Documentation Updates

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

Additional Documentation

Novell SecureLogin 6.0 Overview is a part of documentation set for SecureLogin 6.0. Other documents include:

- *Novell SecureLogin 6.0 Administration Guide*
- *Novell SecureLogin 6.0 Installation Guide*
- *Novell SecureLogin 6.0 User Guide*
- *Novell SecureLogin 6.0 Application Definition Guide*
- *Novell SecureLogin 6.0 Citrix and Terminal Services Guide*
- *Novell SecureLogin 6.0 Congifuration Guide for Terminal Emulation*

Documentation Conventions

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

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

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

Contents

About SecureLogin

1

Novell® SecureLogin has the following features:

- Eliminates the requirement for users to remember multiple user names and passwords beyond their initial network logon. It stores user names and passwords and automatically enters them for users when required. Users no longer need to remember and manually enter credentials, such as user names and passwords, to log on to applications.
- Quickly retrieves and enters credentials, which results in faster login.
- Helps to reduce calls to the Help Desk about locked accounts and forgotten user name and password combinations.
- Is comprised of multiple, integrated security systems that provide authentication and SSO to networks and applications. Provides a single entry point to the corporate network and its user resources, increasing security while enhancing compliance with corporate security policies. SecureLogin utilities and components are designed to SSO-enable Windows*, Java, Web and terminal emulator applications.
- Stores and encrypts user credentials in the directory (eDirectory®, Active Directory*, or other LDAP compliant directories) and optionally caches them in an encrypted format on the local workstation. Only the user can access the encrypted data. Even a network administrator with full rights is unable to view a user's passwords. A network administrator can set a new password if required, for example disaster recovery, but cannot view existing passwords.
- Has wizards, directory console plug-ins, and tools which make it easy to centrally configure for use on the corporate network.
- Includes a management utility that allows users to view their SSO details and, if permitted, to SSO-enable applications.
- Employs two methods of fault tolerance:
  - Using local encrypted caching to ensure that network downtime does not affect SSO performance. Even if the corporate network is down, caching enables application logons to continue uninterrupted.
  - Using application definitions to cater to different logon conditions and errors during logon.
- Maintains SSO integrity for all mobile and remote users, regardless of network connectivity by locally encrypting the cache. If you permit them to, mobile users can update their SSO credentials when disconnected from the network and later update the directory with these details when they are next attached. Because SecureLogin is a directory-enabled product, users can:
  - Log on from anywhere and get the same capabilities as if they were at their own desks.
  - Log on and log off quickly, because they authenticate only to the directory, not to Windows itself.
  - Roam the enterprise, logging on to several different machines during the day.
  - Work on a notebook or laptop in a disconnected mode, because their logon credentials are saved to a local, encrypted cache.
  - Securely use a shared, kiosk-type workstation, where many people log on temporarily for quick work and then log off.

SecureLogin Components

2

This section contains the following information:

2.1 About the SecureLogin Management Utilities

Table 2-1 *SecureLogin Management Utilities*

Use the	To manage users:
Personal Management Utility	In the stand-alone mode. You can configure the local workstation for the logged-on user. It has the same functionality as the Administrative Management Utility, excluding some preference options, advanced settings and secure settings distribution. You can disable users from accessing this utility in a directory environment. For more information, see Section 3.1, “Personal Management Utility User Interface,” on page 15.
Administrative Management Utility	Centrally in a directory environment at the user object, Group Policy, container or OU (organizational unit) level. For more information, see Section 3.2, “Administrative Management Utility User Interface,” on page 16.
iManager Plug-in	In a corporate environment you can allow or prohibit full or part access to this utility depending on organizational requirements. For more information, see “Installing Administrative Tools for eDirectory” in the Novell SecureLogin 6.0 Installation Guide.

2.2 Add Application Wizard

Figure 2-1 *Add Application Wizard*

The Add Application Wizard helps you create and change application definition responses for the following:

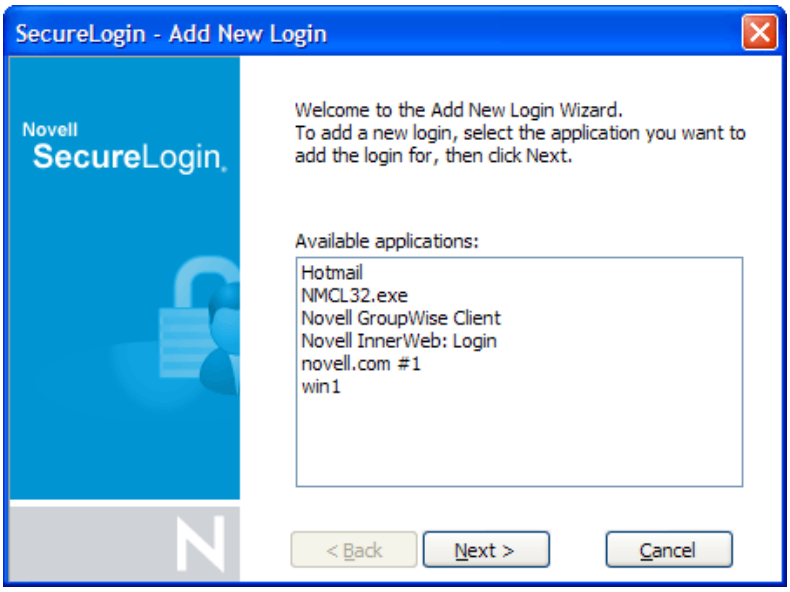
- Login dialog box
- Change Password dialog box
- Change Successful message
- Login Successful message
- Login Failure message

NOTE: The Add Application Wizard launches automatically in response to Windows Login and Password dialog boxes if there is no existing application definition. If there is already an application definition, the Add Application Wizard does not automatically start in response to Login and Password dialog boxes. For previously created application definitions, you can invoke the Add Application Wizard manually, and once the Change Password dialog box is displayed, you can capture the password data.

For more information, see Chapter 4, “Enabling Applications and Web Sites for SSO,” on page 41.

2.3 Add New Login Wizard

Figure 2-2 *Add New Login wizard*



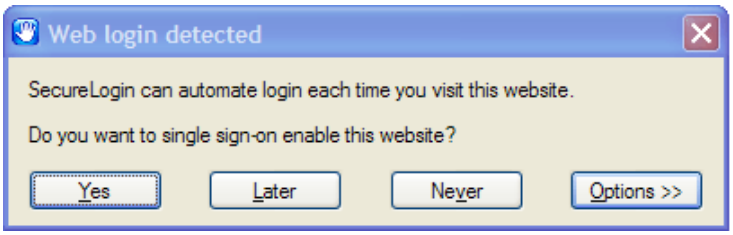
The Add New Login Wizard helps you create multiple logons for the same application or server. The Wizard contains a list of available applications from which you can choose the required logon. For more information, see Chapter 4, “Enabling Applications and Web Sites for SSO,” on page 41.

IMPORTANT: You can use the `PickListAdd` and `PickListDisplay` commands to add logon options for multiple users. For example, if all users in the IT group require three different logons for the help desk application, you could add a `PickList` to the help desk application definition and all users will inherit the list without having to individually add new logons.

2.4 Web Wizard

Use the Web Wizard to SSO-enable Web sites and capture virtually any Web-based logon. You simply access a Web page from your browser and SecureLogin starts the Web Wizard. It captures logon information, error messages, and change password requests. For more information, see Chapter 4, “Enabling Applications and Web Sites for SSO,” on page 41.

Figure 2-3 *Web Wizard*



2.5 Terminal Launcher

Figure 2-4 *Terminal Launcher*

Terminal applications require Terminal Launcher to execute for SSO. After you create the application definition in the Management Utility, you must configure it to start the Terminal Launcher. A shortcut is created to enable the user to run Terminal Launcher and the terminal emulator from the desktop with automated SSO to the application or server. For more information, see Chapter 4, “Enabling Applications and Web Sites for SSO,” on page 41.

SecureLogin Interface

3

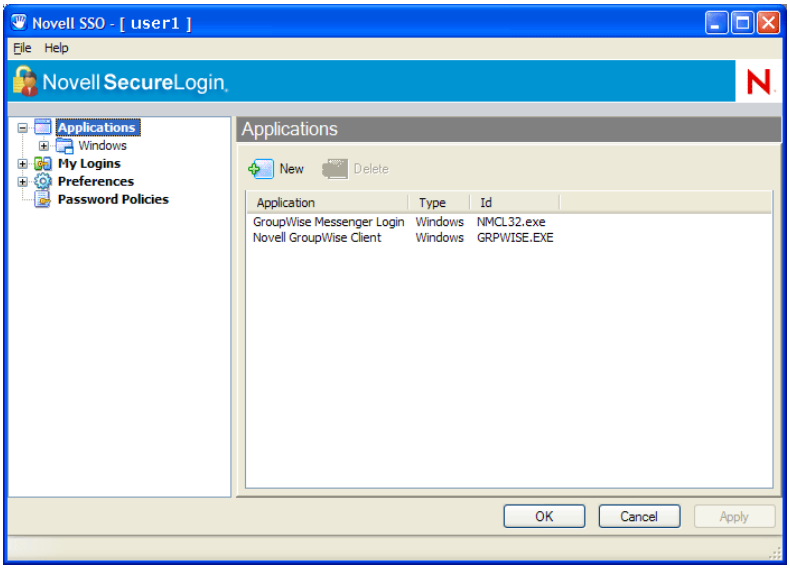
This section contains the following information:

3.1 Personal Management Utility User Interface

The Personal Management Utility user interface consists of a title bar, menu bar, panes, and properties tables.

When you select a folder in the navigation tree, the related information is displayed in the right pane. To display the objects associated with the folders in the navigation tree, click the plus sign next to the icon to expand its contents. But not all icons are expandable.

Figure 3-1 *Personal Management Utility*



The navigation tree contains the following:

- Applications
- My Logins
- Preferences
- Password Policies

Changes made using the Personal Management Utility on the local workstation apply only to the logged on user's SSO, and they override settings made in the directory. For example, if the SecureLogin preference *Allow users to view and modify Application Definitions* is set to *No* at the OU the user object resides in, but *Yes* on the actual user object in the directory, the user object setting applies. The user can view and modify Application Definitions. Other users in the container cannot view and modify application definitions unless they have the option set through the user object.

The Personal Management Utility is used for:

- Providing users with the capability to configure their SecureLogin environment and view their own credentials.
- Testing SecureLogin configuration prior to mass deployment.
- Creating and modifying application definitions for testing.
- Stand-alone installations.
- Troubleshooting.

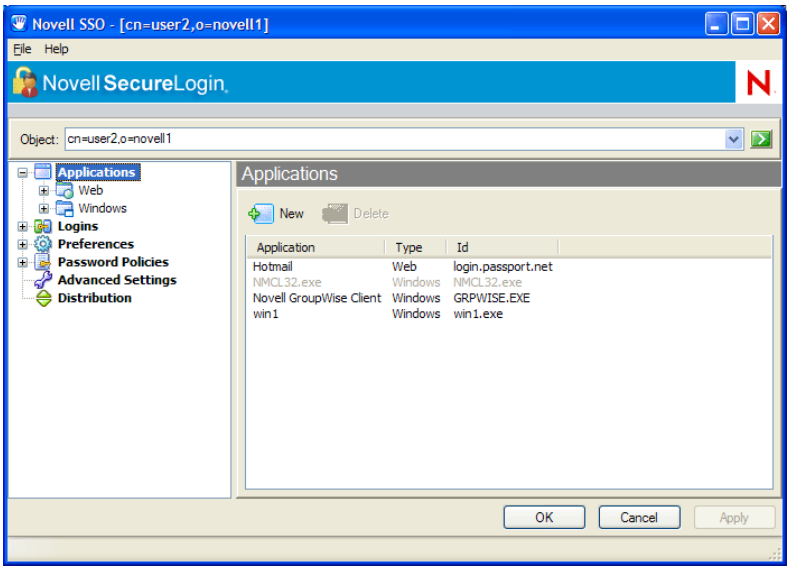
For more information, see the *Novell SecureLogin 6.0 Administration Guide*.

3.2 Administrative Management Utility User Interface

The Administrative Management Utility user interface consists of a title bar, menu bar, context bar, panes, and properties tables.

Selecting a folder in the navigation tree displays the related information in the right pane. To display the objects associated with the folders in the navigation tree, click the plus sign next to the icon to expand its contents.

Figure 3-2 *Administrative Management Utility*



The navigation tree contains the following:

- Applications
- Logins
- Preferences
- Password Policies
- Advanced Settings
- Distribution

3.2.1 Title Bar

The title bar is the bar at the top of the application which displays the application's name.

Figure 3-3 *Personal Management Utility Title Bar*

Figure 3-4 *Administrative Management Utility Title Bar*

3.2.2 Menu Bar

The menu bar appears below the title bar in the Administrative Management Utility and Personal Management Utility. It is used to select menus and commands to perform actions in the software.

Figure 3-5 *Menu Bar*

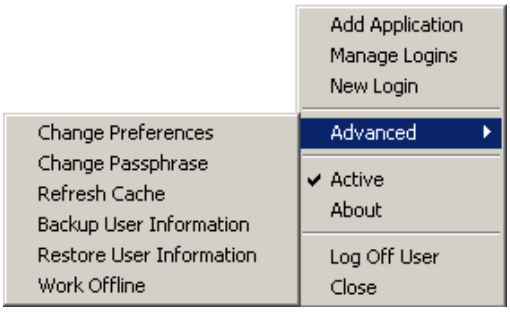
Table 3-1 *Menu Options*

Menu	Command	Function
File	New Application	Displays New Application dialog box.
	New Login	Displays Create Login dialog box.
	New Password Policy	Displays New password policy dialog box.
Help	Help	Provides user access to Help information.

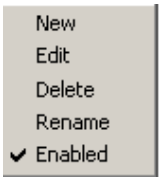
3.2.3 Shortcut Menu

Right-clicking some elements in the Administrative Management Utility, Personal Management Utility, and iManager plug-ins usually displays a shortcut menu that provides support for the most common tasks. The commands that it displays are different for each element. To access shortcut menu commands, click inside the element that you want to work with, and then right-click.

Shortcut menu for the SecureLogin icon



Shortcut menu for the Applications pane



Shortcut menu for the Logins pane

Shortcut menu for the Password Policies pane

3.3 SecureLogin Icon

The SecureLogin icon appears on the workstation's system tray and provides quick access to common functions in the management utilities and wizards.

Table 3-2 *SecureLogin Icon Description*

If...	Then...
SecureLogin is active.	The SecureLogin icon appears in the system tray as 
SecureLogin is inactive.	The SecureLogin icon appears in the system tray as 
	NOTE: SecureLogin does not perform SSO functions such as decrypting and passing credentials to applications while it is inactive.

To display the following options, right-click the SecureLogin icon:

Table 3-3 *Commands and their functions*

Options	Function
Add Application	Starts Add Application Wizard.
Manage Logins	Starts Personal Management Utility.
New Login	Starts Add New Login Wizard.
Advanced	For more information see Section 3.3.1, "Advanced Sub-Menu," on page 20.
Active	Displays check mark when SecureLogin is active on workstation.
About	Displays information about SecureLogin and your system.
Log Off User	Allows you to shut down all programs, including SecureLogin and log off from workstation.

Options	Function
Close	Closes SecureLogin on the workstation.

3.3.1 Advanced Sub-Menu

Following options are found on the Advanced submenu:

Table 3-4 *Description of Advanced Submenu options*

Options	Function
Change Preferences	Starts Personal Management Utility with Preferences Properties Table displayed.
Change Passphrase	Displays Passphrase dialog box. (Enables users to change the passphrase response.)
Refresh Cache	Manually executes synchronization of data between local cache and directory data.
Backup User Information	Enables local workstation settings.
	NOTE: Includes credentials, to be saved to an encrypted XML file.
Restore User Information	Enables backup of XML file to be restored to local workstation SecureLogin cache.
Work Offline/Work Online	Toggles between offline and online network access.
	NOTE: Displays if users are connected to a network (does not display in stand-alone mode)
	It is not necessary to manually select or clear this option, it has been automated in SecureLogin.

3.4 Application Types and Descriptions

The following table describes application types:

Table 3-5 *Application Types Descriptions*

Icon	Application Type	Description
	Generic	Name of application executable.
	Java	Web page URL containing the JavaScript logon. For example, http:/ javaboutique.internet.com/KiserPassword. Class name of application (if it is a stand-alone Java application).

Icon	Application Type	Description
	Startup	An application you choose to run after SecureLogin starts. Unlike other application types, any name is permitted. You must configure this in the application definition editor. For more information, see the *Novell SecureLogin 6.0 Application Definition Guide*.
	Terminal Emulator	Name of emulator, for example, PLAY3270.A3D.
	Web	All or part of the URL of the Web page or application. The name can apply to an entire Web site or a specific Web page. For example, the domain name www.novell.com activates the SecureLogin application definition on any page on the Novell Web site. Alternatively specifying www.novell.com/documentation/nsl60/index.htm activates the application definition solely on the specified Web page.
	Windows	Name of application executable, for example, `notepad.exe`.

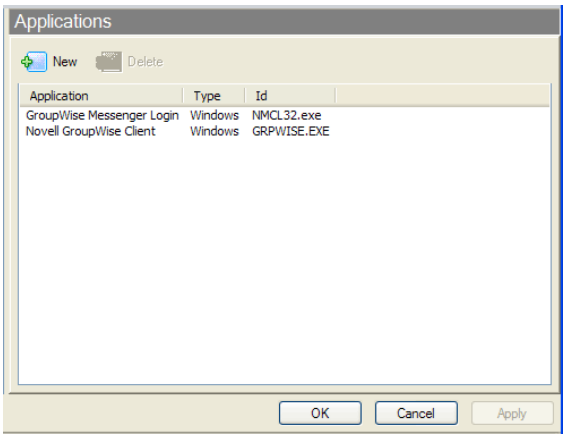
The following table describes application details:

Table 3-6 *Application details*

Icon	Description
	A red triangle in the lower right corner of an application icon denotes a Corporate Application Definition. A Corporate Application Definition is one that has been inherited from a higher-level object, for example, an organizational unit.
	Application definition or predefined application that has no inheritance from a higher level object.

3.5 Applications Pane

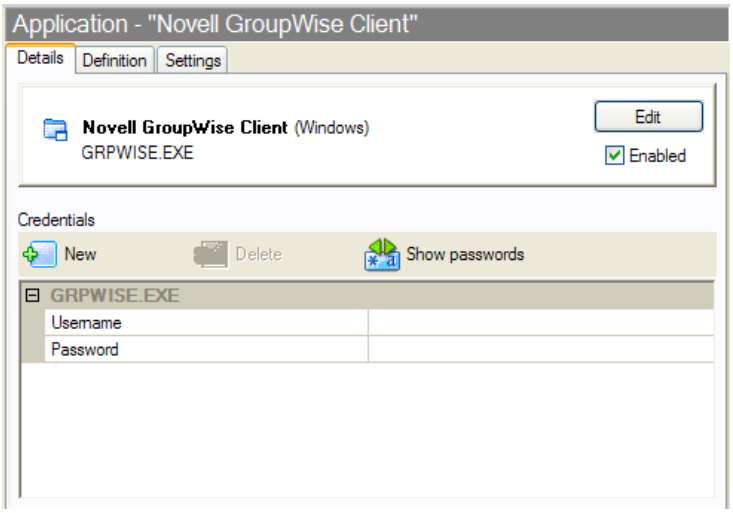
Figure 3-6 *Applications pane*



From the Applications pane, you can create and modify SecureLogin application definitions that SSO-enable applications. For more information, see *Novell SecureLogin 6.0 Application Definition Guide*.

If you double-click an application in the navigation tree or in the Applications pane, then the Application pane for that specific application is displayed.

Figure 3-7 *Application pane for specific application*



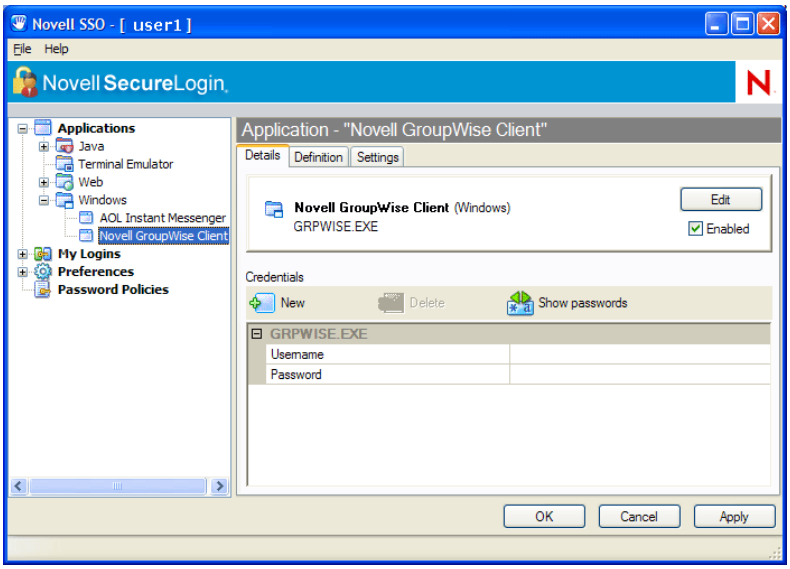
The Application pane contains three tabs:

- Details tab
- Definition tab
- Settings tab

3.5.1 Details Tab

The Details tab contains the following:

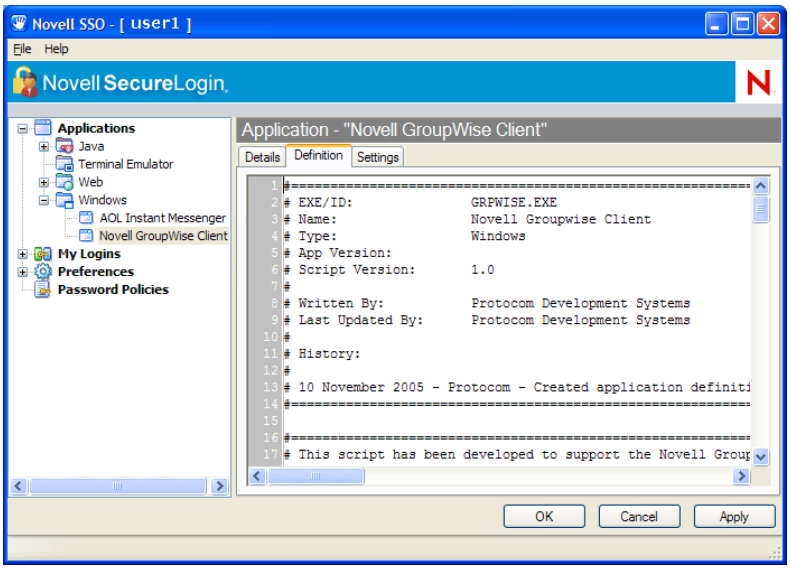
- Application description that uniquely identifies the application definition or predefined application along with the type of application. The application definition or predefined application is either the name given by SecureLogin or the name entered by the user.
- Application name.
- Credentials (logins) linked to the application and tools to create, edit, and delete these credentials.



3.5.2 Definition Tab

The Definition tab contains the application definition. An application definition directs how SecureLogin responds to various screens that are returned by the application. The details displayed are either the application definition created by SecureLogin when the predefined application or application definition was added, or the application definition that was manually created by the user.

Figure 3-8 *Definition tab*



3.5.3 Settings Tab

The Settings tab contains advanced options for the predefined application or application definition.

The following table describes the settings for Web applications:

Figure 3-9 *Settings tab for Web applications*

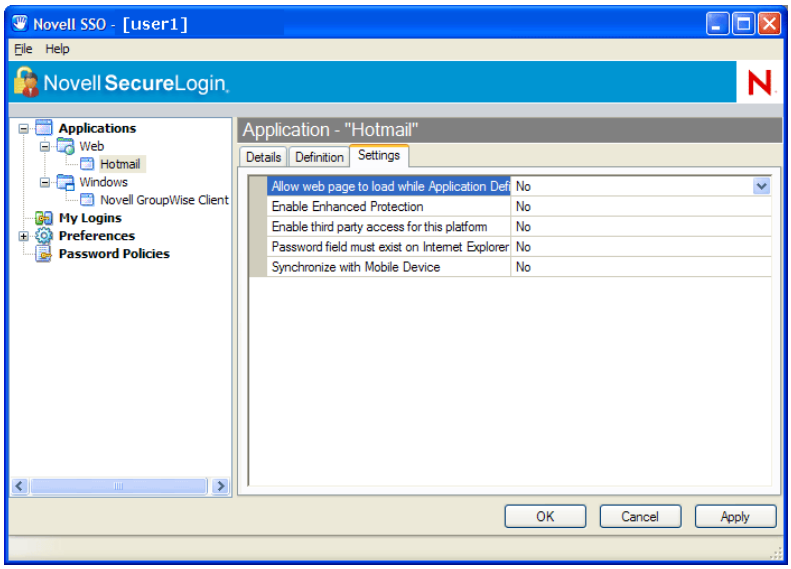
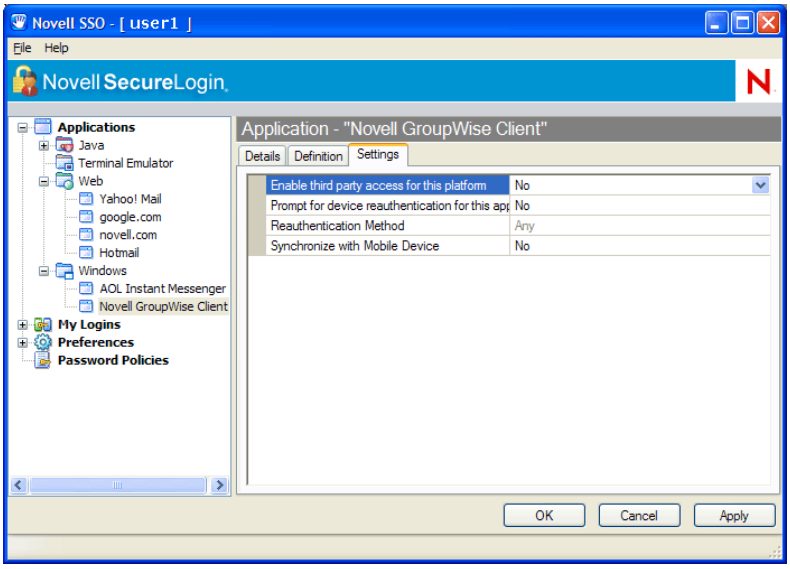


Table 3-7 *Settings for Web Applications*

Item	Description
Allow web page to load while Application Definition is running (Web applications only)	Applies to Microsoft* Internet Explorer and application definitions created for Web pages and JavaScript logons that execute in a Web page. Set to No by default, this suspends completion of any other Internet Explorer tasks until logon has completed. Selecting Yes enables Internet Explorer to continue functioning while SecureLogin is executing logon.
Enable third party access for this platform	Disables API access for this predefined application or application definition. Default setting is No.
Password field must exist on Internet Explorer page for Application Definition to run (Web applications only)	Applies to Microsoft Internet Explorer and application definitions created for Web pages and JavaScripts within Web pages. Selecting Yes ensures SecureLogin does not execute automated logon on pages without a password field. You might need to select No if your Web application returns errors on pages without password fields that you need to handle with SecureLogin (Change Successful message, for example).
Prompt for device reauthentication for this application.	Select Yes to prompt for device reauthentication for the application.
Reauthentication Method	Allows you to reauthenticate an application against an AA device where SecureLogin is used in conjunction with SLAA or NMAS infrastructure.
Synchronize with Mobile Device	Enables synchronization with API-enabled handheld device, for this predefined application or application definition. Default setting is No.

Figure 3-10 *Settings tab for Windows application*



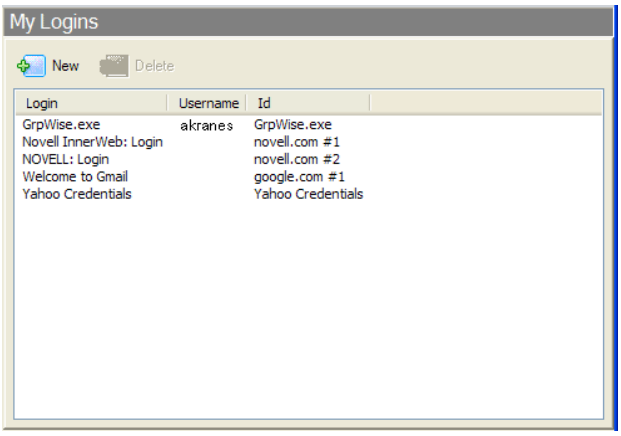
The following table describes the settings for Windows applications:

Table 3-8 *Settings for Windows Applications Here*

Item	Description
Enable third party access for this platform	Disables API access for this predefined application or application definition. Default setting is No.
Prompt for device reauthentication for this application	Select Yes to prompt for device reauthentication for the application.
Reauthentication Method	Allows you to reauthenticate an application against an AA device where SecureLogin is used in conjunction with SLAA or NMAS infrastructure.
Synchronize with Mobile Device	Enables synchronization with API-enabled handheld device, for this predefined application or application definition. Default setting is No.

3.6 Logins Pane

Figure 3-11 *Logins pane*



The My Logins pane in the Personal Management Utility pane manages logins that applications require to logon and their associated credentials, including:

- User name
- User ID
- Logon ID
- Password
- PINs
- Domain
- Database names
- Server IP address

You can:

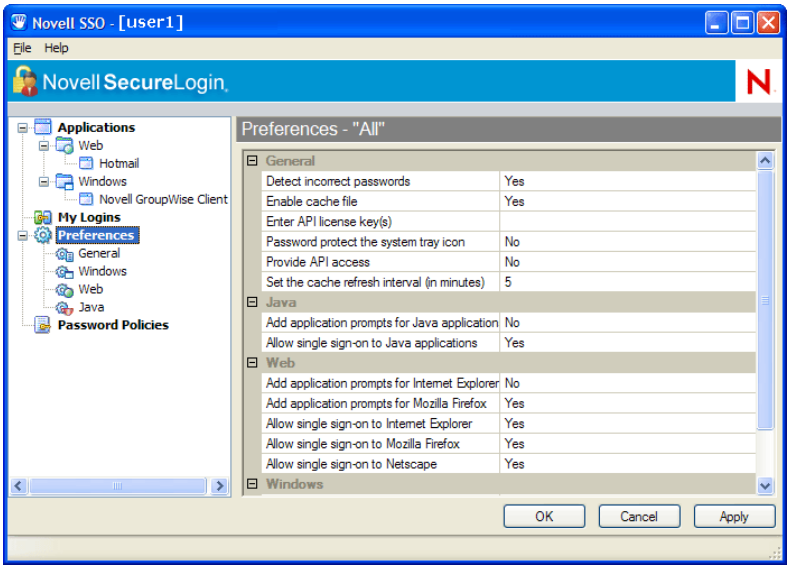
- Manually link logins, including host IP addresses, to applications.
- Configure Credential Sets at the Group Policy, organizational unit, container and user object level.
- Enable a group of users to be configured with seamless logon access to an application with one account of user name and password.

3.7 Preferences Properties Table

The Preferences Properties Table provides tools to configure the parameters of the user's SecureLogin environment, including applications permitted to be SSO-enabled and access to SecureLogin management and administration tools. Preference options, in addition to those

provided in the Personal Management Utility, are provided in this table for directory management tools

Figure 3-12 *Preferences Properties table*



The Preferences Properties Table displays in the right pane after you click *Preferences* in the navigation tree.

Preferences are divided into the following categories:

- General
- Windows
- Web
- Java
- Security

You can:

- Change the values in the Preferences Properties Table of the Administrative Management Utility, iManager plug-in, or the Personal Management Utility, unless otherwise specified.
- Restrict user's access to this table through centrally controlled administrative preferences.

3.7.1 Preferences Properties Table Fields

The following table describes the Preferences Properties Table fields:

Table 3-9 *General Preferences*

Item	Description	Comment
Allow users to activate or deactivated SSO through the system tray	Allows an administrator to prevent users from deactivating SSO through the SecureLogin icon on the task bar.	Not available in the Personal Management Utility.
Allow users to backup/ restore	Enables or disables access to backup and restore user information.	Not available in the Personal Management Utility.
Allow users to change passphrase	Enables or disables access to change passphrase question and answer.	Not available in the Personal Management Utility.
Allow users to modify credentials through the GUI	Allows users to view their credentials but not modify them (by allowing “users to view passwords” and then by setting this preference to No).	Not available in the Personal Management Utility.
Allow users to modify names of applications and logins	Enables or disables access to change values in the Logins and Applications panes.	Not available in the Personal Management Utility.
Allow users to view and change preferences	Enables or disables the option to change preference values. Setting the value to No displays a warning message.	We recommend you create a separate organizational unit for administrators to ensure they are not adversely affected by general user configuration at the OU level. Not available in the Personal Management Utility.
Allow users to view and modify API preferences	Enables user access to API options displayed in the Preferences pane of the Personal Management Utility.	Contact Novell Technical Services for assistance with APIs. Not available in the Personal Management Utility.
Allow users to view and modify application definitions	Enables or disables access to configure applications for SSO in the Applications pane.	Not available in the Personal Management Utility.
Allow users to view passwords	Enables or disables the Show Passwords button in the Details tab of the Applications pane of the Personal Management Utility.	Allowing users to view their passwords gives them an opportunity to view and record passwords if they need to reset their SecureLogin configuration. Resetting a user deletes all SecureLogin data including passwords and passphrase responses. Not available in the Personal Management Utility.

Item	Description	Comment
Container has priority over User	The default setting is No. This value indicates that configuration settings made by the user take precedence over those set at the container level. Only for use in advanced stand-alone mode for the overwriting of locally applied scripts, settings and credentials by centrally created ones. This is for users who receive their encrypted and signed settings through the Distribution pane “signed and encrypted” method.	Not available in the Personal Management Utility.
Detect incorrect passwords	Detect incorrect passwords is, by default, set to Yes. Predefined applications generally include commands to respond to incorrect password dialogs; however, this preference enables SecureLogin to respond to incorrect passwords for Web applications.	
Disable single sign-on	The default setting is No, however to prohibit any access to SecureLogin select Yes.	Not available in the Personal Management Utility.
Display the system tray icon	Enables or disables the SecureLogin icon on the system tray.	When the SecureLogin icon is active, you can double-click it to start the Personal Management Utility. When the SecureLogin icon is inactive, users can still start the Personal Management Utility through the Windows Start menu, unless the option has been disabled during installation. Not available in the Personal Management Utility.
Enable cache file	Enables the creating and updating of a SecureLogin cache file on the local workstation. This cache file stores all user configuration data local and inherited. Set this value to: • Yes for mobile users. • No when storing files locally is not possible or conflicts with organization security policies.	

Item	Description	Comment
Enable logging to Novell Audit	Allows the following events to automatically be sent to a Novell Audit server for the OU or user object against which this is set: • SSO client started • SSO client exited • SSO client activated by user • SSO client deactivated by user • Password provided to an application by a script • Password changed by the user in response to a `changepassword` command • Password changed automatically in response to a `changepassword` command	You can turn on/off the Novell Audit support with a SecureLogin preference. You must install the Novell Audit platform on the client, and register the application ID and schema file on the server. For more information, see the Novell Audit ID and schema files in the Tools folder of the SecureLogin distribution CD. Not available in the Personal Management Utility.
Enable the New Login Wizard on the system tray icon	Enables users to create multiple SSO logons for different accounts on the same application or server using the Add New Login Wizard.	Not available in the Personal Management Utility.
Enforce passphrase use	After SecureLogin is installed, users are required to set up their passphrase authentication. This may require creating a question and response, or providing a response to a question you have created. If this value is set to: • Yes, users must complete the set up of their passphrase before they can proceed with any other activity on the workstation. • No, users can click Cancel and will be prompted with the Passphrase dialog box each time they log on to the workstation until the passphrase is set.	Not available in the Personal Management Utility.
Enter API license key(s)	Enter the API license key provided by SecureLogin to activate API functionality for an application. Contact Novell Technical Services for help configuring APIs.	

Item	Description	Comment
Password protect the system tray icon	Restricts the logged-in users from using the SecureLogin icon shortcut menu without their network password. This password cannot be manually created or changed.	
Provide API access	Enables or disables API functionality. Contact Novell Technical Support for assistance in configuring APIs.	
Set the cache refresh interval (in minutes)	The cache refresh interval defines the regularity (in minutes) of the synchronization of the user data and directory on the local workstation. The default value is five minutes. We recommend between 240 and 480 minutes (4 and 8 hours) depending on your network, number of users, and how often data changes.	Right-click the SecureLogin icon on the system tray, then point to Advanced, and click Refresh Cache to manually refresh the cache.
Stop walking here	Enables or disables inheritance of settings from higher level containers or organizational units.	Not available in the Personal Management Utility. Select Yes during phased upgrades in which higher levels may have a different version of SecureLogin implemented. If inheritance of settings from higher levels is required, select No (the default).

Table 3-10 *Java Preferences*

Item	Description	Comment
Add application prompts for Java applications	Prompts for Java applications.	By default the Java option is set to No. If you plan to SSO-enable JavaScript logins and Java applications, set the value to Yes. (SecureLogin requires a Java Runtime Engine version 1.4 or later to SSO-enable Java-based logons.)
Allow single sign-on to Java applications	Allows SSO to Java applications.	To enable SSO access to the application type, ensure the value is set to Yes. To disable SSO to any applications of the selected type, set the value to No.

Table 3-11 *Security Preferences*

Item	Description	Comment
Allow access using passphrase when smart card not available	Allows the user to access SecureLogin by using a passphrase temporarily.	Not available in the Personal Management Utility.
Certificate selection criteria	Allows you to enter text to uniquely identify a certificate (within searchable fields only)	Not available in the Personal Management Utility.
Certificate type	Allows you to select an encryption or authentication certificate to encrypt user's SSO information in the directory.	Not available in the Personal Management Utility.
Current certificate	Allows you to select a certificate other than the default certificate.	Not available in the Personal Management Utility.
Store SSO data on smart card	Allows you to store application credentials only on smart card.	Not available in the Personal Management Utility.
Use AES for SSO data encryption	Allows you to use AES instead of Triple DES for encrypting SSO data.	Not available in the Personal Management Utility.
Use passphrase for recovery of SSO credentials	Allows passphrase to be used for recovery of SSO credentials. We recommend that you select Yes if key escrow backup is not used.	Not available in the Personal Management Utility.
Use smart card to encrypt SSO data	Allows SSO data to be encrypted using the user's PKI-based credentials, if enabled.	Not available in the Personal Management Utility.
Enable passphrase security system	Enable passphrase security system is, by default, set to Yes. Typically a user sets a passphrase when SecureLogin first runs. This option allows you to enable or disable user-defined passphrases.	Not available in the Personal Management Utility.

Table 3-12 *Web Preferences*

Item	Description	Comment
Add application prompts for Internet Explorer	Prompts for Internet Explorer	Prompts for both Internet Explorer and Netscape, but Netscape support is limited

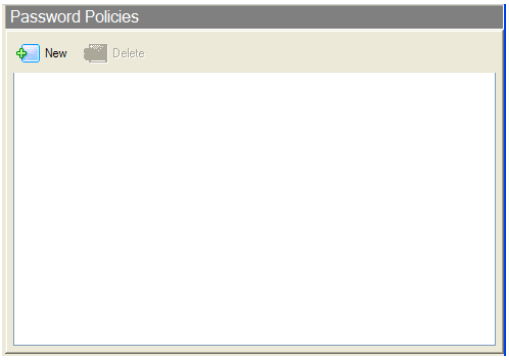
Item	Description	Comment
Add application prompts for Mozilla Firefox	Prompts for Mozilla Firefox	If set to Yes, SecureLogin displays an application prompt confirmation message when it recognizes an application type. The prompt has three options: Yes, No, and Never. Selecting: • Yes, SSO-enables the logon; SecureLogin saves the credentials entered. • No, stops SSO-enabling now, but the prompt displays the next time the Login dialog displays. • Never, ensures SecureLogin will not prompt to SSO for this Login dialog again. Disabling the display of a SecureLogin automated prompt does not restrict users from SSO-enabling the applications.
Allow single sign-on to Internet Explorer	Allows SSO to Internet Explorer	To enable SSO access to the application type, ensure that the value is set to Yes. To disable SSO to any applications of the selected type, set the value to No.
Allow single sign-on Mozilla Firefox	Allows SSO to Mozilla Firefox	To enable SSO access to the application type, ensure the value is set to Yes. To disable SSO to any applications of the selected type, set the value to No.
Allow single sign-on to Netscape	Allows SSO to Netscape	To enable SSO access to the application type, ensure the value is set to Yes. To disable SSO to any applications of the selected type, set the value to No. SecureLogin currently provides predefined applications for a range of Netscape applications but does not provide full support for all current Netscape functionality in the wizards. We recommend you manually create application definitions for Netscape applications since some functionality may be unavailable. Contact Novell Technical Services for help.

Table 3-13 *Windows Preferences*

Item	Description	Comment
Add application prompts for Windows applications	Prompts for Windows applications.	If set to Yes, SecureLogin displays an application prompt confirmation message when it recognizes an application type. The prompt has three options: Yes, No, and Never. Selecting: • Yes, SSO-enables the logon; SecureLogin saves the credentials entered. • No, stops SSO-enabling now, but the prompt displays the next time the Login dialog displays. • Never, ensures SecureLogin will not prompt to SSO for this Login dialog again. Disabling the display of a SecureLogin automated prompt does not restrict users from SSO-enabling the applications.
Allow single sign-on to Windows applications	Allows SSO to Windows applications.	To enable SSO access to the application type, ensure the value is set to Yes. To disable SSO to any applications of the selected type, set the value to No.

3.8 Password Policies Pane

Figure 3-13 *Password Policies pane*

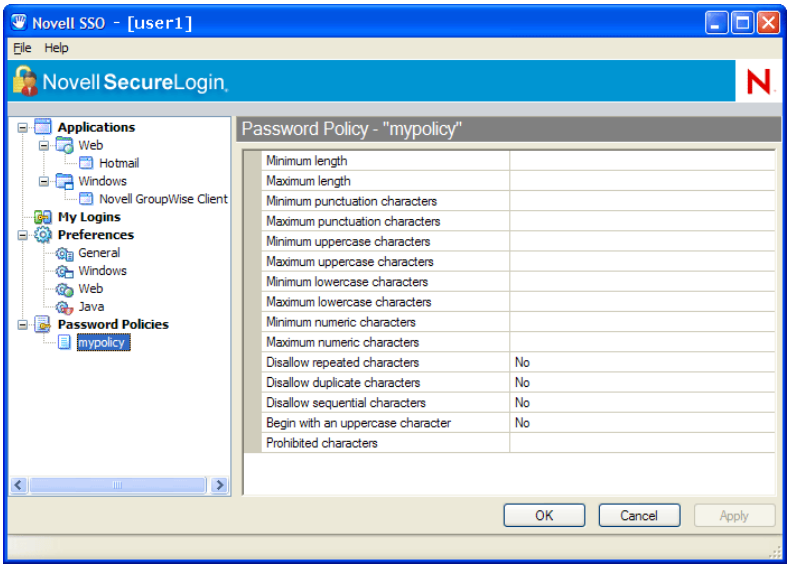


The Password Policies pane contains a list of all your password policies. In this pane you can create a new password policy or delete an existing password policy. If you want to change an existing password policy, double-click the policy you want to change, and then make the changes in the Password Policy Properties Table.

3.9 Password Policy Properties Table

Organizations and applications often have rules about the content of passwords, including the required number and type of characters. The Password Policy Properties Table helps to create and enforce these password rules through a password policy, and apply this policy to one or more application logons.

Figure 3-14 *Password Policy Properties table*



You can access the Password Policy Properties Table in one of the following ways:

- Click a policy under Password Policies in the navigation tree.
- Double-click a policy in the Password Policies pane.

NOTE: You can configure password policies in the Password Policy Properties Table of the Administrative Management Utility, the SSO plug-in of the iManager, or Group Policy snap-ins

3.9.1 Password Policy Properties Table Fields

The following table describes the Password Policy Properties Table fields:

Table 3-14 *Password Properties Table Fields Here*

Rule	Value	Comment
Minimum length	Whole number	Minimum zero, no upper limit.
Maximum length	Whole number	Minimum zero, no upper limit.
Minimum punctuation characters	punctuation character	Minimum zero, no upper limit.
Maximum punctuation characters	Whole number	Minimum zero, no upper limit.
Minimum uppercase characters	Whole number	Minimum zero, no upper limit.

Rule	Value	Comment
Maximum uppercase characters	Whole number	Minimum zero, no upper limit.
Minimum lowercase characters	Whole number	Minimum zero, no upper limit.
Maximum lowercase characters	Whole number	Minimum zero, no upper limit.
Minimum numeric characters	Whole number	Minimum zero, no upper limit.
Maximum numeric characters	Whole number	Minimum zero, no upper limit.
Disallow repeat characters	No, Yes, and Yes, case insensitive	Yes is not case sensitive, therefore does not prohibit upper or lowercase of the same character.
Disallow duplicate characters	No, Yes, and Yes, case insensitive	Yes does not prohibit upper/ lowercase of the same character.
Disallow sequential characters	No, Yes, and Yes, case insensitive	Yes is not case sensitive. This setting applies to any sequence direction, for example, 87654 and edcba.
Begin with uppercase character	Yes, No	Default is No.
Prohibited characters	Keyboard characters	Case sensitive.

3.10 Advanced Settings Pane

The Advanced Settings pane contains three tabs.

Figure 3-15 *Advanced Settings Pane*

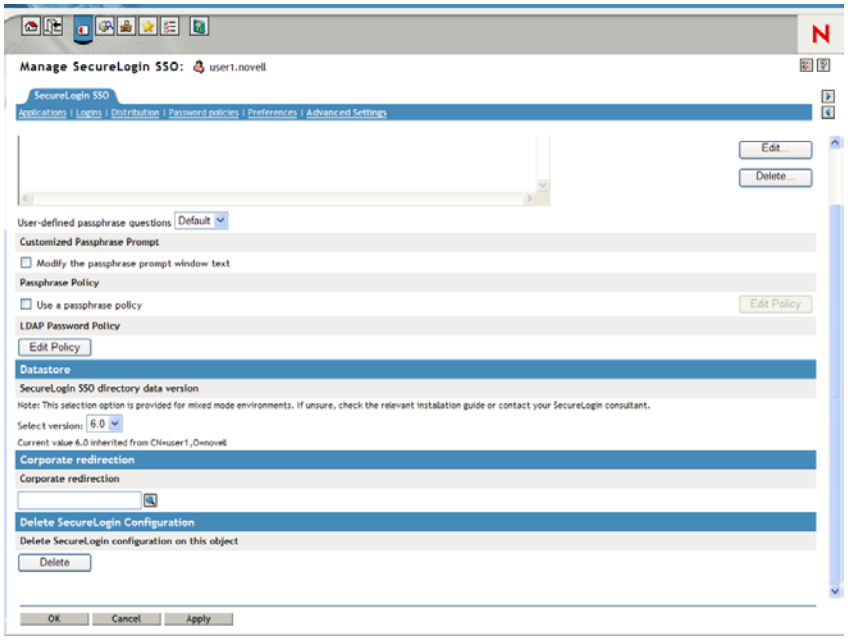


Table 3-15 *Enter Table Title Here*

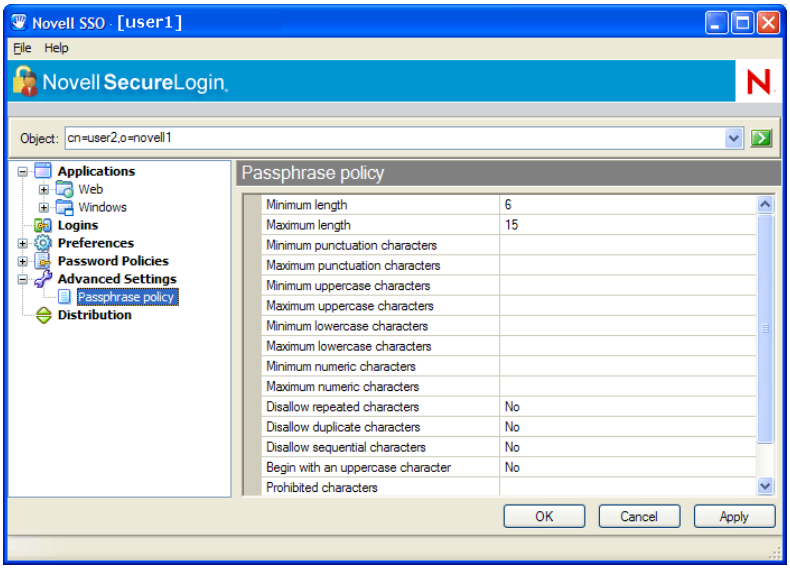
Tab Name	Description
Passphrase	Contains fields for: • Creating, editing, and deleting corporate passphrase questions. • Customizing passphrase prompts. • Editing passphrase policies.
Datastore	Used for: • Selecting directory data version details (for mixed mode environments using earlier versions of the client software). • Deleting the SecureLogin configuration for a datastore object.
Corporate redirection	Used for managing configuration from one directory object when multiple containers/organizational units require the same SecureLogin environment.

NOTE: This pane is not available in the Personal Management Utility.

3.11 Passphrase Policy Properties Table

Organizations and applications often have rules about the content of passphrase, including the required number and type of characters. The Passphrase Policy Properties Table helps to create and enforce these passphrase rules through a passphrase policy, and apply this policy to one or more application logons.

Figure 3-16 *Passphrase Policy Properties table*



The Passphrase Policy Properties Table displays after you click *Edit Policy* on the *Passphrase* tab in the *Advanced Settings* pane.

NOTE: You can configure passphrase policies in the Passphrase Policy Properties Table of the Administrative Management Utility, the iManager plug-in, or Group Policy snap-ins.

3.11.1 Passphrase Policy Properties Table Fields

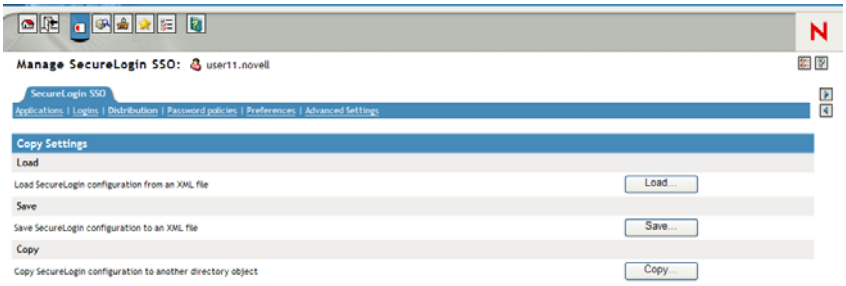
The following table describes the Passphrase Policy Properties Table fields.

Table 3-16 *Passphrase Policy Properties Table Fields Description*

Rule	Value	Comment
Minimum length	Whole number	Minimum zero, no upper limit.
Maximum length	Whole number	Minimum zero, no upper limit.
Minimum punctuation characters	punctuation character	Minimum zero, no upper limit.
Maximum punctuation characters	Whole number	Minimum zero, no upper limit.
Minimum uppercase characters	Whole number	Minimum zero, no upper limit.
Maximum uppercase characters	Whole number	Minimum zero, no upper limit.
Minimum lowercase characters	Whole number	Minimum zero, no upper limit.
Maximum lowercase characters	Whole number	Minimum zero, no upper limit.
Minimum numeric characters	Whole number	Minimum zero, no upper limit.
Maximum numeric characters	Whole number	Minimum zero, no upper limit.
Disallow repeat characters	No, Yes, or Yes, case insensitive	Yes is not case sensitive therefore, does not prohibit upper/lowercase of the same character.
Disallow duplicate characters	No, Yes, or Yes, case insensitive	Yes does not prohibit upper/ lowercase of the same character.
Disallow sequential characters	No, Yes, Yes, case insensitive	Yes is not case sensitive. This setting applies to any sequence direction for example, 87654 and edcba.
Begin with uppercase character	Yes, No	Default is No.
Prohibited Characters	Keyboard characters	Case sensitive

3.12 Distribution Pane

Figure 3-17 *Distribution Pane*



The Distribution pane provides access to the following:

- Load dialog box
- Save dialog box
- Manage signing keys for secure file distribution dialog box

  These dialog boxes help you import and export SecureLogin configurations.
- Copy dialog box

  This dialog box helps you copy an object's SecureLogin configuration from one object to another.

NOTE: This pane is not available in the Personal Management Utility.

Enabling Applications and Web Sites for SSO

4

SecureLogin:

- Has predefined applications for SSO access to a wide range of commercially available applications.
- Detects applications for which a predefined application exists. For example, if SecureLogin detects an SAP logon dialog box, then SecureLogin displays a prompt providing the user with the option to allow SecureLogin to automatically SSO the application.

  NOTE: Predefined applications for commonly used applications are provided with the SecureLogin application, and with each new version, more are developed and made available to Novell customers.

- Provides wizards and application definitions to facilitate SSO to almost any new or proprietary application if a predefined application is not available. This helps you or Novell Technical Services to build an application definition for almost any proprietary application or upgrade. For more information, see Chapter 2, "SecureLogin Components," on page 11.
- Supports SSO-enabling of most standard terminal emulator applications.

  NOTE: You can SSO-enable terminal emulators using the Terminal Launcher tool. For more information, see *Novell SecureLogin 6.0 Administration Guide*.

- Has additional SSO tools, such as the Window Finder and LoginWatch, which help you SSO-enable even the most difficult applications. For more information, see *Novell SecureLogin 6.0 Administration Guide*.
- Stores the login information requirements for applications including:

Credentials, including but not limited to:	Username
	UserID
	LoginID
	Password
	PINs
	Domain
	Database names
	Server IP address

Responses to dialog boxes, messages and windows events, such as:	Login Incorrect credentials Password expiration and reset Error messages, including non-compliance to password rules Account locked Database unavailable

Before SecureLogin can SSO-enable an application for a particular user, it must “learn” a user’s application credentials so it can encrypt and store them for future logins unless it is used in conjunction with Identity Management solutions such as IBM Tivoli.

When a user starts an application for the first time after it has been SSO-enabled, SecureLogin prompts the user for application credentials, and then encrypts and stores them in the directory against the user object. The credentials are passed automatically to the application for subsequent logons.

Automated SSO is achieved using proprietary application definitions. Application definitions are managed in directory environments through SecureLogin management utilities, including the Administrative Management Utility, iManager plug-ins, and Active Directory MMC snap-ins. Locally and in stand-alone deployments, application definitions are managed in the Personal Management Utility or distributed using the advanced offline signed and encrypted method.

SSO-enabled applications are created, modified and deleted in the Applications pane. You can also create application definitions with SecureLogin wizards. There are a wide range of options in SecureLogin to enable applications. Regardless of the origin of the application definition, when an application is SSO-enabled, it is added and maintained in the Applications Properties Table.

For detailed procedures about enabling applications and Web sites for SSO, see *Novell SecureLogin 6.0 Administration Guide*

Operational Environment

5

This section contains the following information:

5.1 Operating Systems

- Microsoft* Windows XP SP 2
- Microsoft Windows 2000 Workstation SP 4

5.2 Platforms

- Novell® eDirectory
- Most Lightweight Directory Access Protocol version 3 (LDAP V.3) compliant directories, operating on any of the following platforms:
  - Novell NetWare 4.x or later
  - Microsoft Windows 2000/2003 Server
- Microsoft Active Directory Application Mode (ADAM)
- Microsoft Active Directory

5.3 Clients

- Citrix Win32 ICA Client V.6.00.905 or later
- Microsoft Terminal Services Clients, RDP version 5.0 or later
- Novell Client for Windows 2000 and XP version 4.7 or later

NOTE: If your environment is not included in this list, contact Novell Customer Support for help.

5.4 Windows

Some of the predefined applications for Windows applications are:

- AOL Instant Messenger
- Citrix Program Neighborhood
- Entrust Client

- Internet Explorer
- Lotus Notes v5 and v6.5
- Microsoft Outlook Express
- Novell GroupWise Client
- Novell Groupwise Notify Client
- Novell iFolder

NOTE: If SecureLogin does not prompt to SSO-enable the application, use the Add Application Wizard to build an application definition.

5.5 Terminal Servers

Citrix® MetaFrame 1.8 and above, including:

- Citrix MetaFrame XP Presentation Server
- Citrix MetaFrame Presentation Server 3.0
- Microsoft Windows 2000 Terminal Server
- Microsoft Windows 2003 Terminal Server

5.6 Terminal Emulators

SecureLogin provides SSO support for applications running on any back end system (e.g., UNIX, RACF, CICS, ACF2) using emulators such as:

- Attachmate KEA!
- Attachmate Personal Client
- Eicon Aviva
- HBO Star Navigator
- Microsoft Telnet 2000
- Passport TN 3270E
- PowerTerm
- QWS3270 Plus
- TeraTermPro
- Tiny Term
- ViewNow
- WallData Rumba
- WinComm
- Window Telnet VT
- WRQ Reflection

5.7 Web/Internet

SecureLogin includes SSO support for Web applications accessed using the following browsers:

- Internet Explorer
- Mozilla Firefox
- Netscape

NOTE: SecureLogin currently provides predefined applications for a range of Netscape applications. However, it does not provide support for all current Netscape functionality in the wizards. We recommend you to manually create application definitions for Netscape applications, since some functionality may be unavailable. SecureLogin does include full support for Mozilla Firefox. If you want to SSO-enable a Netscape application that is not provided as a predefined application, contact Novell Technical Services for help.

SecureLogin provides predefined applications for a number of Web applications with embedded logon fields, including:

- Citrix Web Portal
- CNN Member Services
- eBay
- Fidelity.com Web Logon
- Hotmail
- Onebox.com
- Qantas Frequent Flyer
- Yahoo! Mail
- Monster.com

NOTE: If a predefined application is available for the application, the SecureLogin prompt will display when you log in to the application. Use the Add Application Wizard to build an application definition for the application.
