AUTHORIZED DOCUMENTATION

Overview Guide

Novell® SecureLogin

6.1 SP1

June, 2009

www.novell.com

Legal Notices

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

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

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

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

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

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About This Guide

This document provides to you an overview of the features, functionality, customizing, and administration of Novell® SecureLogin.

Audience

This guide is intended for:

- Network administrators
- System administrators
- IT support staff
- End users

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 the Novell Feedback Web site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Documentation Updates

For the most recent version of the *Overview Guide*, visit the Novell Documentation Web site (http://www.novell.com/documentation/securelogin61/index.html).

Additional Documentation

Novell SecureLogin 6.1 Overview is a part of documentation set for Novell SecureLogin 6.1. Other documents include:

- *Novell SecureLogin 6.1 SP1 Installation Guide*
- *Novell SecureLogin 6.1 SP1 Administration Guide*
- *Novell SecureLogin 6.1 SP1 Application Definition Guide*
- *Novell SecureLogin 6.1 SP1 Citrix and Terminal Services Guide*
- *Novell SecureLogin 6.1 SP1 User Guide*

- Quick Start. *NMAS Login Method and Login ID Snap-In for pcProx*
- Readme. Available online at the Novell Documentation Web site. (http://www.novell.com/documentation/securelogin61/index.html)

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.

About Novell SecureLogin

1

In large enterprises and organizations, employees must interact with multiple applications and access sensitive information. Each application has its own authentication methods that require users to specify different usernames and passwords. This forces the users to maintain and manage different usernames and passwords to each of the numerous applications, which can be inconvenient and difficult.

To resolve these issues, a solution is needed to avoid the necessity of users remembering numerous passwords while simultaneously providing users access to the required sensitive data without compromising on security.

Novell SecureLogin is a single sign-on product that provides this kind of ease for password management.

Novell SecureLogin has the following features:

- Eliminates the requirement for users to remember multiple usernames and passwords beyond their initial login. It stores usernames and passwords and automatically specifies them for users when required. With this feature, users are no longer required to remember and manually provide their credentials to log in to an application.
- It quickly retrieves and specifies user credentials, which results in faster login.
- It helps reduce calls to the Help Desk about locked accounts and forgotten usernames and passwords.
- It makes use of multiple integrated security systems that provide authentication and single sign-on to networks and applications.

  It provides a single entry point to the corporate network and its user resources, which increases security and enhances compliance with corporate security policies.
- It 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.

  With this level of encryption, an administrator with complete rights cannot view a user's credentials.

  If required, an administrator can set a new password under some circumstances, such as disaster recovery, but cannot view the existing password.

Other Advantages

- Novell SecureLogin utilities and components are designed to enable single sign-on for Windows*, Web, and terminal emulator applications.
- It supports both username and password authentication, and also multi-factor authentication such as smart card, token, or biometric authentication at the network and application levels.

- It employs two methods of fault tolerance:
  - It uses local encrypted caching to ensure that the network downtime does not affect the single sign-on performance. If the corporate network is down, caching enables application logins to continue uninterrupted.
  - It uses application definitions to cater to different login conditions and errors during the login.
- It maintains single sign-on integrity for all mobile and remote users by locally encrypting the cache regardless of the network connectivity. If permitted, mobile users can update their single sign-on credentials when they are disconnected from the network and update the directory with these details when they attach later.

  Because Novell SecureLogin is a directory-enabled product, users can:
  - Log in from anywhere and get capabilities as if they were working from their own desks.
  - Log in and log out quickly because they authenticate only to the directory, and not to Windows itself.
  - Roam the enterprise and log in to different machines during the day.
  - Work on a 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, then log out.

Additional Tools

- Novell SecureLogin includes wizards, directory console plug-in, and tools which make it easy to centrally configure for use on the corporate network.
- Includes management utilities that allows the administrators and end-users to view their single sign-on details and, if permitted enable single sign-on applications.

New Features

2

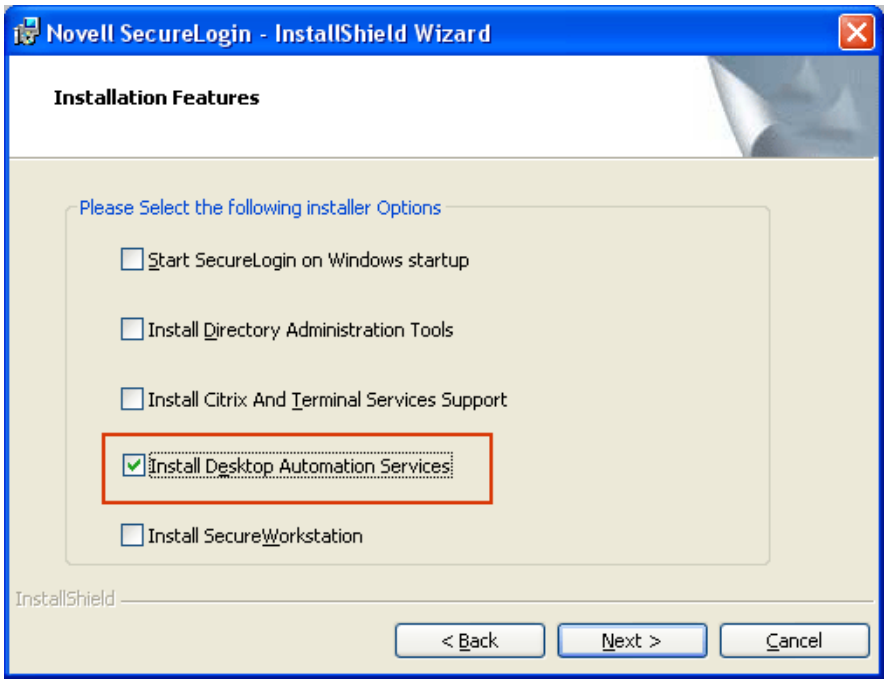
Following is the new feature introduced in the Support Pack (SP) release of Novell SecureLogin 6.1:

2.1 Integration of Desktop Automation Services

With this release of Novell SecureLogin, you can choose to install Desktop Automation Services (DAS) along with Novell SecureLogin.

Previously, DAS was released as a standalone component and you had to downloaded it separately for use with Novell SecureLogin. With this release, you can install DAS during the installation process of Novell SecureLogin 6.1 SP1*Install Desktop Automation Services* is one of the options displayed on the Installation Features during the installation of Novell SecureLogin 6.1 SP1.

Figure 2-1 *Selecting to install DAS*



2.2 Support for Prebuilt Script

Novell SecureLogin comes with prebuilt script, which is installed when installing Novell SecureLogin.

However, if you want to use an customized prebuilt script, do one of the following before installing Novell SecureLogin:

2.2.1 Replacing the Default Prebuilt Script

1. Place your prebuilt script (`pbscript.dll`) at `C:\`, which is the default path of the customized prebuilt script.
2. Run Novell SecureLogin.
3. Follow the wizard instructions and install Novell SecureLogin.

NOTE: Novell Securelogin installer replaces the original `pbscript.dll` (present in the installation directory) with the customised pbscript.dll present on C:drive.

2.2.2 Replacing the Default Prebuilt Script Present In the Custom Path

1. Place your prebuilt script (`pbscript.dll`) at the custom path for example, `D:\SecureLogin_Cutomizedscript`.
2. Install Novell SecureLogin with the `msiexec /i "NSL MSI path" X_PBSCRIPT=`<custom path> for example, “D:\SecureLogin_Standalone”

NOTE: Novell Securelogin installer replaces the original `pbscript.dll` (present in the installation directory) with the customized `pbscript.dll` from the custom path (in this example, “D:\SecureLogin_Standalone”)

The Novell SecureLogin Components

3

This section discusses the following topics:

3.1 The Novell SecureLogin Management Utilities

Table 3-1 *Novell SecureLogin Management Utilities*

Use This Utility	To Manage These Users
Administrative Management utilities	Centrally in a directory environment at the user object, Group Policy, Container, or the Organizational Unit (OU) level. For more information, see Section 4.2, “The Administrative Management Utilities,” on page 20. The administrative management utility includes the Novell iManager. In a corporate environment, the administrators can allow or prohibit all or part of this utility, depending on the organizational requirements. For more information, see “Installing Administrative Tools for eDirectory” in the *Novell SecureLogin 6.1 Installation Guide*.
Personal Management utility	Users in the standalone mode. Users can configure the local workstation for the logged-in user. This utility has the same functionality as the Administrative Management utility, excluding some preference options, advanced settings, and secure settings distribution. Administrators can disable the users from accessing this utility in a directory environment. For more information, see Section 4.1, “Personal Management Utility,” on page 19

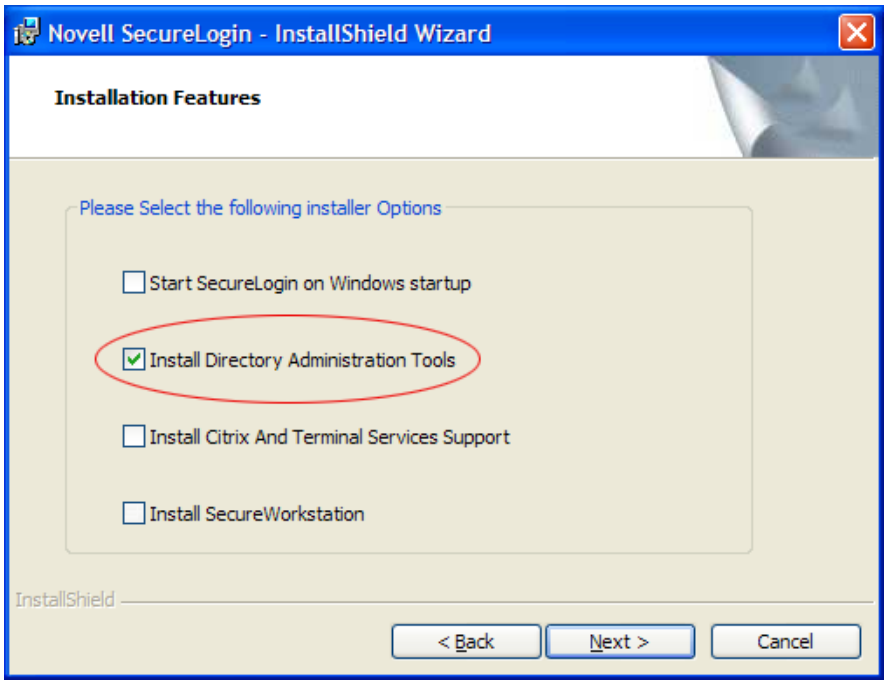
Use This Utility	To Manage These Users
Active Directory Users and Computers snap-in	Centrally in an Active Directory environment. Using Microsoft Active Directory, Novell SecureLogin installs an administration tab in the Users and Computers Properties snap-in. This provides access to the administrative management utility functionality. In a corporate environment you can allow or prohibit full or part access to this utility depending on organizational requirements.

3.2 Active Directory Users and Computer Snap-In

In Microsoft* Active Directory* environment, you can manage users centrally from the Active Directory users and computer snap-in.

The snap-in and the SecureLogin Administrative Management utility is installed when you select the *Install Directory Administration Tools* during the Novell SecureLogin installation.

Figure 3-1 *Installing Directory Administration Tools*



When you select the *Install Directory Administration Tools* option during the Novell SecureLogin installation:

- It installs an Administration tab in the Active Directory Microsoft Management Console (MMC). This allows you access the Administrative Management utility functionality in the Users and Computers snap-in.
- It also provides a snap-in to Active Directory Users and Computers snap-in for configuration in the Microsoft Active Directory environment.

NOTE: If you select the *Enable Microsoft Active Directory Group Policies* option during the installation, you can administer Novell SecureLogin by using the Group Policy object.

3.3 Add Application Wizard

The Add Application Wizard help the users to create and change the application definition responses for the following:

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

The Add Application Wizard launches automatically in response to Windows Login and Password dialog boxes if there is no existing application definition. If an application definition exists, the Add Application Wizard does not start automatically in response to the Login and Password dialog boxes.

For previously created application definitions, the Add Application Wizard can be invoked manually, and after the Change Password dialog box appears, the password data can be captured.

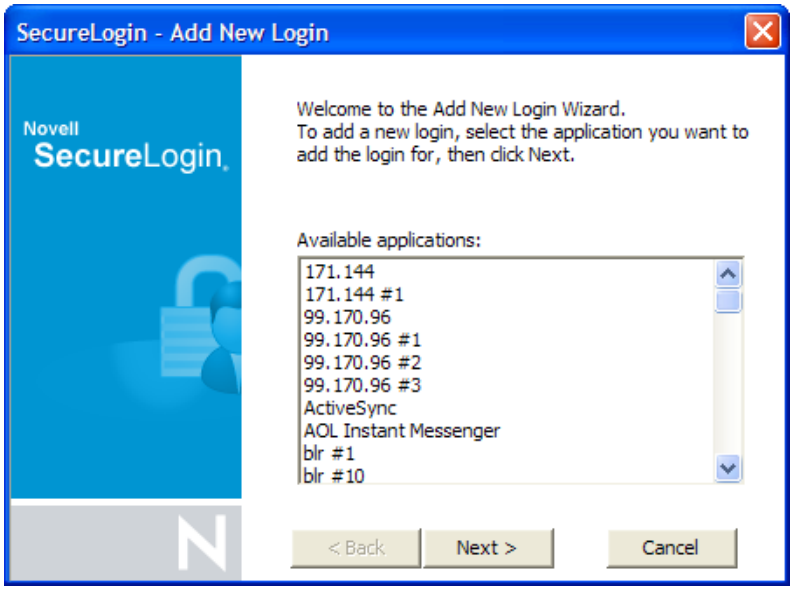
Figure 3-2 *Add Application Wizard*

3.4 Add New Login Wizard

The Add New Login Wizard helps the users to create multiple logins for the same application or server. The Wizard contains a list of available applications from which users can choose the required login.

The users can use the `PickListAdd` and `PickListDisplay` commands to add login options for multiple users. For example, if all users in an IT group require three different log ins for a help desk application, the administrator can add a pick list to the help desk application definition, so all users inherit the list without individually adding the new log ins.

Figure 3-3 *Add New Login Wizard*

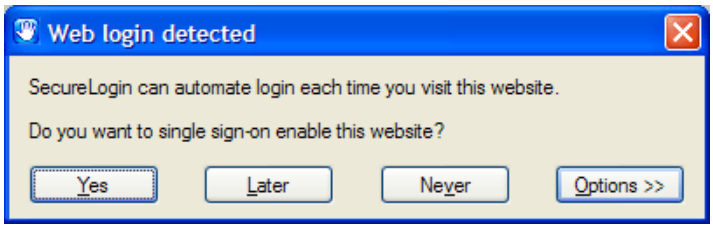


3.5 The Web Wizard

The Web Wizard is used to enable single sign-on for Web sites and capture virtually any Web-based login. The Web Wizard starts when users access a Web page through the browser. The Wizard captures the login information, error messages, and change password requests.

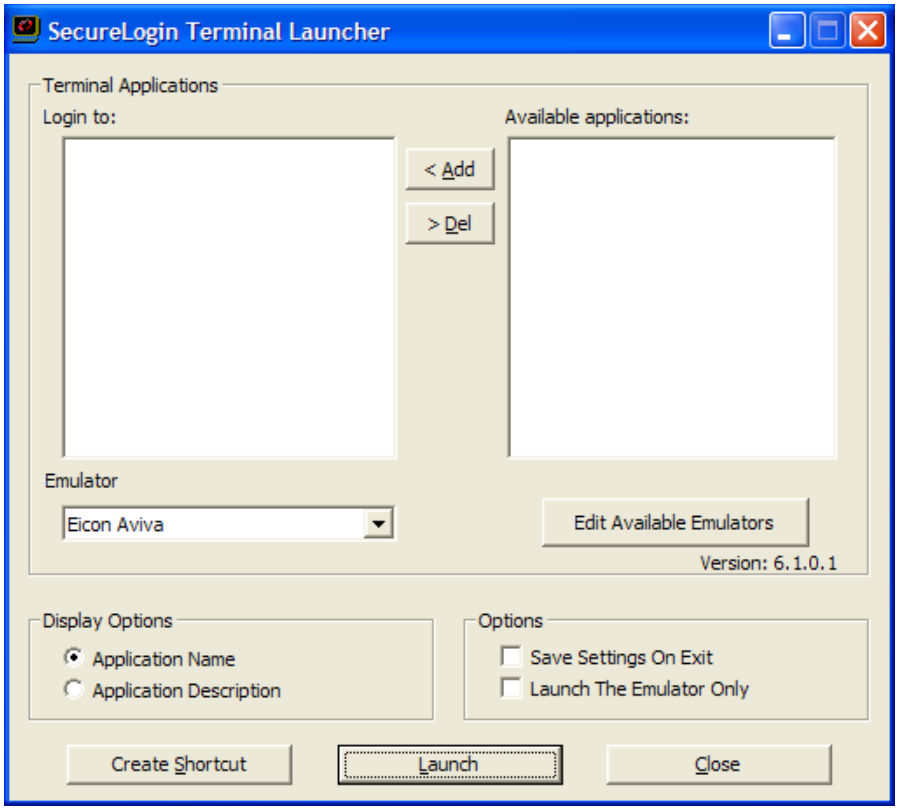
It captures login information, error messages, and change password requests. For more information, see Chapter 5, “Enabling Applications and Web Sites for Single Sign-On,” on page 63.

Figure 3-4 *Web Wizard*



3.6 Terminal Launcher

Figure 3-5 *The Terminal Launcher*



Terminal applications require a terminal launcher to execute. After an application definition is created, the users must configure it to start the terminal launcher. With this, a shortcut is created to enable the user to run the terminal launcher and the terminal emulator from the desktop with automated single sign-on to the application or the server.

The Novell SecureLogin Interface

4

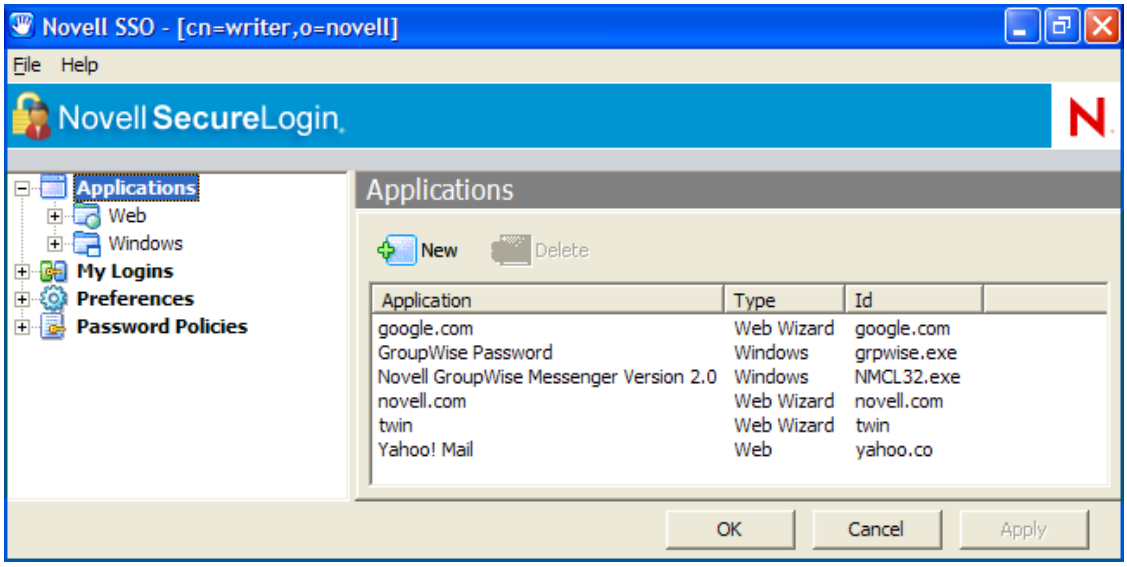
This section consists of the following sections:

4.1 Personal Management Utility

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

When a folder in the navigation tree is selected, the related information is displayed in the right pane. To display the objects associated with the folders in the navigation tree, click the plus (+) symbol next to the icon to expand its contents. Not all icons are expandable.

Figure 4-1 *The Personal Management Utility*



The navigation tree in the left pane contains the following:

- *Applications*
- *My Logins*
- *Preferences*
- *Password Policies*

Changes made by using the Personal Management utility on the local workstation apply only to the currently logged-in user's single sign-on and they override the settings made in the directory. For example, if the *Allow users to view Application Definitions* preference is set to *No* at the organizational unit (OU) level where the object resides in, and set to *Yes* on the actual user object in the directory, the user object setting applies. The user can view the application definitions. Other users in the container cannot view the application definitions unless they have the option set through the user object.

The Personal Management utility is used for:

- Providing the users with the capability to configure the Novell® SecureLogin environment and view their credentials.
- Testing the Novell SecureLogin configuration before mass deployment.
- Creating and modifying the application definitions for testing.
- The standalone mode.
- Troubleshooting.

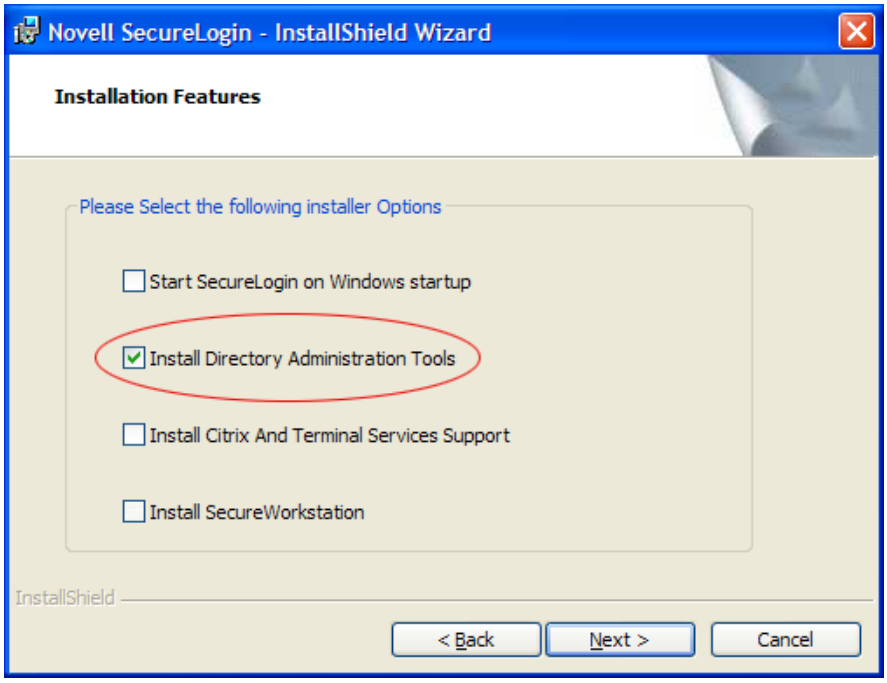
For more information see, the *Novell SecureLogin 6.1 SP1 Administration Guide*.

4.2 The Administrative Management Utilities

Through the Administrative Management utilities you can set up and administer the Novell SecureLogin for a user.

IMPORTANT: The *Install Directory administration tools* option must be selected during the Novell SecureLogin installation.

Figure 4-2 *Directory Administration Tools*



Novell SecureLogin can be administered either through Novell or the SecureLogin Manager.

- Section 4.2.1, “Accessing iManager,” on page 21
- Section 4.2.2, “Accessing the SecureLogin Manager,” on page 23

4.2.1 Accessing iManager

1 In a supported Web browser, type the following in the Address (URL) field:

`http://server_IP_address/nps/iManager.html`

For example:
`http://127.0.0.1/nps/iManager.html`

You might be redirected to an HTTPS secure page

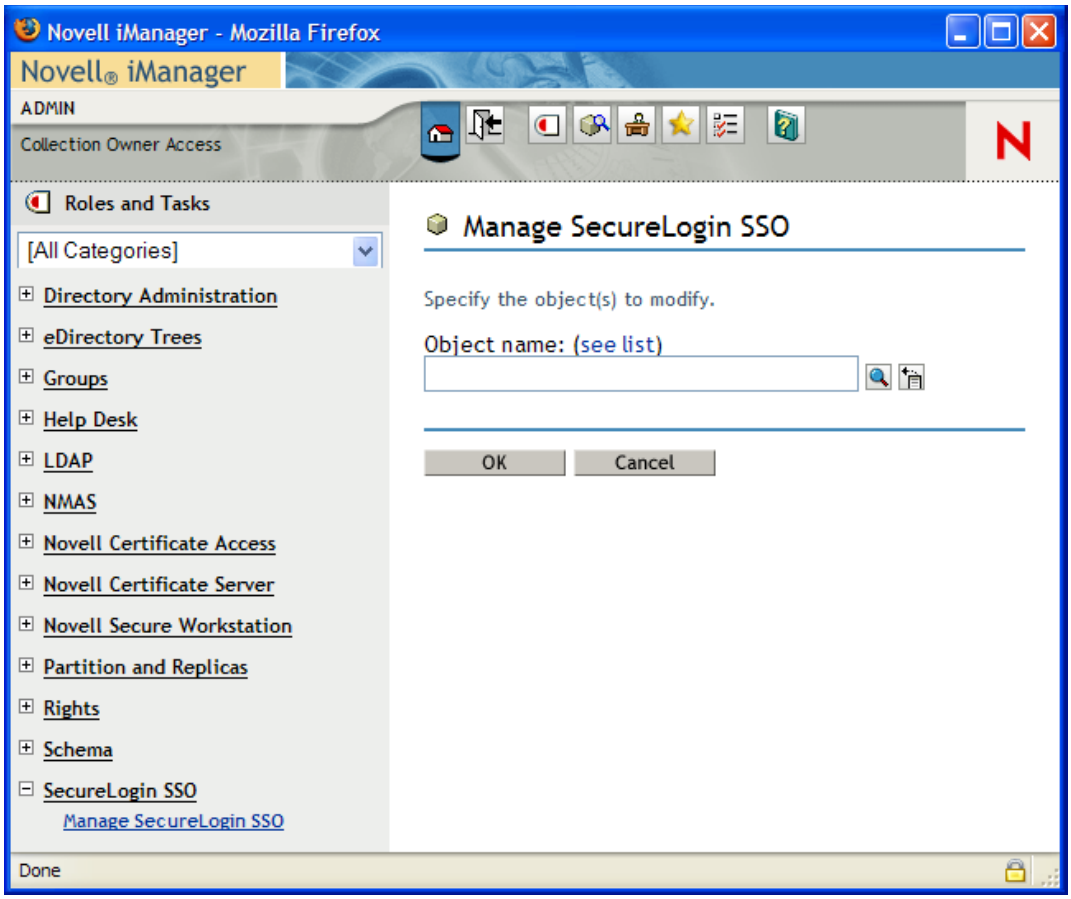
IMPORTANT: The URL is case sensitive.

---

2 Log in using your username, password, and eDirectory tree name.

You can substitute the IP address of an eDirectory server for the tree name.

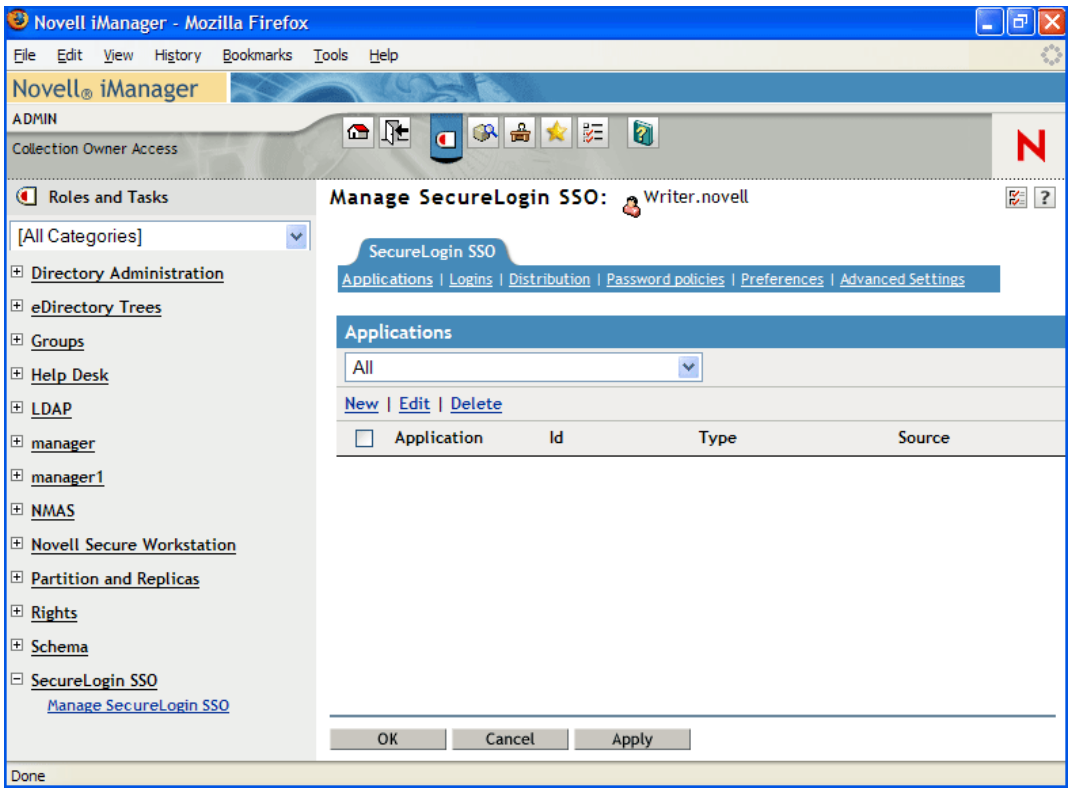
To have full access to all Novell iManager features, you must log in as a user with administrator-equivalent rights to the tree.



For details on accessing iManager, go to the Novell Documentation Web site for iManager 2.6 (http://www.novell.com/documentation/imanager26/index.html)

For accessing and using SecureLogin Manager refer, Section 4.2.2, “Accessing the SecureLogin Manager,” on page 23.

3 Click *OK*. The SecureLogin SSO page with the single sign-on options is displayed.



The navigation tree in the top consists of the following options:

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

NOTE: The same options are available in SecureLogin Manager too.

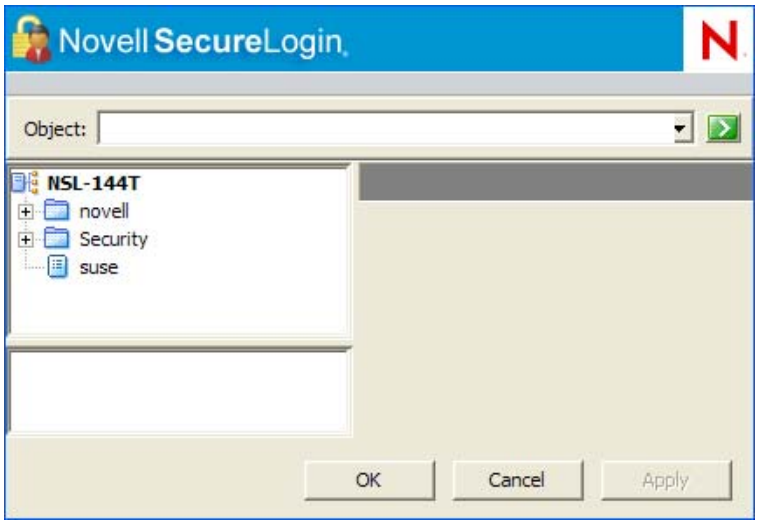
4.2.2 Accessing the SecureLogin Manager

Novell SecureLogin now incorporates an LDAP-compliant browser.

To launch the SecureLogin Manager:

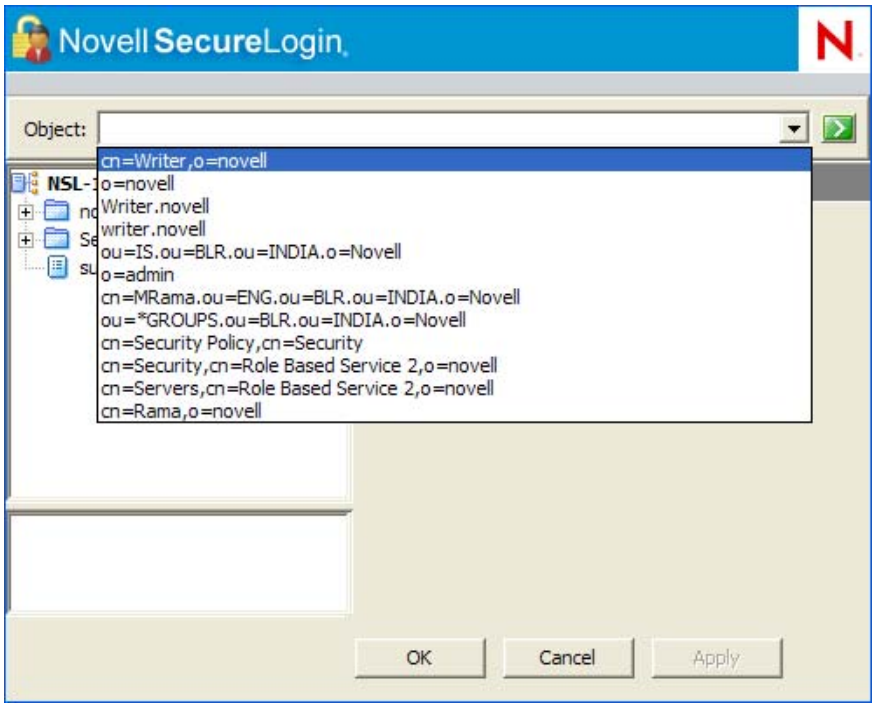
1 Click *Start* > *Programs* > *Novell SecureLogin* > *SecureLogin Manager*.

The SecureLogin Manager is displayed.



2 From the *Object* drop-down list, select the object or specify the full distinguished name (DN) of the user object, container, or the organizational unit for administration.

Alternatively, use the  icon to navigate to the appropriate object.



3 Press Enter to submit the entry specified in the object field.

Clicking *OK* closes the dialog box and cancels the specified entry.

The navigation tree in the left pane consists of the following options:

- *Applications*
- *Logins*
- *Preferences*

- *Password Policies*
- *Advanced Settings*
- *Distribution*

NOTE: The same options are available in iManager too.

The SecureLogin manager interface consists of a title bar, menu bar, context bar, panes, and the properties table.

You can access various options in the SecureLogin Manager through the menu bar and shortcut menus.

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

NOTE: Not all icons are expandable.

- "The Menu Bar" on page 25
- "Shortcut Menus" on page 25

The Menu Bar

The menu bar appears below the title bar in iManager, the SecureLogin Manager, and the Personal Management utility. It is used to select menus and commands to perform actions in the software.

Table 4-1 *Menu Options*

Menu	Command	Function
File	*New Application*	Displays the *New Application* dialog box.
	New Login	Displays the *Create Login* dialog box.
	New Password Policy	Displays the *New Password Policy* dialog box.
Help	*Help*	Provides access to the online help information.

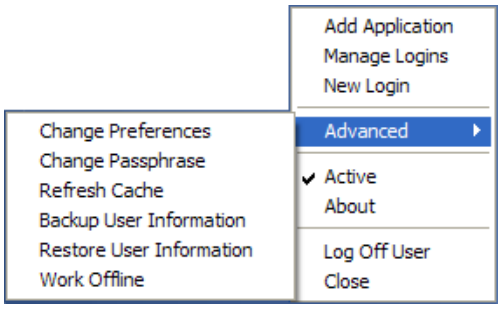
Shortcut Menus

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

- "Shortcut Menu for the Novell SecureLogin Icon" on page 26
- "Shortcut Menu for the Applications Pane" on page 26
- "Shortcut Menu for the Logins Pane" on page 26
- "Shortcut Menu for the Password Policies Pane" on page 26

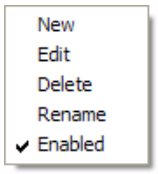
Shortcut Menu for the Novell SecureLogin Icon

Figure 4-3 *Shortcut Menu for the Novell SecureLogin Icon*



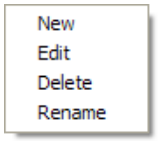
Shortcut Menu for the Applications Pane

Figure 4-4 *Shortcut Menu for the Applications Pane*



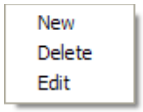
Shortcut Menu for the Logins Pane

Figure 4-5 *Shortcut Menu for the Logins Pane*



Shortcut Menu for the Password Policies Pane

Figure 4-6 *Shortcut Menu for the Password Policies Pane*



4.3 The Novell SecureLogin Icon

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

Table 4-2 *Novell SecureLogin Icon Status*

If	Then
Novell SecureLogin is active.	The Novell SecureLogin icon appears on the notification area as .

If	Then
Novell SecureLogin is inactive.	The Novell SecureLogin icon appears on the notification area as  . **NOTE:** In this case, the Novell SecureLogin does not perform single sign-on functions such as decrypting and passing credentials to applications.

Following are the options that are available by right-clicking the Novell SecureLogin icon on the notification area.

Table 4-3 *Novell SecureLogin Icon Menu Options*

Option	Function
Add Applications	Launches the Add Application Wizard.
Manage Logins	Launches the Personal Management utility.
New Login	Launches the Add New Login Wizard.
Advanced	Has some advanced Novell SecureLogin management options. See Table 4-4 on page 27.
Active	Displays a check (✓) mark when Novell SecureLogin is active on the workstation.
About	Displays information about Novell SecureLogin and your system.
Log Off User	Allows you to shut down all programs, including Novell SecureLogin, and log out the user from the workstation.
Close	Closes Novell SecureLogin on the workstation.

Following are the options available on the *Advanced* menu:

Table 4-4 *Novell SecureLogin Advanced Menu Options*

Option	Function
Change Preferences	Launches the Personal Management utility with the *Preferences* properties table displayed.
Change Passphrase	Displays the *Passphrase* dialog box. It enables users to change their passphrase answer.
Refresh Cache	Manually executes the synchronization of data between the local cache and directory data.
Backup User Information	Enables local workstation settings. This includes credentials that can be saved as an XML file.
Restore User Information	Enables the XML file that is backed up to be restored in the local workstation single sign-on cache.

Option	Function
Work Offline / *Work Online*	Toggles between offline and online network access. Displays whether the user is connected to the network or not. **NOTE:** This is not displayed in standalone mode. It is necessary to manually select this option because this is automated in Novell SecureLogin.

4.4 Application Types and Descriptions

The following table describes the application type icons as available in SecureLogin Manager:

Table 4-5 *Application Types and Description*

Icon	Application Type	Description
	Generic	The name of the application executable.
	Java	• The Web page URL containing the JavaScript* login, for example, `http:/javaboutique.internet.com/KiserPassword`. • Class name of the application (if it is a stand-alone Java* application).
	Startup	This is the application that the user decides to run after the Novell SecureLogin starts. Unlike any other application types, any name of the application is permitted. This must be configured in the application definition editor. For more information, see the *Novell SecureLogin 6.1 SP1 Application Definition Guide*.
	Terminal Emulator	The name of the emulator. For example, `PLAY3270.A3D`.
	Web	All or part of the URL of the Web page or an 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 Novell SecureLogin application definition on any page on the Novell Web site. Alternatively, `www.novell.com/` activates the application definition solely on the specified Web page.
	Windows	The name of the application executable, for example, `notepad.exe`.

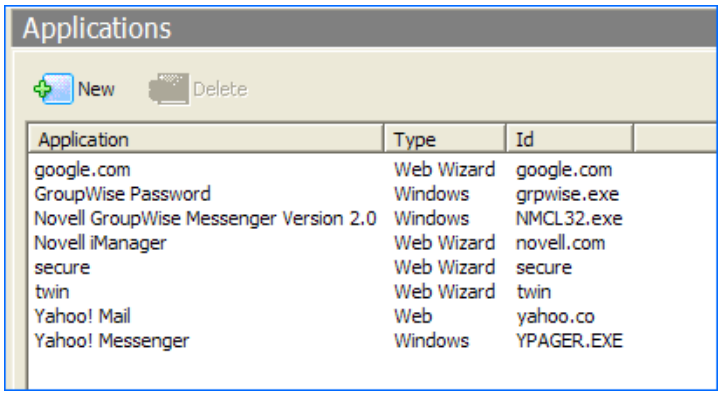
The following table describes the application details icons as available in SecureLogin Manager:

Table 4-6 *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 the one that is inherited from a higher-level object, for example, an organizational unit.
	An application icon without the red triangle in the lower corner is an application definition or a predefined application that is not inherited from a higher-level object.

4.5 The Applications Pane

Figure 4-7 *The Applications Pane in SecureLogin Manager*



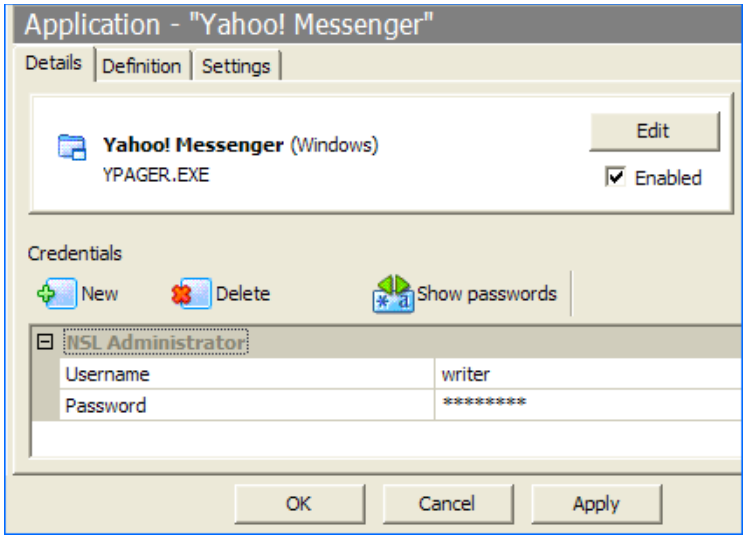
From the applications pane, users can create and modify the Novell SecureLogin application definitions that enable the single sign-on. For details, see the *Novell SecureLogin 6.1 SP1 Application Definition Guide*.

To display a specific application, double-click an application in the navigation tree or in the Application pane. The Application pane for that specific application is displayed. It contains three tabs:

- Section 4.5.1, “The Details Tab,” on page 30
- Section 4.5.2, “The Definition Tab,” on page 31
- Section 4.5.3, “The Settings Tab,” on page 31

4.5.1 The Details Tab

Figure 4-8 *The Details Tab in SecureLogin Manager*

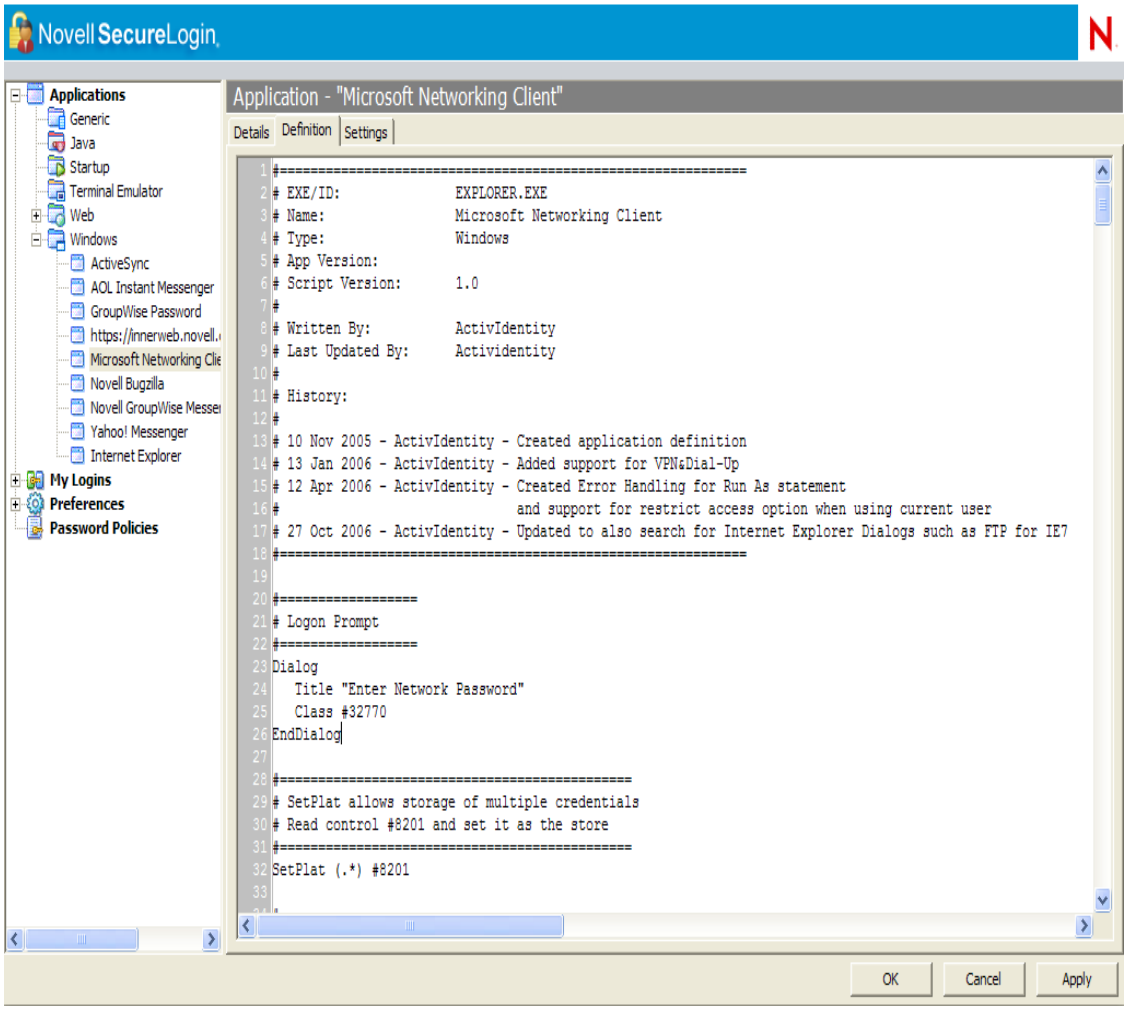


The *Details* tab contains:

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

4.5.2 The Definition Tab

Figure 4-9 *The Definition Tab in SecureLogin Manager*



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

NOTE: Predefined Web applications such as eBay* and Hotmail* under the *Type* option are titled *Web* and not *Advanced Web*. There is no difference between a Web application definition and an Advanced Web application definition.

4.5.3 The Settings Tab

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

Figure 4-10 *The Settings Tab for Terminal Emulator, Windows, Startup, Java, and Generic Applications*

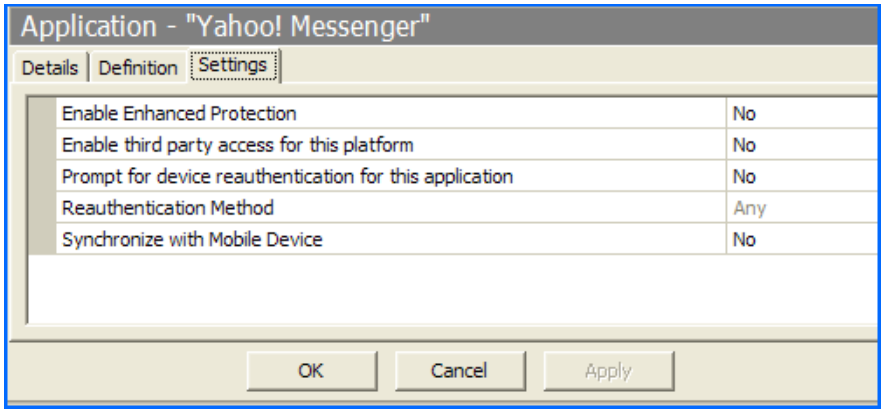
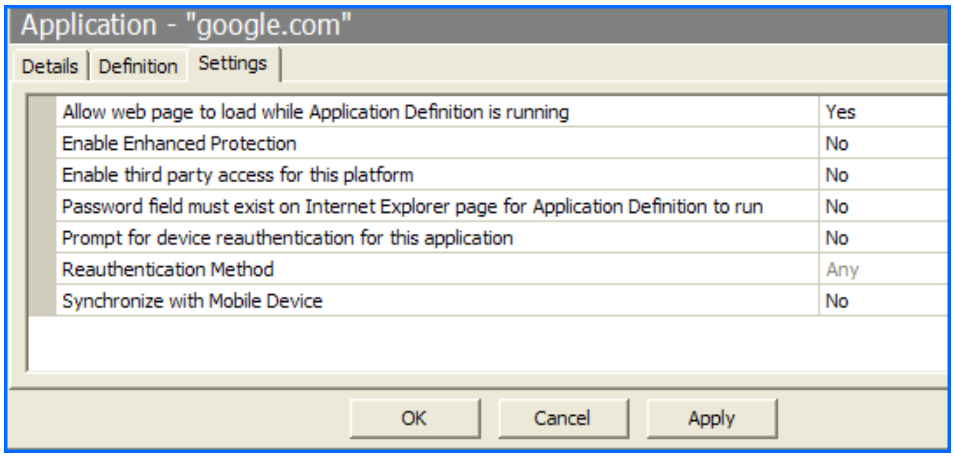


Figure 4-11 *The Settings Tab for Windows Applications*



The following table describes the settings for Terminal Emulator, Windows, Startup, Java, and Generic Applications:

Table 4-7 *Settings for the Windows Applications*

Item	Description
Enable third party access for this platform	This disables the API access for the predefined application or the application definition. The default setting is *No*.
Prompt for device reauthentication for this application	If *Yes* is selected, users are prompted for device reauthentication for the application.
Reauthentication Method	Allows the user to reauthenticate an application against an AA device where Novell SecureLogin is used in conjunction with SLAA or the NMAS infrastructure.

Item	Description
Synchronize with Mobile Device	This enables the synchronization with the API-enabled handheld device, for the predefined application or the application definition. The default setting is *No*.

The following table describes the settings for Web applications:

Table 4-8 *Settings for Web Applications*

Item	Description
Allow web page to load while Application Definition is running (Web applications only)	This applies to Microsoft* Internet Explorer and the application definitions created for Web pages and JavaScript logins that are executed in a Web page. By default, this option is set to *No*. This suspends the completion of any other Internet Explorer tasks until the login is completed. If this option is set to *Yes*, then the Internet Explorer continues to function while Novell SecureLogin is executing the login.
Enable third party access for this platform	This option disables the API access for the predefined application or application definition. The default setting is *No*.
Password field must exist on Internet Explorer page for Application Definition to run (Web applications only)	This applies to the Microsoft Internet Explorer and application definitions created for the Web pages and JavaScripts within the Web pages. If *Yes* is selected, it ensures that Novell SecureLogin does not execute the automated login on pages without the password field. If *No* is selected, the Web application returns errors on pages without the password fields that you need to handle with Novell SecureLogin. For example, the *Change Successful* message.
Prompt for device reauthentication for this application.	This allows you to reauthenticate an application against an Advanced Authentication (AA) device. The default setting is *No*. If *Yes* is selected, users are prompted for device reauthentication for the application.

Item	Description
Reauthentication Method	This allows users to reauthenticate an application against an SLAA device where the Novell SecureLogin is used in conjunction with the SLAA or the NMAS™ infrastructure. This option is available only when *Prompt for device reauthentication for this application* is set to *Yes*. The available options are: ◆ *Any* ◆ *Biometric* ◆ *Smart card* ◆ *Token* ◆ *Password* ◆ *Passphrase* ◆ *Directory password*
Synchronize with Mobile Device	This enables the synchronization with the API-enabled handheld device for the predefined application or the application definition. The default setting is *No*.

4.6 The Logins Pane

The *My Logins* pane in the Personal Management utility manages the logins that applications require to log in, along with their associated credentials, including:

- Username
- User ID
- Login ID
- Password
- PINs
- Domain
- Database names
- Server IP address

Through the Logins pane, the user can:

- Link the logins manually, including the host IP addresses to the applications.
- Configure the credential sets at the Group policy, organizational unit, container, and the user object level.
- Enable the group of users to be configured with seamless login access to an application with one account or by logging in with the username and password.

4.7 The Preferences Properties Table

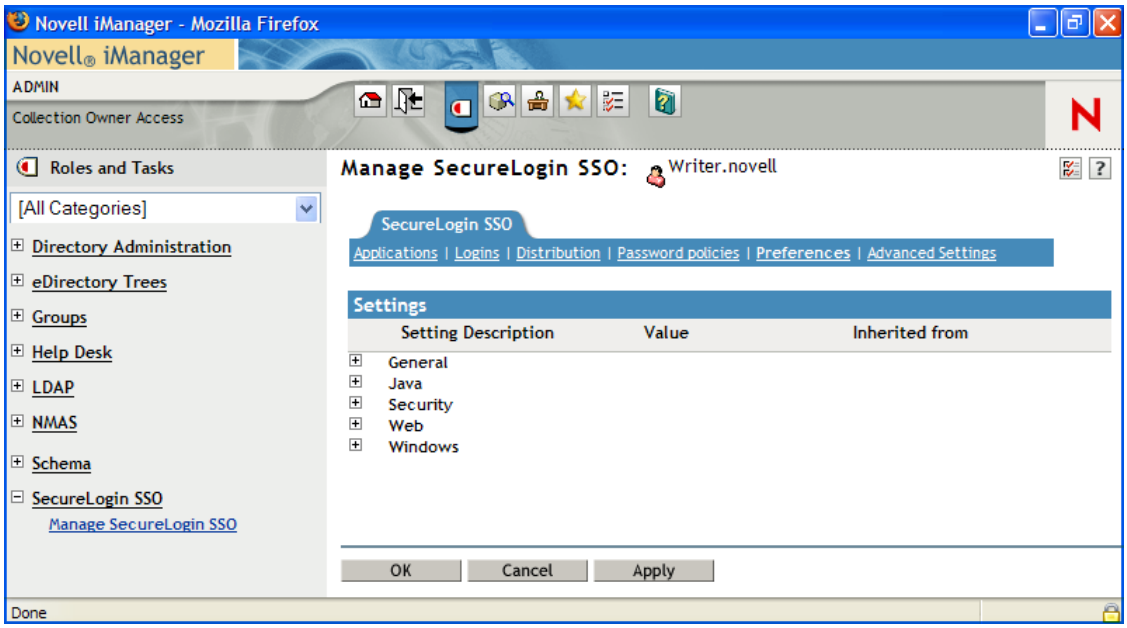
The *Preferences* properties table provides tools to configure the parameters of the user's Novell SecureLogin environment, including applications permitted to be enabled for single sign-on and access to the Novell SecureLogin management and administration tools.

The following table provides the options for the Personal Management utility, the SecureLogin Manager, and iManager. If the option is available only in one of the management utilities, this is mentioned in the Description column in the following Preferences tables.

The *Preferences* are displayed on the right pane when *Preferences* is clicked in the Management utility.

Click the plus (+) symbol next to the names of the preferences to expand the preference options.

Figure 4-12 *The Preferences*



In previous versions of Novell SecureLogin, the application definition preference was a single preference called *Allow users to view and modify application definitions*. This is now split into two preferences:

- *Allow application definition to be modified by users*
- *Allow application definition to be viewed by users*

When you upgrade from a previous version of Novell SecureLogin to Novell SecureLogin 6.1, if you are using the legacy directory data (that is, data from Novell SecureLogin 6.0 or 3.5) and if the *Allow users to view and modify application definition to be modified by users* option was set to *No*, then the new *Allow application definition to be modified by users* for Novell SecureLogin 6.1 is disabled and dimmed.

Administrators must reset the *Allow application definition to be viewed by users* option to *Yes* before users can modify the application definitions.

The Preferences has the following categories:

- Table 4-9, “The General Preferences Properties Table,” on page 37
- Table 4-10, “The Java Preferences Properties Table,” on page 45
- Table 4-11, “The Security Preferences Properties Table,” on page 46
- Table 4-12, “The Web Preferences Properties Table,” on page 49
- Table 4-13, “The Windows Preferences Properties Table,” on page 50

User or the administrators can change the value of the Preferences in the Administrative Management utility or the Personal Management utility unless otherwise specified.

The administrators can restrict the user’s access to this table through the centrally controlled administrative preferences.

NOTE: The *Security* option is not available in the Personal Management utility.

Figure 4-13 *The General Preferences*

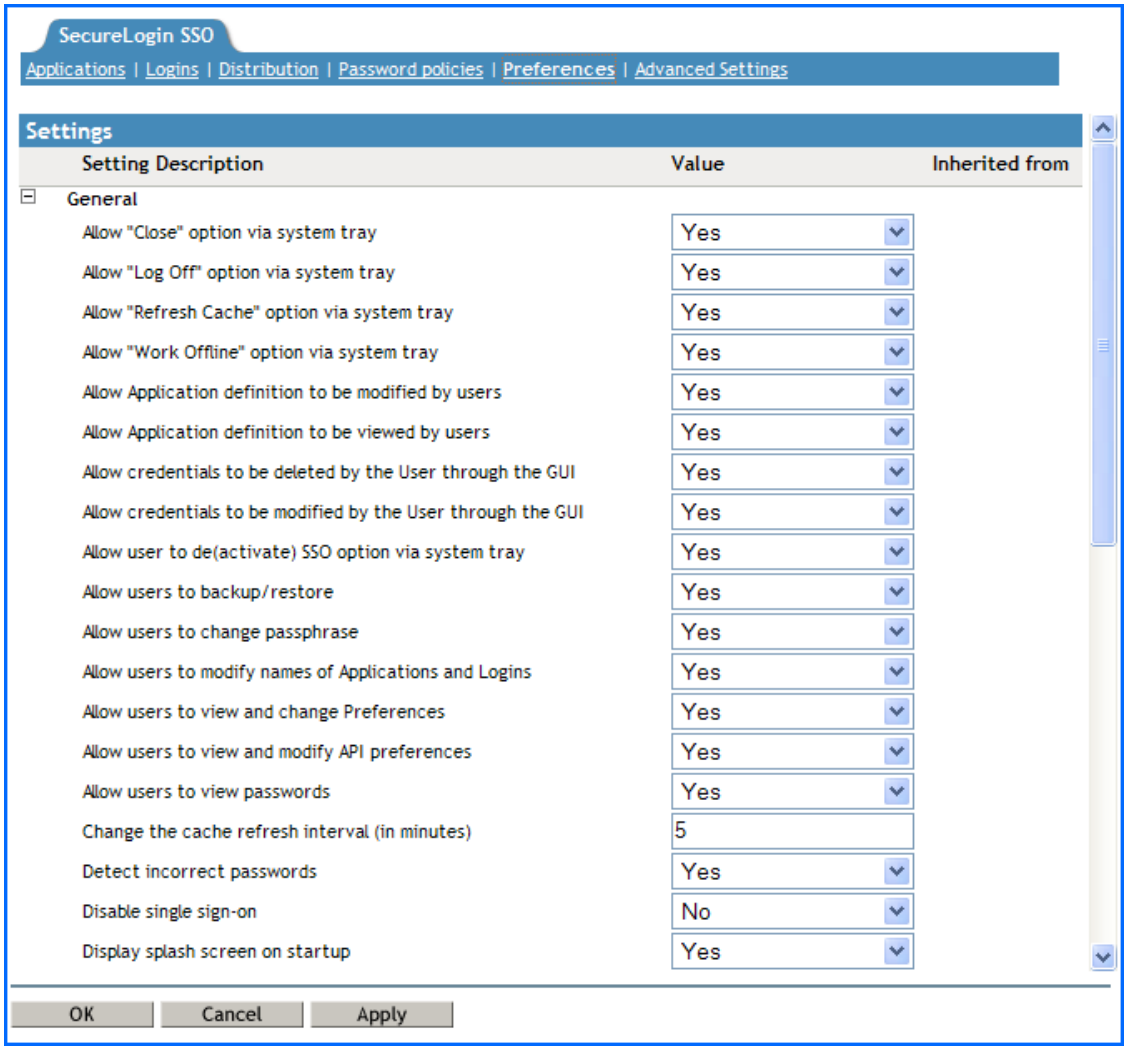


Table 4-9 *The General Preferences Properties Table*

Preference	Value	Description
Allow "Close" option via system tray	*Yes*/*No*/*Default*	If the option is set to *No*, the *Close* option is not displayed and accessible in the Novell SecureLogin notification area icon. If this option is set to *Yes* or *Default*, the *Close* option is displayed and accessible in the Novell SecureLogin notification area icon. The default value is *Yes*. This preference is a available only through the administrative management utilities.
Allow "Log Off" option via system tray	*Yes*/*No*/*Default*	If this option is set to *Yes* the *Log Off User* option is displayed and accessible in the Novell SecureLogin notification area icon. If this option is set to *No* or *Default*, the *Log Off User* option is not displayed in the Novell SecureLogin notification icon. The default value is *No*. This preference is available only through the administrative management utilities.
Allow "Refresh Cache" option via system tray	*Yes*/*No*/*Default*	If this option is set to *Yes*, the *Refresh Cache* option is not displayed and accessible in the notification area icon. If this option is set to *No* or *Default*, the *Refresh Cache* option is displayed in the notification area icon. The default value is *No*. This preference is available only through the administrative management utilities.
Allow "Work Offline" option via system tray	*Yes*/*No*/*Default*	If this option is set to *No* or *Default*, the *Work Offline* option is displayed in the notification area icon. If this option is set to *Yes*, the *Work Offline* options is not displayed in the notification area icon. The default value is *No*. This preference is available only through the administrative management utilities.

Preference	Value	Description
Allow application definition to be modified by users	*Yes*/*No*/*Default*	If this option is set to *Yes* or *Default*, end user can view and modify their application definitions. If this option is set to *No*, the end user cannot change their application definitions. The default option is *Yes*. **NOTE:** Disabling this preference does not disable the users from creating new applications through the wizards. This preference is available only through the administrative management utilities.
Allow application definition to be viewed by users	*Yes*/*No*/*Default*	If this option is set to *Yes* or *Default*, users can view the application definition. If this option is set to *No*, users cannot view the application definition. The default value is *Yes*. This preference is available only through the administrative management utilities.
Allow credentials to be deleted by users through the GUI	*Yes*/*No*/*Default*	If this option is set to *Yes* or *Default*, users can delete their credentials through the GUI. If this option is set to *No*, users cannot delete their credentials. The default value is *Yes*. This preference is available only through the administrative management utilities.
Allow credentials to be modified by users through the GUI	*Yes*/*No*/*Default*	If this option is set to *Yes* or *Default*, users can modify their credentials through the GUI. If this option is set to *No*, users cannot modify their credentials through the GUI. The default value is *Yes*. This preference is available only through the administrative management utilities.
Allow users to (de) activate SSO via system tray	*Yes*/*No*/*Default*	If this option is set to *Yes* or *Default*, users can switch between active and inactive modes of Novell SecureLogin. If this option is set to *No*, Novell SecureLogin is always active. User do not have the option to switch. The default value is *Yes*. This preference is available only through the administrative management utilities.

Preference	Value	Description
Allow users to backup/ restore	*Yes*/*No*/*Default*	If this option is set to *Yes* or *Default*, users can back up and restore their single sign-on information. If this option is set to *No*, users cannot back up and restore their single sign-on configuration. The default value is *Yes*. This preference is available only through the administrative management utilities.
Allow users to change passphrase	*Yes*/*No*/*Default*	If this option is set to *Yes* or *Default*, users can change their passphrase through the notification area icon. If this option is set to *No,* the *Change Passphrase* option is not displayed and users cannot change their passphrase through the notification area icon. The default value is *Yes*. This preference is available only through the administrative management utilities.
Allow users to modify names of Applications and Logins	*Yes*/*No*/*Default*	If this option is set to *Default*, Novell SecureLogin behaves as if it is set to *Yes*. The default value is *Yes*. This preference is available only through the administrative management utilities.
Allow users to view and change Preferences	*Yes*/*No*/*Default*	If this option is set to *Yes* or *Default*, users can view and change their preferences. If this option is set to *No*, users cannot view and change their preferences. The default value is *Yes*. **NOTE:** We recommend that you create a separate ou to ensure that they are not adversely affected by the general user configuration preferences at the ou level. This preference is available only through the administrative management utilities.

Preference	Value	Description
Allow users to view and modify API preferences	*Yes*/*No*/*Default*	The API preference defines the following options for users to: ◆ Enter an API licence key(s). ◆ Provide API access. If this option is set to *Yes* or *Default* users can view and modify the API preference. If this option is set to *No*, users cannot view and modify the API preference. The default value is *Yes*. This preference is available only through the administrative management utilities.
Allow users to view passwords	*Yes*/*Yes, per applications*/*No*/*Default*	if this option is set to *Yes* or *Default*, users can view their passwords. If this option is set to *No*, users cannot view their passwords. If this option is set to *Yes, per application*, users can view their passwords for only specific applications. The default value is *Yes*. **NOTE:** Allowing users to view their passwords gives them an opportunity to view and record passwords if they need to reset the Novell SecureLogin configuration. This preference is available only through the administrative management utilities.
Change the cache refresh interval (in minutes)	*5*	This preference defines the time in minutes of the synchronization of the user data and directory on the local workstation. The default value is set to *5* minutes. However, depending on the network traffic and the number of users the interval can be set between 240 minutes and 480 minutes (four and eight hours). This preference is available in both the Personal Management utility and the administrative management utilities.
Container has priority over User	*Yes*/*No*/*Default*	If this option is set to *Yes*, the container settings has priority over user settings. If this option is set to *No* or *Default*, the container settings does not have priority over the user settings. The default value is *No*. This preference is available only through the administrative management utilities.

Preference	Value	Description
Detect incorrect passwords	*Yes*/*No*/*Default*	If this option is set to *Yes* or *Default*, incorrect passwords for Web applications are detected. If this option is set to *No*, incorrect passwords for Web applications are not detected. The default value is *Yes*. This preference is available in both the Personal Management utility and the administrative management utilities.
Disable single sign-on	*Yes*/*No*/*Default*	If this option is set to *Yes*, access to Novell SecureLogin is disabled. If this option is set to *No* or *Default*, access to Novell SecureLogin is enabled. The default value is *No*. This preference is available only through the administrative management utilities.
Display splash screen on startup	*Yes*/*No*/*Default*	If this option is set to *Yes* or *Default*, the splash screen appears when Novell SecureLogin startsup. If this option is set to *No*, the splash screen is hidden and users cannot see the splash screen when Novell SecureLogin startsup. The default value is *Yes*. This preference is available only through the administrative management utilities.
Display the system tray icon	*Yes*/*No*/*Default*	If this option is set to *Yes* or *Default*, the Novell SecureLogin icon appears on the notification area. If this option is set to *No*, the Novell SecureLogin icon does not appear on the notification area. The default value is *Yes*. **NOTE:** When the Novell SecureLogin is active, users can double-click the icon on the notification area to launch the Personal Management utility. When the Novell SecureLogin is inactive, user can start the Personal Management utility through *Start* > *Programs* > *Novell SecureLogin* > *Novell SecureLogin* This preference is available only through the administrative management utilities.

Preference	Value	Description
Enable cache file	*Yes*/*No*/*Default*	This options defines the enabling or disabling of the creation of a Novell SecureLogin cache file on the local workstation. The cache stores user configuration data: local and inherited. Set this option to *Yes* for mobile users. If this option is set to *No*, you cannot store files locally or you are have some conflicts with organizational security policy If this option is set to *Default*, Novell SecureLogin behaves as if it is set to *Yes*. The default value is *Yes*. This preference is available in both the Personal Management utility and the administrative management utilities.
Enable Logging to Novell Audit	*Yes*/*No*/*Default*	This preference defines the enabling or disabling of log events to be automatically sent to Novell Audit tool, NSure. The following ou or user objects are logged by NSure: ◆ Single sign-on client started ◆ Single sign-on client exited ◆ Single sign-on client activated by user ◆ Single sign-on client deactivated by user ◆ Password provided to an application by a script ◆ Password changed by the user in response to a change password command ◆ Password changed automatically in response to a change password command **NOTE:** The Novell Audit platform must be installed on the client with a registered application ID and schema file on the server. If this option is set to *Yes* or *Default*, logging to Novell Audit is enabled. If this option is set to *No*, logging to Novell Audit is disabled. The default value is *Yes*. This preference is available only through the administrative management utilities.

Preference	Value	Description
Enable the New Login Wizard on the system tray icon	*Yes*/*No*/*Default*	This preference defines the enabling or disabling the user's ability to create multiple logins for different accounts on the same application or server. If this option is set to *Yes* or *Default*, users can create multiple logins. If this option is set to *No,* users cannot create multiple logins. The default value is *Yes*. This preference is available only through the administrative management utilities.
Enforce passphrase use	*Yes*/*No*/*Default*	Enforces the user definition of a passphrase question and answer when Novell SecureLogin is launched. If this option is set to *Yes*, users must complete setting up their passphrase before they proceed with any other activity on the workstation. If this option is set to *No* or *Default*, users can postpone setting up the passphrase. The default value is *No*. This preference is available only through the administrative management utilities.
Enter API license key(s)	Specify API licence key(s)	Specify the API license key(s) provided by Novell SecureLogin to activate the API functionality for an application. **NOTE:** You can add more than one API license keys.
Password protect the system tray icon	*Yes*/*No*/*Default*	Restricts the users from accessing the Novell SecureLogin icon menu option (from the notification area) without their network login password. If this option is set to *Yes*, the Novell SecureLogin icon on the notification area is password protected. If this option is set to *No* or *Default*, the Novell SecureLogin icon on the notification area is not password protected. The default value is *No*. This preference is available in both the Personal Management utility and the administrative management utilities.

Preference	Value	Description
Provide API Access	*Yes*/*No*/*Default*	Enables or disables the API functionality. If this option is set to *Yes*, the APII access is enabled. If this option is set to *No* or *Default*, the API access is disabled. The default value is *No*. This preference is available in both the Personal Management utility and the administrative management utilities.
Standalone distributed settings have priority over user's	*Yes*/*No*/*Default*	Allows or disallows the values of configuration settings made by user to take precedence over the configuration settings made after settings distribution. Use this preference in advanced standalone mode for overwriting locally applied scripts, settings, and credentials by centrally created credentials. Use this preference also for suers who receive the encrypted and signed settings. If this option is set to *Yes*, the standalone distributed settings have priority over user's settings. If this option is set to *No* or *Default*, the standalone distributed settings do not have priority over user's settings. The default value is *No*. This preference is available only in SecureLogin Manager.
Stop walking here	*Yes*/*No*/*Default*	Enables or disables the inheritance of settings from higher level containers or organizational units. If this option is set to *Yes*, the inheritance of settings from higher level containers or organizational units is disabled. Set the option to *Yes* during phased upgrades when higher levels might have a different version of Novell SecureLogin implemented. If this option is set to *No* or *Default*, the inheritance of settings from higher level containers or organizational units is enabled. The default value is *No*. This preference is available only through the administrative management utilities.

Figure 4-14 *The Java Preferences*

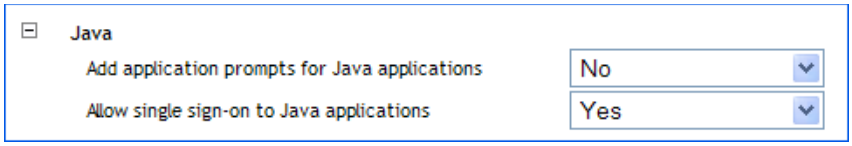


Table 4-10 *The Java Preferences Properties Table*

Preference	Value	Description
Add application prompts for Java applications	*Yes*/*No*/*Default*	If the preference is set to *Yes* or *Default*, as soon as Novell SecureLogin detects a Java application login page, it prompts the user to record it. If this option is set to *No*, this process never occurs, only Java predefined applications are prompted and supported The default value is *Yes*. This preference is available in both the Personal Management utility and the administrative management utilities.
Allow single sign-on to Java applications	*Yes*/*No*/*Default*	If the preference is set to *Yes* or *Default*, as soon as Novell SecureLogin detects a Java application login page, it prompts the user to enable it for single sign-on. If this option is set to *No*, Java applications are not enabled for single sign-on. The default value is *Yes*. This preference is available in both the Personal Management utility and the administrative management utilities.

Figure 4-15 *The Security Preferences*

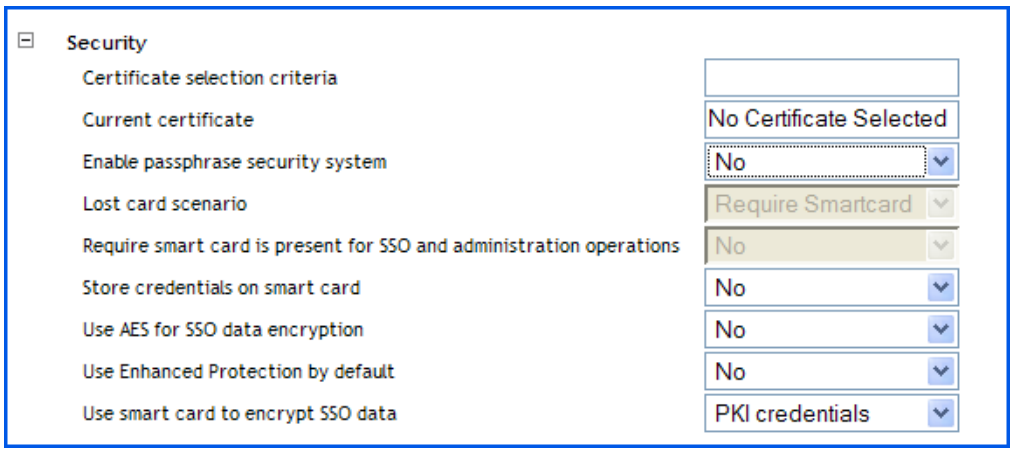


Table 4-11 *The Security Preferences Properties Table*

Preference	Value	Description
Certificate selection criteria	Specify text to identify your certificate	Allows you to specify a text to uniquely identify a certificate (within searchable field only). This preference is available only through the administrative management utilities.
Current certificate	No certificate selected	Allows selecting a certificate other than the default certificate. This preference is available only through the administrative management utilities.
Enable passphrase security system	*Yes*/*No*/*Hidden*	Prevents a rouge administrator from accessing the user's single sign-on credentials because they are prompted for the user's passphrase answer it they try to reset the user's network password and start Novell SecureLogin. If this option is set to *Yes* or *Default*, the passphrase must be answered by the user. Consequently, user contribution and knowledge is required in specific configurations to start Novell SecureLogin. If this option is set to *Hidden*, the user is not requested to answer a passphrase question. It is automatically generated by SecureLogin according to the user's parameters. This process is then automatically used in the configuration where a passphrase is required. If this option is set to *No*, the passphrase system is absent. Consequently, there is no backup process to store the user key. If the primary key is lost, Novell SecureLogin cannot be used by this user. The default value is *Yes*. **NOTE:** The *Enable passphrase security system* preference is supported only with the datastore version 6.0. The *Disable passphrase security system* preference applicable for datastore version 3.5 is removed and is no longer supported. If you are using this preference with datastore version 3.5, you must upgrade the datastore version 6.0 to use the *Enable passphrase security system* preference. This preference is available only through the administrative management utilities.

Preference	Value	Description
Lost card scenario	*Allow passphrase*/ *Require smart card*	Determines how Novell SecureLogin handles a user forgetting, losing or damaging their smart card. The Lost card option can only be used if, and only if, the Enable passphrase security system option is set to *Yes* or *Hidden* and *Use smart card to encrypt single sign-on data* is set to one of the smart card values. If this option is set to *Allow passphrase* or *Default*, the passphrase functions as a secondary key. If the smart card is not available, the passphrase is required in online mode to retrieve credentials from the directory. If this option is set to *Require smart card*, then there is no way to retrieve the credentials. The default value is *Allow passphrase.* **NOTE:** This preference is not available to users who have not upgraded their datastore to version 6.0. This preference is available only through the administrative management utilities.
Require Smart Card is present for SSO and administration operations	*Yes*/*No*/*Default*	This preference requires that a smart card must be accessible by SecureLogin each time a single sign-on operation is performed by an end user operation or administration operation. If this preference is set, SecureLogin cannot start without the smart card. As soon as the smart card is removed, SecureLogin is locked. By default, this preference is not set. If this option is set to *Yes*, Novell SecureLogin cannot start without the smart card. As soon as the smart card is removed, Novell SecureLogin is locked. If this option is set to *No* or *Default*, Novell SecureLogin can start without the smart card. The default value is *No*. **NOTE:** ◆If the *Lost card scenario* is set to *Allow passphrase*, the *Require smart Card is present for SSO and administration operations* preference is dimmed. ◆ If the *Lost card scenario* is set to *Require smart card*, then the *Require smart Card is present for SSO and administration operations* preference is available and behaves as if set to *No*. ◆ This preference is not available to users who have not upgraded their datastore to version 6.0. This preference is available only through the administrative management utilities.

Preference	Value	Description
Store credentials on smart card	*Yes*/*No*/*Default*	Allows you to store application credentials only on smart card. If this option is set to *Yes*, all credentials are stored in the PIN-protected area of a smart card instead of being encrypted in the cache file. If this option is set to *No* or *Default*, credentials are not stored in the PIN-protected area of a smart card. Scripts, settings, and policies are stored in the user's local cache, which is a mandatory preference for using smart cards. The default value is *No*. This preference is not available to users who have not upgraded their datastore to version 6.0. This preference is available only through the administrative management utilities.
Use AES for SSO data encryption	*Yes*/*No*	This option is defined to change the data encryption mode. This option is not available prior to version 6.0 of Novell SecureLogin. If the preference is set to *Yes* or *Default*, you can use AES instead of Triple DES for encrypting single sign-on data. If the preference is set to *No*, you cannot use AES instead of Triple DES for encrypting single sign-on data. The default value is *Yes*. This preference is available only through the administrative management utilities.
Use enhanced protection by default	*Yes*/*No*/*Default*	This setting is only relevant in a Novell environment; it concerns the SecretStore protection. If this option is set to *Yes* or *Default*, then a password protection is added. If this option is set to *No*, a password protection is not added. The default value is *Yes*. This preference is not available to users who have not upgraded their datastore to version 6.0. For details, see the SecretStore documentation. (http://www.novell.com/documentation/secretstore34/index.html) This preference is available only through the administrative management utilities.

Preference	Value	Description
Use smart card to encrypt SSO data	*No*/*PKI credentials*/ *Key stored on smart card*	Allows PKI credentials or a self-generated key to be created as the encryption source to encrypt the single sign-on data in the directory. If this preference is set to *No* or *Default*, all other smart card options are dimmed. If this preference is set to *PKI credentials*, single sign-on data is encrypted using the user's PKI credentials. Single sign-on data stored in the Directory and in the offline cache (if enabled) is encrypted using the public key from the selected certificate and he private key (stored on a PIN-protected smart card) is used for decryption. If this preference is set to *Key stored on smart card*, single sign-on data is encrypted using a randomly generated symmetric key that is stored on the user's smart card. This key is used to encrypt and decrypt single sign-on data stored in the Directory and in the offline cache (if enabled). The default preference is *No*. This preference is available only through the administrative management utilities.

Figure 4-16 *The Web Preferences Properties Table*

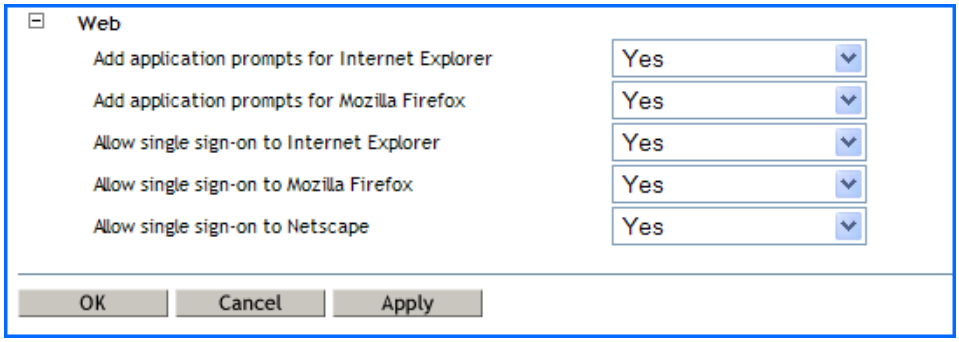


Table 4-12 *The Web Preferences Properties Table*

Preference	Value	Description
Add application prompts for Internet Explorer	*Yes*/*No*/*Default*	The default value is *Yes*. This preference is available in both the Personal Management utility and the administrative management utilities.
Add application prompts for Mozilla Firefox	*Yes*/*No*/*Default*	The default value is *Yes*. This preference is available in both the Personal Management utility and the administrative management utilities.

Preference	Value	Description
Allow single sign-on to Internet Explorer	*Yes*/*No*/*Default*	The default value is *Yes*. This preference is available in both the Personal Management utility and the administrative management utilities.
Allow single sign-on Mozilla Firefox	*Yes*/*No*/*Default*	The default value is *Yes*. This preference is available in both the Personal Management utility and the administrative management utilities.
Allow single sign-on to Netscape	*Yes*/*No*/*Default*	The default value is *Yes*. This preference is available in both the Personal Management utility and the administrative management utilities.

Figure 4-17 *The Windows Preferences Properties Table*

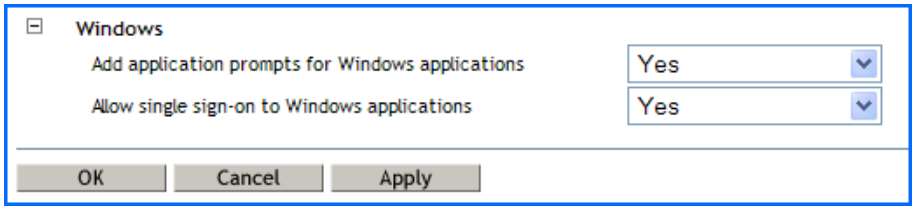
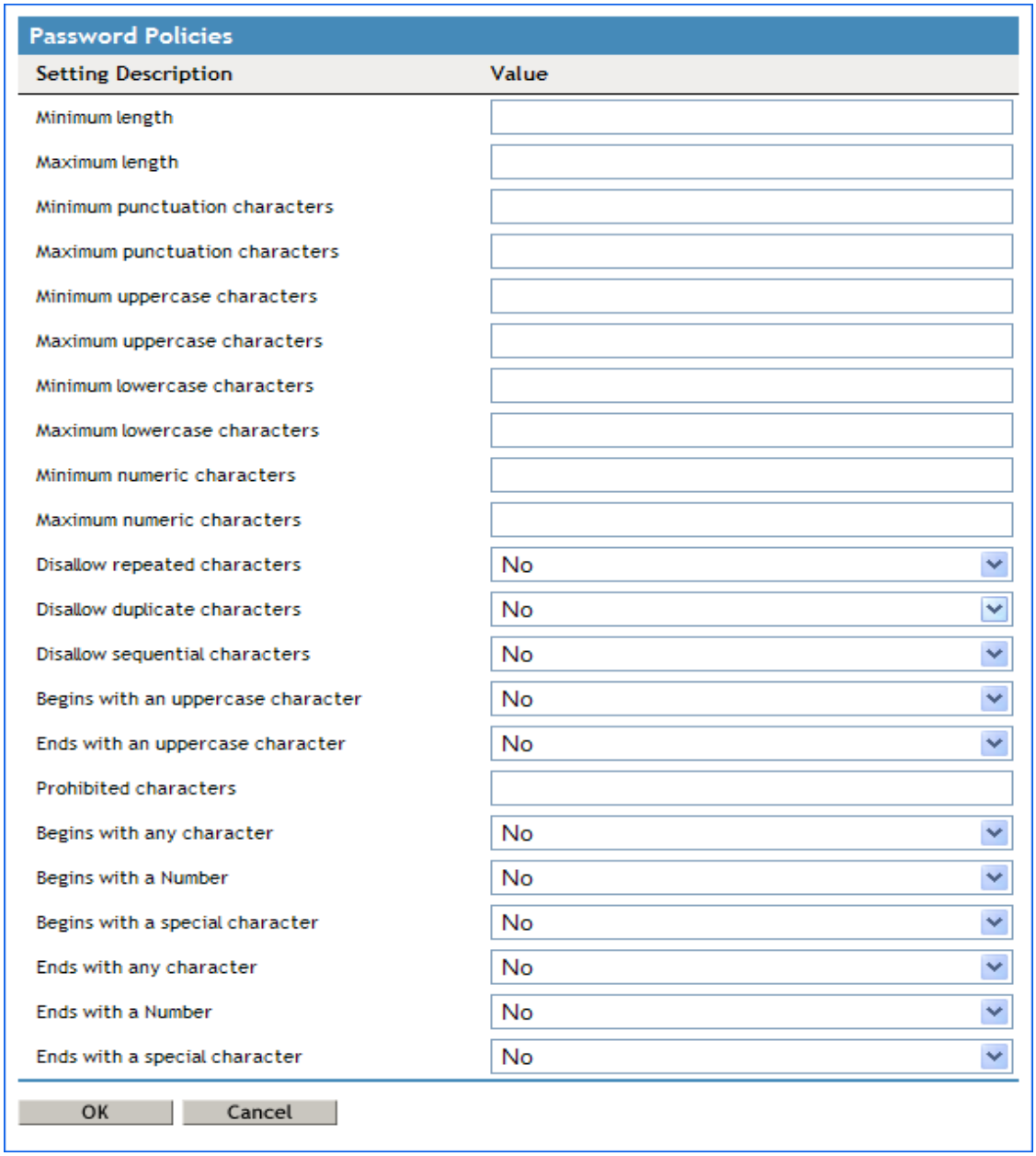


Table 4-13 *The Windows Preferences Properties Table*

Preference	Value	Description
Add application prompts for Windows applications	*Yes*/*No*/*Default*	The default value is *Yes*. This preference is available in both the Personal Management utility and the administrative management utilities.
Allow single sign-on to Windows applications	*Yes*/*No*/*Default*	The default value is *Yes*. This preference is available in both the Personal Management utility and the administrative management utilities.

4.8 The Password Policy Properties Table

Figure 4-18 *The Password Policy Properties Table*



The Password Policies pane contains a list of all the password policies. Through this pane, a user can create a new policy or delete an existing password policy.

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 the users to create and enforce these password rules through a password policy, then apply this policy to one or more application logins.

Table 4-14 *The Password Policy Properties Table*

Policy	Value To Be provided	Description
Minimum length	Whole number	Defines the minimum length of the password; that is, the number of characters required for the password.
Maximum length	Whole number	Defines the maximum length of the password; that is, the maximum number of characters allowed in password.
Minimum punctuation characters	Punctuation characters	Defines the minimum number of punctuation characters allowed in a password.
Maximum punctuation characters	Punctuation characters	Defines the maximum number of punctuation characters allowed in a password.
Minimum uppercase characters	Whole number	Defines the minimum number of uppercase characters allowed in a password.
Maximum uppercase characters	Whole number	Defines the maximum number of uppercase characters allowed in a password.
Minimum lowercase characters	Whole number	Defines the minimum number of lowercase characters allowed in a password.
Maximum lowercase characters	Whole number	Defines the maximum number of lowercase characters allowed in a password.
Minimum numeric characters	Whole number	Defines the minimum number of numeric characters allowed in a password.
Maximum numeric characters	Whole number	Defines the maximum number of numeric characters allowed in a password.
Disallow repeat characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of repeated characters, or the use of the same successive characters. If this option is set to *No*, characters can be repeated. This is the default value. If this option is set to *Yes*, same alphabetic characters in a different case are considered as different characters. For example, A and a are different. If this option is set to *Yes, case insensitive*, the successive use of the same alphabetic characters in a different case is not allowed.

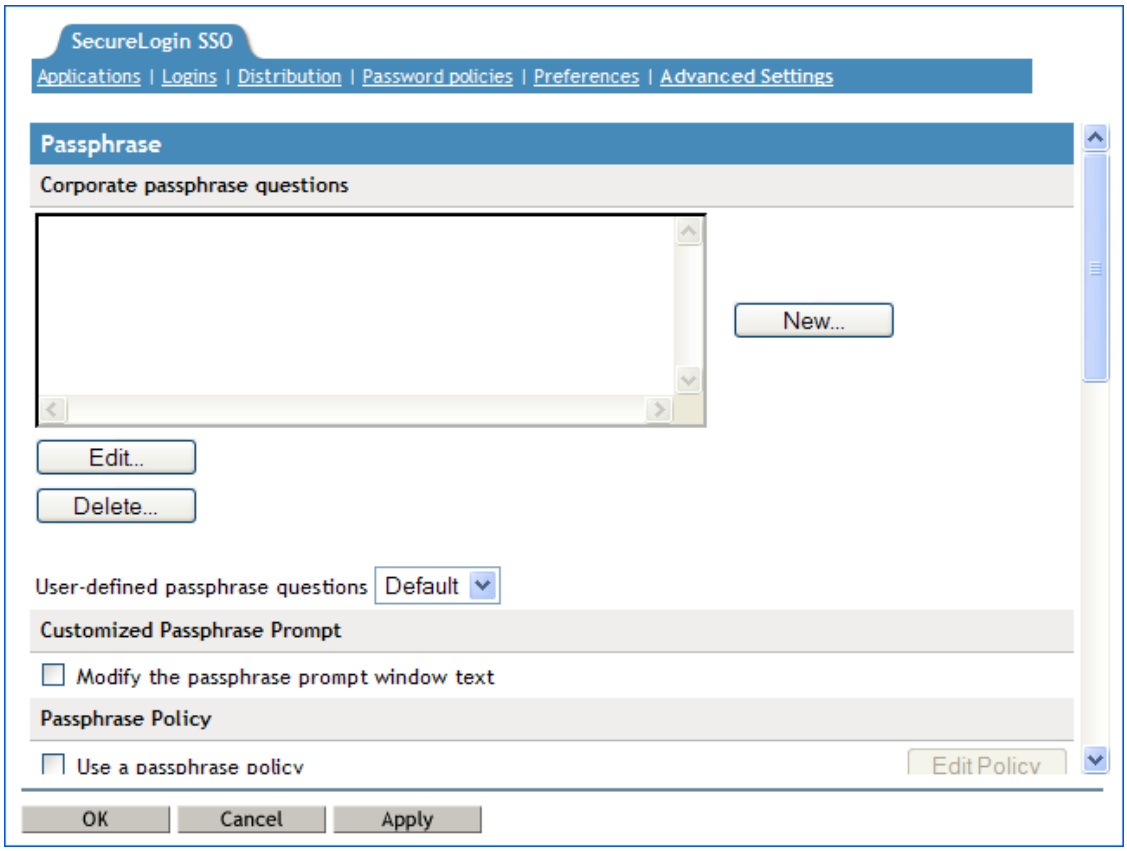
Policy	Value To Be provided	Description
Disallow duplicate characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of the same non-successive characters. If this option is set to *No*, duplicate characters are allowed. This is the default value. If this option is set to *Yes*, the same alphabetic characters in a different case are considered as different characters. For example, A (uppercase) and a (lowercase) are different. If this option is set to *Yes, case insensitive*, duplication of the same alphabetic characters in a different case is not allowed.
Disallow sequential characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of successive characters in an alphabetical order. If this option is set to *No*, sequential characters are allowed. This is the default value. If this option is set to *Yes*, sequential characters in a different case are considered as non-sequential. For example, a and b and non-sequential. If this option is set to *Yes, case insensitive*, sequential characters in different cases is disallowed.
Begin with an uppercase character	*No*/*Yes*	Enforces the use of an uppercase alphabetic character as the beginning character of a password. The default value is *No*. If this option is set to *Yes*, all other policies that indicate that a password must begin with a particular character or in a specific manner are disabled. **IMPORTANT:** Only one type of character can be designated as the first value of a password.
End with an uppercase character	*No*/*Yes*	Enforces the use of an uppercase letter at the end of a password. The default value is *No*. If this option is set to *Yes*, all other policies that indicate that a password must end with a particular character or in a specific manner are disabled.

Policy	Value To Be provided	Description
Prohibited characters	Keyboard characters	Defines a list of characters that cannot be used in a password. **NOTE:** There is no need of a separator in the list of prohibited characters. For example, @#$%&*
Begin with any Alpha character	*No*/*Yes*	Enforces the use of an alphabetic character at the beginning of a password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the password should be.
Begin with any number	*No*/*Yes*	Enforces the use of a numeric character as the first character of the password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the password should be.
Begin with any symbol	*No*/*Yes*	Enforces the use of a symbol character as the first character of the password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the password should be.
End with any Alpha character	*No*/*Yes*	Enforces the use of an alphabetic character as the last character of the password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the password should end with.
End with any number	*No*/*Yes*	Enforces the use of a numeric character as the last character of the password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the password should end with.

Policy	Value To Be provided	Description
End with any symbol	*No*/*Yes*	Enforces the use of a symbol character as the last character of the password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the password should end with.

4.9 The Advanced Settings Pane

Figure 4-19 *The Advanced Settings Pane with the Passphrase Option*



The *Advanced Settings* page contains the following three tabs:

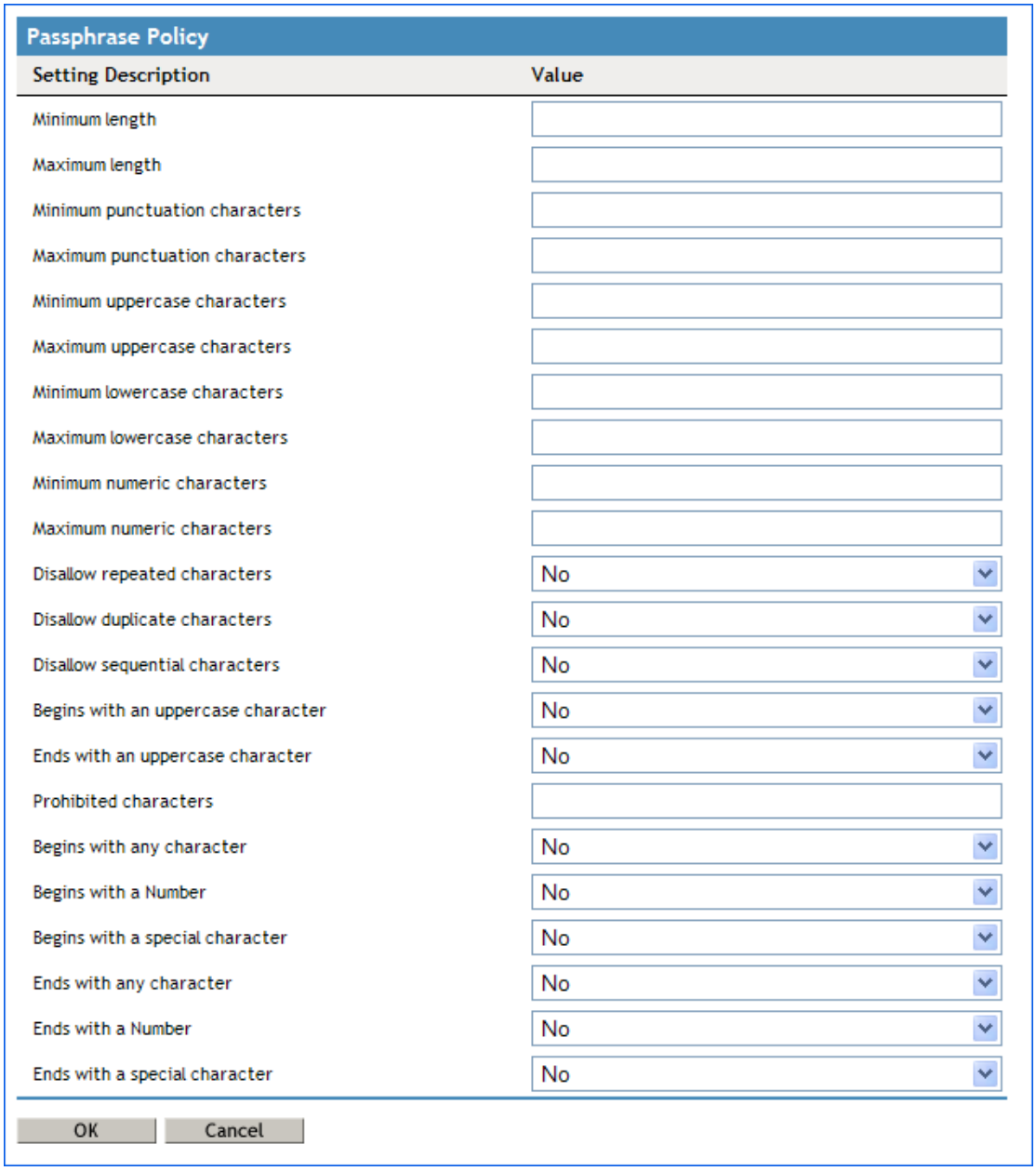
Table 4-15 *The Advanced Settings Pane*

Tab Name	Description
Passphrase	This page contains fields for: ◆ Creating, editing, and deleting corporate passphrase questions. ◆ Customizing passphrase prompts. ◆ Editing passphrase policies.
Datastore	This is used for: ◆ Selecting directory data version details (for mixed mode environments by using the earlier versions of the client software). ◆ Deleting the Novell SecureLogin configuration for a datastore object.
Corporate Redirection	This is used for managing configuration from one directory object when multiple container or organizational units require the same Novell SecureLogin environment.

NOTE: The *Advanced Settings* option is not available in the Personal Management utility.

4.10 The Passphrase Policy Properties Table

Figure 4-20 *The Passphrase Policy Properties Table*



Organizations and applications often have rules about the content of a passphrase, including the required number and type of characters. The *Passphrase* policy properties table helps the user or the administrator to create and enforce these passphrase rules through a passphrase policy, then apply this policy to one or more application logins.

Table 4-16 *The Passphrase Policy Properties Table*

Policy	Value To Be provided	Description
Minimum length	Whole number	Defines the minimum length of the passphrase; that is, the number of characters required for the passphrase.
Maximum length	Whole number	Defines the maximum length of the passphrase; that is, the maximum number of characters allowed in passphrase.
Minimum punctuation characters	Punctuation characters	Defines the minimum number of punctuation characters allowed in a passphrase.
Maximum punctuation characters	Punctuation characters	Defines the maximum number of punctuation characters allowed in a passphrase.
Minimum uppercase characters	Whole number	Defines the minimum number of uppercase characters allowed in a passphrase.
Maximum uppercase characters	Whole number	Defines the maximum number of uppercase characters allowed in a passphrase.
Minimum lowercase characters	Whole number	Defines the minimum number of lowercase characters allowed in a passphrase.
Maximum lowercase characters	Whole number	Defines the maximum number of lowercase characters allowed in a passphrase.
Minimum numeric characters	Whole number	Defines the minimum number of numeric characters allowed in a passphrase.
Maximum numeric characters	Whole number	Defines the maximum number of numeric characters allowed in a passphrase.
Disallow repeat characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of repeated characters, or the use of the same successive characters. If this option is set to *No*, characters can be repeated. This is the default value. If this option is set to *Yes*, same alphabetic characters in a different case are considered as different characters. For example, A and a are different. If this option is set to *Yes, case insensitive*, the successive use of the same alphabetic characters in a different case is not allowed.

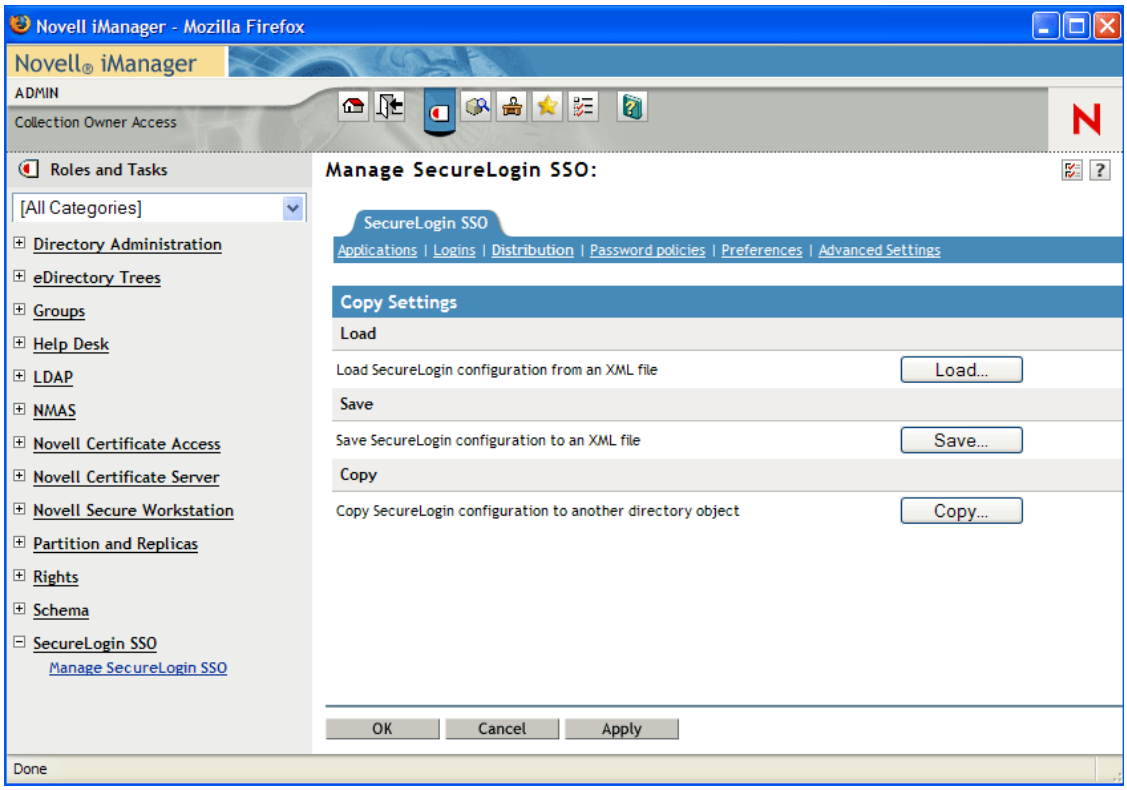
Policy	Value To Be provided	Description
Disallow duplicate characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of the same non-successive characters. If this option is set to *No*, duplicate characters are allowed. This is the default value. If this option is set to *Yes*, the same alphabetic characters in a different case are considered as different characters. For example, A (uppercase) and a (lowercase) are different. If this option is set to *Yes, case insensitive*, duplication of the same alphabetic characters in a different case is not allowed.
Disallow sequential characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of successive characters in an alphabetical order. If this option is set to *No*, sequential characters are allowed. This is the default value. If this option is set to *Yes*, sequential characters in a different case are considered as non-sequential. For example, a and b and non-sequential. If this option is set to *Yes, case insensitive*, sequential characters in different cases is disallowed.
Begin with an uppercase character	*No*/*Yes*	Enforces the use of an uppercase alphabetic character as the beginning character of a passphrase. The default value is *No*. If this option is set to *Yes*, all other policies that indicate that a passphrase must begin with a particular character or in a specific manner are disabled. **IMPORTANT:** Only one type of character can be designated as the first value of a passphrase.
End with an uppercase character	*No*/*Yes*	Enforces the use of an uppercase letter at the end of a passphrase. The default value is *No*. If this option is set to *Yes*, all other policies that indicate that a passphrase must end with a particular character or in a specific manner are disabled.

Policy	Value To Be provided	Description
Prohibited characters	Keyboard characters	Defines a list of characters that cannot be used in a passphrase. **NOTE:** There is no need of a separator in the list of prohibited characters. For example, @#$%&*
Begin with any Alpha character	*No*/*Yes*	Enforces the use of an alphabetic character at the beginning of a passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the passphrase should be.
Begin with any number	*No*/*Yes*	Enforces the use of a numeric character as the first character of the passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the passphrase should be.
Begin with any symbol	*No*/*Yes*	Enforces the use of a symbol character as the first character of the passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the passphrase should be.
End with any Alpha character	*No*/*Yes*	Enforces the use of an alphabetic character as the last character of the passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the passphrase should end with.
End with any number	*No*/*Yes*	Enforces the use of a numeric character as the last character of the passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the passphrase should end with.

Policy	Value To Be provided	Description
End with any symbol	*No*/*Yes*	Enforces the use of a symbol character as the last character of the passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the passphrase should end with.

4.11 The Distribution Pane

Figure 4-21 *The Distributions Pane*



The *Distribution* pane provides access to:

- The Load dialog box
- The Save dialog box
- The Copy dialog box

The Load and Save dialog boxes help the administrator to import and export the SecureLogin configurations.

The Copy dialog box help the administrator to copy an object's SecureLogin configuration from one object to another.

NOTE: The *Distribution* pane is not available for the Personal Management utility.

Enabling Applications and Web Sites for Single Sign-On

5

The Novell SecureLogin has predefined applications for single sign-on access to a wide range of commercially available applications.

Novell SecureLogin detects applications for which a predefined application exists. For example, if Novell SecureLogin detects a SAP* dialog box, then it prompts the user to allow the Novell SecureLogin to enable single sign-on for the application.

NOTE: Predefined applications for some commonly used applications are incorporated with the Novell SecureLogin, and with each new version, more applications are developed and made available to the customers. For detailed information on the predefined applications, see "Using a Predefined Application to Enable a Web Application" in the *Novell SecureLogin 6.1 Administration Guide.*

The Novell SecureLogin provides wizards and applications to facilitate single sign-on to almost any new or proprietary application if a predefined application is not available. This helps the users or a Novell Consultant to build an application definition for almost any proprietary application or an upgrade. For more information, see Chapter 3, "The Novell SecureLogin Components," on page 13.

Novell SecureLogin also supports enabling the single sign-on for standard terminal emulator applications.

- Users can enable single sign-on for terminal emulators by using the terminal launcher tool.
- Novell SecureLogin has additional tools such as, `Window Finder` and `LoginWatch`, which help the user to enable single sign-on for even the most difficult applications. For details, refer to the *Novell SecureLogin 6.1 SP1 Application Definition Guide*.

Novell SecureLogin stores the login information requirements for applications including the following:

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

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

Before Novell SecureLogin can enable an application for single sign-on for a particular user, it must learn a user's application credentials so that it can encrypt and store them for future logins unless it is used in conjunction with Identity Management solutions such as Novell Identity Manager.

When a user starts an application for the first time after it is enabled for single sign-on, the Novell SecureLogin prompts the user for application credentials, then encrypts and stores them in the directory against the user object. The credentials are passed automatically to the application for subsequent logins.

Automated single sign-on is achieved by using the proprietary application definitions. The application definitions are managed in directory environments through the Novell SecureLogin administrative management utilities. In local and standalone deployments, the application definitions are managed in the Personal Management utility or distributed by using the advanced offline signed and encrypted method.

The single sign-on applications are created, modified, and deleted in the Applications pane. Users can also create application definitions with the Novell SecureLogin Wizard. There a wide range of options in the Novell SecureLogin to enable applications. Regardless, of the origin of the application definition when an application is enabled for single sign-on, it is added and maintained in the *Applications* properties table.

For detailed procedures about enabling applications and Web sites for single sign-on, see "Enabling Applications and Web Sites" in the *Novell SecureLogin 6.1 Administration Guide.*

Operational Environment

6

This section contains information on the following:

6.1 Operating Systems

The Novell SecureLogin 6.1 supports the following 32 bit operating systems:

- Microsoft Windows Vista*
- Microsoft Windows XP
- Microsoft Windows 2000 Workstation

6.2 Platforms

The Novell SecureLogin supports the following platforms:

- Microsoft Active Directory*
- Microsoft Active Directory Application Mode (ADAM)
- 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

6.3 Clients

The Novell SecureLogin supports the following 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

If your environment is not included in this list, contact Novell Support for assistance.

6.4 Windows

The following is a list of predefined applications for Windows applications:

- 401K Web Login
- ActiveSync*
- AOL Instant Messenger*
- Cisco* VPN
- Citrix Program Neighborhood
- Citrix Program Neighborhood Agent
- Citrix Web Portal
- CNN* Member Services
- Cyberview*
- eBay*
- Entrust* Client
- Entrust Server
- Eudora* eMail
- ExcelCare* Application
- EzTeller
- Firewall-1 Session Authentication Agent
- GoldMine* v. 5.5
- Heat* Call Logging
- Internet Explorer
- Lotus* Notes* v5 and v6.5
- MEDITECH* v3.*x* and 4.*x*

  NOTE: The support for MEDITECH 3.*x* and 4.*x* is dependant on the presence of the MEDITECH `mrwscript.dll` file. The `.dll` file is provided by MEDITECH and must be installed during the installation of the MEDITECH application workstation.

- Microsoft Networking Client
- Microsoft Outlook*
- Microsoft Outlook Express
- Microsoft SQL
- MSN* Messenger 4.5 and 4.7
- MSN Messenger 5.0, 6.0, and 7.5
- My Novell Account Web login
- Netscape*
- Novell BorderManager® Web Login - HTML
- Novell BorderManager Web Login - Java*
- Novell BorderManager VPN Client

- Novell Groupwise® Client 5.5, 6.0, and 7.0
- Novell Groupwise Messenger 2.0
- Novell Groupwise Notify Client
- Novell Groupwise PDA Synchronization Application
- Novell Groupwise 7.0 Web Login
- Novell Groupwise iChain® Web Login
- Novell iFolder® 2.*x*
- Novell iFolder 3
- Novell iManager Web Login
- ODBC Driver Connect
- Onebox* e-mail
- Optima
- PCAnywhere* 8.0
- Protocom SecureRemote
- QANTAS* Frequent Flyer
- Remedy* Notifier
- SaveTime
- SAP - `SAPlogon.exe`
- SAP R/3 Login
- Superiew
- Supportworks* 4.5
- Trillian*
- Visual SourceSafe* Login
- VNC 3.0 and 4.0
- Windows 9*x* Dialup Networking
- Windows 9*x* Login
- Windows NT* Login
- Yahoo! Mail*
- Yahoo! Messenger

If the Novell SecureLogin does not prompt to enable single sign-on for applications, use the Add Application Wizard to build an application.

6.5 Terminal Servers

The Novell SecureLogin supports the following terminal servers:

- Citrix MetaFrame* 1.8 and above, including:
  - Citrix MetaFrame XP Presentation Server
  - Citrix MetaFrame Presentation Server 3.0
- Microsoft Windows 2000/2003 Terminal Server

6.6 Terminal Emulators

The Novell SecureLogin provides single sign-on support for the applications running on any back end system for example, UNIX*, RACF*, CICS*, ACF2* using the following emulators:

- AbsoluteTelnet
- Attachmate* Extra
- Attachmate Extra 2000
- Attachmate KEA!
- Attachmate Personal Client
- Chameleon HostLink*
- CRT
- Eicon Aviva*
- GLink
- HBO* Star Navigator
- IBM* Personal Communications
- IDXTerm Healthcare
- Info Connect
- Microsoft Telnet 2000
- Microsoft Telnet NT
- Microsoft Telnet Win 9*x*
- Mocha W32 Telnet
- NetTerm 4.2
- NS/Elite*
- Passport TN 3270E
- PowerTerm*
- QVT
- QWS3270 Plus
- SDI TN3270
- TeraTermPro
- TinyTERM
- ViewNow*
- Wall Data Rumba*
- Wall Data Rumba 2000
- Wall Data Rumba Web To Host
- WinComm
- Window Telnet VT
- WRQ Reflection*

6.7 Web or Internet

The Novell SecureLogin includes single sign-on support for Web applications accessed by using the following browsers:

- Internet Explorer

  Mozilla Firefox

- Netscape

IMPORTANT: Novell 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.

Novell recommends to users that they manually create application definitions for Netscape applications because some functionality might not be available.

Contact Novell Support to enable single sign-on for Netscape application that is not provided a predefined application.

Novell SecureLogin provides predefined applications for a number of Web applications with embedded login fields including:

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

NOTE: The Novell SecureLogin prompts you if a predefined application is available. You can also use the Add Application Wizard to build an application definition for the application.

Glossary

administrative management utilities
The utility available in Novell® SecureLogin to manage the users in a directory environment. It provides additional functionality that is not available in the Personal Management utility.

application programming Interface
Enables programmatic communication with the application.

application definition
The Novell SecureLogin configuration data that enables the single sign-on for a specific application's login and other events.

cache
The cache encrypts the local copy of the Novell SecureLogin data so that a user can continue to use the Novell SecureLogin even if the directory is unavailable. In a standalone mode (non-directory) mode, the cache contains all the Novell SecureLogin single sign-on data for a user.

User data includes credentials, preferences, password policies, and application definitions. By default, the Novell SecureLogin cache is created on the local hard drive. In a corporate implementation, this data is also stored in the directory. The data in the directory and the workstation cache are regularly synchronized to ensure that the user data is current.

container
The Microsoft Active Directory object used to contain other directory objects.

corporate configuration
Allows the administrators in a directory environment to configure where the Novell SecureLogin setting on objects are inherited from.

credentials
Usernames, passwords, and other data that uniquely identifies and authenticates a user to an application.

Directory Services
Structured repository that identifies all aspects of a network. It is made up of users, software, hardware, and any rights or policies assigned.

distinguished name
The full name of a directory object, including the domain name and organizational units to which the user belongs.

domain
A security boundary that groups users or devices. Domain objects are defined by schema, configuration, and security policies of the network.

Group policy
The Group policy enables the centralized configuration and management of selected objects. User or computers are selected by the administrators to be included in the group policy group for collective administration.

High Level Language Application Programming Interface (HLLAPI)
The API that enables a terminal emulator screen to read and be interpreted by an application and enables the keyboard input to be processed by the emulator.

Lightweight Directory Access Protocol (LDAP)
The protocol used for updating and searching directories running over TCP/IP.

login
The set of credentials (such as username and password) stored in the Novell SecureLogin.

management utility
Novell SecureLogin's management utility. It generically refers to the administrative management utilities and the Personal Management utility.

object
In a directory environment, a set of attributes that identifies a user, hardware, or an application.

organizational unit (ou)
In a directory environment, a domain subgroup that has administrative control of all the associated objects.

passphrase
A combination of a question and answer used to protect the user credentials from unauthorized use.

password policy
One or more password rule grouped under a unique name.

password rule
A password parameter configured in the Password Policies properties table. Password rules are grouped under a Password policy.

personal management utility
Provides user administration tools to the user from his or her desktop.

predefined application
Automates single sign-on for many commercially available applications.

Schema
A database for the classes (tables). It defines the objects and the attributes (columns) and stores the object data.

Novell SecureLogin
The application that allows users to access a wide range of applications, Web sites, and mainframe sessions. With this, users need not log in to the application separately.

SecureLogin Attribute Provisioning (SLAP)
The tool that enables Novell SecureLogin to leverage user data from an organization's provisioning system.

Single Sign-On-Enabled
When an application is enabled for single sign-on for a user, the user need not specify his or her credentials to log in to the application. When the user launches an application, the Novell SecureLogin transparently manages the login process.