SecureLogin 9.0

User Guide

June, 2021

Legal Notice

Contents

About This Guide

This guide provides information about how to use SecureLogin to enable single sign-on to your applications.

Additional Documentation

For the latest version of this guide and other SecureLogin documentation resources, see the SecureLogin Documentation and keep up to date on patches and versions of both SecureLogin and the host operating system.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the **comment on this topic** link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care at https://www.microfocus.com/support-and-services/.

1 Overview

SecureLogin is a single sign-on (SSO) product. It eliminates the necessity for users to remember multiple username and passwords. It stores username and passwords and automatically retrieves them for users when required.

SecureLogin consists of multiple, integrated security systems that provide authentication and single sign-on to networks and applications. It has wizards and tools that make it easy to centrally configure for use on the corporate network.

It supports username, passwords, and multi-factor authentication such as smart cards, tokens, or biometrics at the network and application levels.

1.1 Administrative Manage Utilities

Administrators use the Administrative Management utilities: SLManager and Active Directory Computer Users and Snap Ins to define the settings and preferences of SecureLogin for use by the end-users.

1.2 SecureLogin Client Utility

You can use the SecureLogin Client Utility to customize SecureLogin to suit your requirements. For example, you can set your own passphrase question and answer, and set your own password policies.

2 Accessing the SecureLogin Client Utility

The SecureLogin Client Utility is represented by an icon in the notification area (system tray).

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

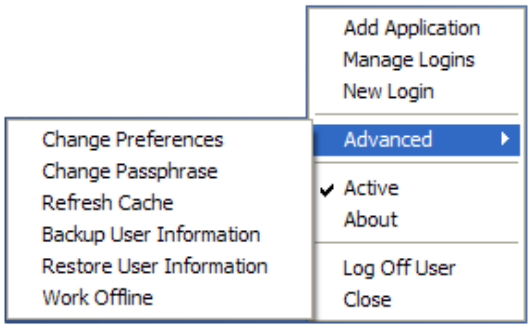
After you successfully launch SecureLogin, appears in the notification area. This icon is a shortcut for the SecureLogin functionality on your workstation. Double-click this icon to launch the SecureLogin Client Utility.

2 Right-click the SecureLogin icon in the notification area.

3 Select the task you want to perform.

For example, select **Add Applications** to add, delete, and manage the applications.

Figure 2-1 *The Advanced Preferences*



The following table lists the options available in the menu. If any of these options does not appear in the menu, your administrator has not enabled this functionality for you.

Option	Description
Add Application	Starts the Add Applications wizard. Enables an application for single-sign on by creating a script that automates the login.
Manage Logins	Launches the SecureLogin Client Utility. Adds login IDs (login credentials), links login IDs to applications, manages password policies, and manages SecureLogin settings.
New Login	Enables you to create multiple single sign-ons or login IDs for an application. For example, if you have three accounts on the same application, SecureLogin manages the three sets of credentials. SecureLogin provides the option to select the preferred account when the application starts.
Advanced > **Change Preferences**	Opens the SecureLogin Client Utility, with the **Preferences** option selected.

Option	Description
Advanced > **Change Passphrase**	Enables you to change your passphrase question or passphrase answer.
Advanced > **Refresh Cache**	Refreshes the local cache settings and updates cache with any changes made at the associated container or organizational unit level.
Advanced > **Backup User Information**	Backs up the SecureLogin user information into a file.
Advanced > **Restore User Information**	Restores SecureLogin information from the backup file.
Advanced > **Work Online** / **Offline**	Toggles between online and offline states of SecureLogin. When you work offline, SecureLogin uses the local (secondary) cache rather than the directory. This option is not displayed in the Standalone mode.
Active	Determines whether SecureLogin is enabled (active) or disabled.
About	Displays the SecureLogin version number and the status of the data stores. The primary data store is the directory. The secondary is the local cache.
Log User Off Windows	Enables you to shut down all programs, including SecureLogin, and log out from the workstation. Performs the same function as the **Shut Down** > **Log Off** option on the Windows Start menu.
Close	Shuts down SecureLogin.

3 Automating Logging In to Applications

An application definition is a set of instructions for SecureLogin about how to handle the login for an application. SecureLogin uses application definitions to automatically log you in to Windows, web, or Java applications. SecureLogin has predefined application definitions for a few applications. You can use the Application Definition Wizard to create new application definitions.

The wizard captures and stores your login name (username), password, and any other information required for authentication. SecureLogin stores all application definitions in a secure encrypted cache on your computer and in the corporate directory.

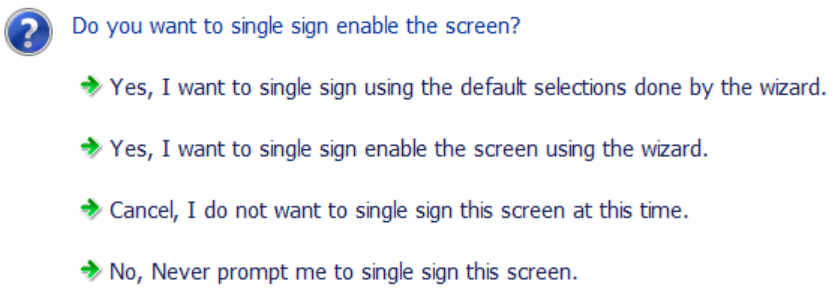
You can also write your own application definitions. However, it is recommended that you use the Application Definition Wizard to create your application definition.

3.1 Responding to Pop-Up Prompts

After SecureLogin is installed on your desktop, it watches for applications that are not enabled for SSO. Upon detecting such an application, it launches the wizard window to enable those applications for SSO. If you do not require SSO to the application, ignore the notification. On a Windows 10 computer, the wizard window is launched soon after SecureLogin detects an application for SSO.

If SecureLogin detects an login screen on an application, it presents the following dialog box:

Figure 3-1 *Prompt to Enable for Single Sign-On*



Select one of the following options:

- **Yes, I want to single sign using the default selections done by the wizard**: Select this option to create an application definition using the default settings.

  Through the default settings, you can create an application definition to handle the username and password fields and submit button identified by the Wizard.
- **Yes, I want to single sign enable the screen using the wizard (Recommended)**: If SecureLogin detects more than two text fields or one button in a login window, select this option. Through this, you can review the fields identified by the wizard, confirm that correct fields are selected, and button are identified.
- **Cancel, I do not want to single sign this screen at this time**: Select this option if you do not want to enable an application for SSO at this time.
- **No, Never prompt me to single sign this screen**: Select this option if you do not want to enable an application for SSO. You are not be prompted to enable the application for SSO again.

3.2 Predefined Application Definitions

SecureLogin has predefined application definitions to automatically capture and store login credentials for many common applications.

If a predefined application definition does not exist for your favorite application you, use Application Definition Wizard to create a new application definition to capture and store your logon credentials, along with any other information required for authentication. For details about using the Application Definition Wizard, see the *NetIQ SecureLogin 9.0 Application Definition Guide*.

3.2.1 Windows Applications

Some of the predefined application definitions for Windows applications include:

- 401K Web Login
- ActiveSync
- AOL Instant Messenger
- Cisco VPN
- Citrix Program Neighborhood
- Citrix Program Neighborhood Agent
- Lotus Notes v5 and v6.5
- Microsoft Outlook
- Microsoft Outlook Express

3.2.2 Web Applications

Some of the predefined application definitions for Web applications are:

- Amazon.com
- eBay
- Hotmail
- QANTAS Frequent Flyer

- CNN Member Services
- Monster.com

3.3 Enabling an Application for Single Sign-On Using a Predefined Application Definition

The procedure to use a predefined application definition to enable an application definition is the same for all web, Windows, and Java applications.

1. Launch an application.

   If a predefined application definition exists for that application, SecureLogin automatically detects the application definition.

2. Select **Yes, I want to single sign the screen using the predefined application definition**.

   SecureLogin identifies the application and displays the name of the application in the prompt.

3. You are prompted to specify the credentials for the application. Specify the username, password, and any other information required.

4. Click **OK**.

   The next time you launch the application, you are not prompted for username and password. SecureLogin provides this.

3.3.1 Enabling SSO for Novell WebAccess

The following example demonstrates enabling SSO for Novell WebAccess. SecureLogin provides a predefined application for Novell WebAccess.

This procedure assumes that you already have a GroupWise account.

1. Launch Novell WebAccess.

   SecureLogin detects the application and the SecureLogin dialog box is displayed.

2. Select **Yes, I want to single sign the screen using the predefined application definition. Novell GroupWise Messenger V7.0 Web Login**.

   The Wizard detects the name of the application. In this example, SecureLogin identifies that you are creating an application definition for Novell GroupWise WebAccess.

3. Specify your Username and password, then click **OK**.

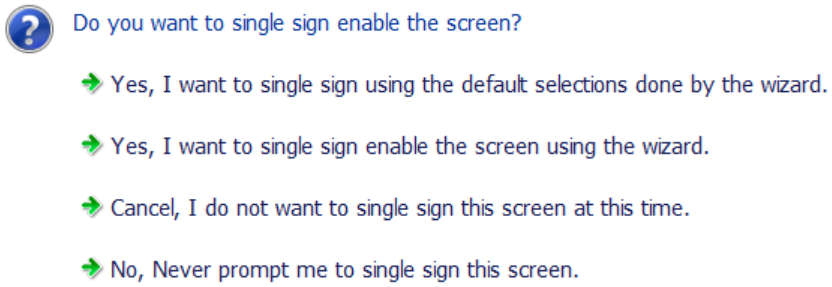
   Next time, you do not need to specify your credentials.

   To test the application definition, log out and log in. If the application is defined correctly with the correct credentials, you are logged in successfully. If your login is not successful, delete the application definition and repeat the above steps. You might also need to review the application definition for completeness of event responses and errors.

3.4 Using the Default Selections

1. Launch the web application for which you want to enable SSO.
2. SecureLogin detects the application and prompts you to enable SSO.

Figure 3-2 *Prompt to Enable for SSO*



3 Select **Yes, I want to single sign using the default selections done by the wizard**.

4 Specify your credentials, then click **OK**.

SecureLogin saves your credentials in the directory. The next time you launch the application, SecureLogin provides the credentials for you.

3.5 Using the SecureLogin Client Utility to Enable Applications for SSO

You can enable an application for SSO through the SecureLogin Client Utility or the Application Definition Wizard.

1 Double-click the SecureLogin icon in the notification area. This launches the SecureLogin Client Utility with the **Application** menu selected.

2 Click New. Alternatively, select **File** > **New** > **Application**.

3 From the **Predefined Application Definition** list, select the appropriate application definition.

4 Click **OK**. Details of the selected application appear.

5 On the Details page, specify the username and password of the application.

6 (Optional) Select the **Settings** tab and define your preferences.

7 Click **Apply** > **OK**.

3.6 Using a New Application Definition to Enable Applications for SSO

1 Double-click the SecureLogin icon in the notification area. This launches the SecureLogin Client Utility with the **Application** menu selected.

2 Click New Alternatively, click **File** > **New** > **Application**.

3 Select **New Application Definition**.

4 From the **Type** list, select the type of application.

You can select:

- Windows

- Terminal Launcher
- Startup
- Java
- Generic
- Advanced Web
- Web wizard Script

NOTE: For a Flash application, select the type as **Windows**. Use the Flash Window finder tool to read the title of the application and provide the same in the **EXE** text box.

5 Specify other details such as the name, the URL, executable, and description as required.

6 Click **OK**.

7 From the **Application** navigation tree on the left pane, select the application you created.

8 Specify the username and password of the application.

9 (Optional) Specify the application definition of this application.

10 (Optional) Change the default settings to suit your requirements.

11 Click **Apply** > **OK**.

3.7 Changing the Name of an Application Definition

1 Double-click the SecureLogin  icon in the notification area.

2 In the Application navigation area on the left panel, select the application you want to modify.

3 Click **Edit**.

4 Make the required changes. You can modify the name, ID, and type of the application.

5 Click **OK**.

3.8 Modifying an Application Definition

This section provides information about modifying the application definitions created using the Application Definition Wizard. You can use the Application Definition Wizard to add or modify the definition, add notifications for password change and login notifications.

NOTE: Predefined application definitions cannot be edited using the Application Definition Wizard. You must edit them manually. For more information about editing the application definitions manually, see *NetIQ SecureLogin 9.0 Application Definition Guide*.

You can modify the Application Definition Wizard in one of the following ways:

- Section 3.8.1, “Modifying through the Application Definition Wizard,” on page 16
- Section 3.8.2, “Modifying through the Manage Logins Menu,” on page 16

3.8.1 Modifying through the Application Definition Wizard

1. Double-click the SecureLogin icon on the notification area.
2. From the **Applications** pane, select the application definition you want to modify.
3. Select the **Definition** tab.
4. Click **Edit Wizard**. The attributes pane opens enabling you to edit the application definition.
5. Make the changes. Each of the attributes are explained in detailed in the earlier section.
6. Click **Apply** > **OK**.

3.8.2 Modifying through the Manage Logins Menu

1. Right click the SecureLogin icon on the notification area, then select **Manage Logins**.
   The Administrative Management utility displays a list of applications enabled for SSO.
2. From the **Applications** pane, select the application deviation you want to modify.
3. Select the **Definition** tab.
4. Click **Edit Wizard**. The attributes pane opens enabling you to edit the application definition.
5. Make the changes.
   See the *NetIQ SecureLogin 9.0 Application Definition Wizard Administration Guide*
6. Click **Apply** > **OK** to save and exit.

3.9 Deleting an Application Definition

1. Double-click the SecureLogin  icon in the notification area.
2. In the Application navigation on the left panel, right-click the application you want to delete.
3. Click **Delete**. The selected application is deleted.

4 Creating Login Credentials

SecureLogin allows you to enable multiple logins for single sign-on (SSO) to the same application.

Through the **My Login** page, you can view and edit SecureLogin user data, such as username and passwords that allow you to successfully log in to an application.

To use SecureLogin to automatically log you in to an application, you must create a Login (set of credentials) and link it to that application.

If you add an application that has a predefined application, you need to link the login to it. You can provide login variables the next time that you access the application. However, you do not need to add or create login for applications that you enabled for SSO in the following ways:

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

In these two cases, the Application Definition Wizard created the login while you were adding the application to the SSO functionality.

You can use the same login to log you in to more than one application.

Also, if you have multiple roles, you can set up multiple logins for the same application. For example, you might be a network administrator as well as a user. When you log in to the network as administrator and then launch an application, SecureLogin prompts you to select a profile. After you select the administrator profile, SecureLogin then automatically logs you in with the appropriate credentials.

4.1 Creating Login Credentials Using the Add New Login wizard

4.1.1 Creating the Login

1 Right-click the SecureLogin icon in the notification area, then click **Manage Logins**.

or,

Double-click the SecureLogin icon in the notification area.

2 Click **My Logins > New**.

3 Specify a name or ID and click **OK**.

You have now successfully created a new login. Repeat Step 1 through Step 3 to create other logins. However, you need to specify the username and password to this login.

4 Continue with Specifying the Credentials to specify the username and password for this login.

4.1.2 Specifying the Credentials

1 In the **My Login** list in the left panel, select the login you created. The login page is displayed.

2 Select **Username**, then specify the username in the adjacent text field.

3 Select **Password** and specify the password.

4 Click **Apply** > **OK**. Your login credentials are saved.

Repeat Step 1 on page 18 through Step 4 on page 18 to specify the credentials to other logins.

4.1.3 Linking a Login to an Application

1 From **My Logins**, select the login that you want to link to an application.

2 Click 

. The Applications List window opens.

3 Select the applications you want to link to this login. Click **OK**.

4 Click **Apply**, then click **OK**.

4.1.4 Delinking a Login from an Application

1 From **My Logins**, select the login that you want to delink to an application.

2 Click 

. The Application List window opens.

3 Select the applications you want to delink from the login.

4 Click **Apply** > **OK**.

4.2 Adding Multiple Logins

4.2.1 Prerequisites

- Ensure that the first account is enabled for SSO before you add another login to the existing login.
- It is recommend that you make a list of the username, passwords, and a unique name to identify the login before you add multiple logins to the first account.

Table 4-1 An Example List of Additional Logins

Unique Name	User Name	Password
Administrator	admin	123456
Support	help	abcdef
User	test1	xyz123

4.2.2 Creating Another Login

1. Right-click the SecureLogin icon in the notification area, then select **New Login**.
2. Select the required application.
3. Click **Next**. A page displays where you can provide a description for the login.
4. In **Description**, specify a descriptive name for the login (for example, NSL Administrator).
5. Click **Finish**. A page appears where you can enter your credentials.
6. In **Username**, specify the username.
7. In **Password**, specify the password.
8. Specify any additional variables as required.
9. Click **OK** to save your information and exit the SecureLogin Client Utility.
10. Repeat Step 1 on page 18 through Step 9 on page 19 to add any additional logins. When you have created all logins, you can view and manage them in the SecureLogin Client Utility.

4.2.3 Viewing the Additional Login

1. Right-click the SecureLogin icon in the notification area, then select **New Login**. The SecureLogin - Add New Login wizard welcome dialog box is displayed.
2. In the navigation tree, select **My Logins**. The My Login page is displayed.
3. Verify that the additional login is added to the My Logins pane.
4. Click **OK** to close the SecureLogin Client Utility.

4.2.4 Testing the Multiple Logins

1. Launch the application for which you added multiple logins.
2. Select the functionality you want to access. The login selection dialog box is displayed.
3. Select the appropriate login credential set.
4. Click **OK**. SecureLogin enters the credentials and you are automatically logged in to the application.

5 Changing Preferences

The Preferences allow you to customize SecureLogin. Use this option to customize SecureLogin to function in the way you want it.

The administrator can also set the SecureLogin user preferences in the Administrative Management utility. Each preferences has a default value until an alternative value is specified.

NOTE: The preferences value that you set at the user object-level overrides all higher level object values.

The list of preferences is a subset of the preferences that the administrator controls through the Administrative Management utility. If an administrator has disabled a setting, you cannot use it or change it on your workstation.

5.1 Viewing and Changing the Preferences

1. Click **Preference**.
2. Select the setting you want to customize. You can change preferences for the following settings:
   - “General Preference, Definitions, and Values” on page 22
   - “Java Preference, Definitions, and Values” on page 24
   - “Web Preferences, Definitions, and Values” on page 25
   - “Windows Preferences, Definitions, and Values” on page 27
3. In **Value**, select the appropriate value.
4. Click **OK**.
5. Click **Yes** to save the settings and exit.

5.2 General Preference, Definitions, and Values

Table 5-1 *The General Preferences Properties Table*

Preference	Possible Values	Description	Default Value
Display logged on user in task bar	**Disable/First name/Last name/Full name/ Distinguished name/Default**	This preference controls the display of the logged in user name on the task bar. If this option is set to **Disable**, the logged in username is not displayed on the task bar. If this option is set to First name/Last name/Full name/ Distinguished name/Default, based on the selection respective value is displayed on the task bar. **NOTE:** For the logged in username to be displayed in the task bar, you must right-click the **Secure Login** icon on the notification area (system tray) and select **Show User bar** or you can right-click on the task bar and select **Toolbar -> SecureLogin SSO User**. This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).	**Disable**
Detect incorrect passwords	**Yes**/**No**/**Default**	Predefined applications generally include commands to respond to incorrect password dialogs. This preference enables SecureLogin to respond to incorrect passwords for web applications. 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. This preference is available in both the SecureLogin Client Utility and the administrative management utilities (SLManager and MMC snap-ins).	**Yes**

Preference	Possible Values	Description	Default Value
Enable cache file	**Yes**/**No**/**Default**	This preference controls creating and updating of a SecureLogin cache file on the local workstation. The cache file stores all 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 might have some conflicts with organizational security policy. If this option is set to **Default**, SecureLogin behaves as if it is set to **Yes**. This preference is available in both the SecureLogin Client Utility and the administrative management utilities (SLManager and MMC snap-ins).	**Yes**
Enter API license key(s)	Specify API license key(s)	Specify the API license key(s) provided by SecureLogin to activate the API functionality for an application. You can add more than one API license key.	Specify the API license key
Password protect the system tray icon	**Yes**/**No**/**Default**	This preference restricts the users from accessing the SecureLogin icon menu option (from the notification area (system tray) without their network login password. If this option is set to **Yes**, the SecureLogin icon on the notification area (system tray) is password protected. If this option is set to **No** or **Default**, the SecureLogin icon on the notification area (system tray) is not password protected. This preference is available in both the SecureLogin Client Utility and the administrative management utilities (SLManager and MMC snap-ins).	**No**
Provide API Access	**Yes**/**No**/**Default**	This preference controls the API functionality use. If this option is set to **Yes**, the API access is enabled. If this option is set to **No** or **Default**, the API access is disabled. This preference is available in both the SecureLogin Client Utility and the administrative management utilities (SLManager and MMC snap-ins).	**No**

Preference	Possible Values	Description	Default Value
Set the cache refresh interval (in minutes)	5	This preference defines the time in minutes the synchronization of user data and directory on the local workstation. 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 SecureLogin Client Utility and the administrative management utilities (SLManager and MMC snap-ins).	5 minutes

5.3 Java Preference, Definitions, and Values

Table 5-2 *The Java Preferences Properties Table*

Preference	Possible Values	Description	Default Value
Add application prompts for Java applications	Yes/No/Default	This preference controls whether SecureLogin detects Java application. If the preference is set to Yes or Default, as soon as 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. This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).	The default value is No.
Allow single sign-on to Java applications	Yes/No/Default	This preference controls whether SecureLogin allows single sign-on for Java applications. If the preference is set to Yes or Default, as soon as 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. This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).	The default value is Yes.

5.4 Web Preferences, Definitions, and Values

Table 5-3 *The Web Preferences Properties Table*

Preference	Possible Values	Description	Default Value
Add application prompts for Internet Explorer	**Yes**/**No**/**Default**	This preference controls the display of the Web login detection wizard and confirmation dialog box when a Web application is detected and recognized by Internet Explorer. If you select **Yes** or **Default**, the specified credentials are saved and the application is enabled for single sign-on. If you select **No**, SecureLogin skips enabling the application for SSO in this instance. You are prompted to enable the application when you launch it the next time. This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).	The default value is **Yes**.
Add application prompts for Mozilla Firefox	**Yes**/**No**/**Default**	This preference controls the display of Web login detection wizard and confirmation dialog box when a Web application is detected and recognized by Mozilla Firefox. If you select **Yes** or **Default** the specified credentials are saved and the application is enabled for single sign-on. If you select **No**, SecureLogin skips enabling the application for SSO in this instance. You are prompted to enable the application when you launch it the next time. This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).	The default value is **Yes**.

Preference	Possible Values	Description	Default Value
Add application prompts for Google Chrome	**Yes**/**No**/**Default**	This preference controls the display of Web login detection wizard and confirmation dialog box when a Web application is detected and recognized by Google Chrome. If you select **Yes** or **Default** the specified credentials are saved and the application is enabled for single sign-on. If you select **No**, SecureLogin skips enabling the application for SSO in this instance. You are prompted to enable the application when you launch it the next time. This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).	The default value is **Yes**.
Allow single sign-on to Internet Explorer	**Yes**/**No**/**Default**	This preference defines single sign-on access to Web application using Internet Explorer. If you select **Yes** or **Default** the specified credentials are saved and the application is enabled for single sign-on. If you select **No**, SecureLogin does not prompt for credentials (if none exist or are incorrect) and does not submit credentials into the application. This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).	The default value is **Yes**.
Allow single sign-on Mozilla Firefox	**Yes**/**No**/**Default**	This preference defines single sign-on access to Web application using Mozilla Firefox. If you select **Yes** or **Default** the specified credentials are saved and the application is enabled for single sign-on. If you select **No**, SecureLogin does not prompt for credentials (if none exist or are incorrect) and does not submit credentials into the application. This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).	The default value is **Yes**.

Preference	Possible Values	Description	Default Value
Allow single sign-on Google Chrome	**Yes**/**No**/**Default**	This preference defines single sign-on access to Web application using Google Chrome. If you select **Yes** or **Default** the specified credentials are saved and the application is enabled for single sign-on. If you select **No**, SecureLogin does not prompt for credentials (if none exist or are incorrect) and does not submit credentials into the application. This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).	The default value is **Yes**.

5.5 Windows Preferences, Definitions, and Values

Table 5-4 *The Windows Preferences Properties Table*

Preference	Possible Values	Description	Default Value
Add application prompts for Windows applications	**Yes**/**No**/**Default**	This preference controls the display of a Windows login detection and confirmation message when a Windows application is detected and recognized. If you select **Yes** or **Default**, the specified credentials are saved and the application is enabled for single sign-on. If you select **No**, SecureLogin skips enabling the application for SSO in this instance. You are prompted to enable the application when you launch it the next time. This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).	The default value is **Yes**.
Allow single sign-on to Windows applications	**Yes**/**No**/**Default**	This preference controls the display of Windows login detection wizard and confirmation dialog box when a Windows application is detected and recognized by Mozilla Firefox. If you select **Yes** or **Default** the specified credentials are saved and the application is enabled for single sign-on. If you select **No**, SecureLogin skips enabling the application for SSO on this instance. You are prompted to enable the application when you launch it the next time. This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).	The default value is **Yes**.

6 Managing Your Passwords

SecureLogin provides the password policy functionality to enable you to effectively and efficiently manage your password.

Organizations and applications often have rules about the content of passwords, such as the required number of characters and type of characters. The **Password Policies** option in SecureLogin, the SecureLogin Client Utility provides functionality to create and enforce these password rules through a Password policy, and apply this policy to one or more application logins.

6.1 Creating a Password Policy

1. Double-click the SecureLogin icon in the notification area.
2. Click **Password Policies**, then click 

.
3. Specify a name for your password policy, then click **OK**.

   You have now successfully created a new password policy. Now, set your preferences for the password policy. These preferences are unique to you and are enforced on your workstation.
4. In the **Password Policies** navigation area, select the password policy you want to edit.
5. You can view and change the following settings:

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.

Policy	Value To Be provided	Description
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.
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 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 are non-sequential. If this option is set to **Yes, case insensitive**, sequential characters in different cases are disallowed.

Policy	Value To Be provided	Description
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.
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 other policies that specify the first character of the password.
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.

Policy	Value To Be provided	Description
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.
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.

6 Click Apply. The settings are saved.

6.2 Editing a Password Policy

To edit an existing password policy settings:

1 Double-click the SecureLogin icon in the notification area.

2 In the Password Policies navigation area, select the password policy you want to edit. The settings of the selected password policy are displayed.

3 Select the setting you want to change.

4 In the adjacent column, change the value of the settings as required. Refer to Section 6.1, “Creating a Password Policy,” on page 29 for the setting options and their descriptions.

5 Click Apply.

6.3 Deleting a Password Policy

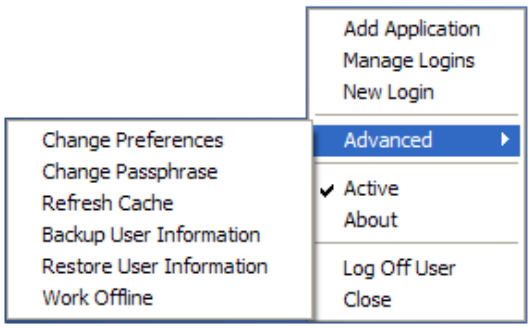
1 Double-click the SecureLogin icon in the notification area.

2 In the Password Policies navigation area, right-click the password policy you want to delete, then click Delete.

7 Managing Information Cache

Use the **Advanced** menu to change your information cache to refresh the cache, back up and restore information, and work online or offline.

Figure 7-1 *The Advanced Menu*



7.1 Refreshing the Cache

The SecureLogin cache is encrypted local copy of SecureLogin data. It allows users who are not connected to the network, for example, if they are working offline or using a laptop, to continue using SecureLogin even if the directory is unavailable.

By default, a cache file is created on the workstation as part of the SecureLogin installation. The cache file stores your data locally and is synchronized regularly with your data in the directory.

The directory and workstation caches are synchronized regularly, by default every five minutes.

To refresh the cache manually:

1 Right-click in the notification area, and select **Advanced** > **Refresh Cache**.

The cache is refreshed and it is synchronized with the cache in the directory.

7.2 Backing Up User Information

Because SecureLogin data is stored in the directory, existing directory backups also back up SecureLogin data. In addition, the local cache synchronizes with the directory for further redundancy of data.

Backing up or restoring by using the SecureLogin menu options is typically performed by users who have been disconnected from the network for long periods of time, such as weeks or months.

To create a backup file:

1. In the notification area, right-click the SecureLogin icon, then select **Advanced** > **Backup User Information**.
2. Select a folder where you want to store the backup file.

   The file can be stored in any location.
3. In the **File name** field, specify a name for the backup file.
4. Click **Save**. The Password dialog box is displayed.
5. In the **Password** field, specify a password.
6. Click **OK**.

   The encrypted and password-protected backup file is saved, and a confirmation message appears.
7. Click **OK**.

7.3 Restoring User Information

IMPORTANT: Before restoring the backup file, you must delete the cache file on the workstation.

7.3.1 Deleting the Workstation Cache

1. Right-click the Windows **Start** button, then click **Explore**.
2. Browse to the following directory:

   `C:\Documents and Settings\[user]\Application Data\SecureLogin\Cache`

   Select **Show hidden files and folders** in the Windows Folder Options dialog box.
3. Delete the cache directory.
4. Close Windows Explorer.

7.3.2 Restoring the Backup File

To restore the user information from the local cache backup file:

1. In the notification area, right-click the SecureLogin icon, then select **Advanced** > **Restore User Information**. The Load Settings dialog box is displayed.
2. Select the backup file.
3. Click **Open**. The Password dialog box is displayed.
4. In the **Password** field, specify the password.
5. Click **OK**.

   A message appears, confirming that cache data has been loaded to the local workstation cache.
6. Click **OK**.

7.4 Working Online and Working Offline

The **Work Offline** option stops the synchronization process with the directory, so SecureLogin relies only on its local cache file or equivalent smart card.

If this option is set to **Yes** in the Administrative Management utility by the administrator, the **Work Offline** option is not displayed on the notification area icon.

SecureLogin detects if it is online or offline and adapts its behavior accordingly.

If this option is set to either **No** or **Default**, the **Work Offline** option is displayed and accessible in on the notification area icon.

To work offline:

1. In the notification area, right-click the SecureLogin icon, then select **Advanced** > **Work Offline**.

   The synchronization process with the directory stops.

To work online:

1. In the notification area, right-click the SecureLogin icon, then select **Advanced** > **Work Online**.

   You are now working online and the synchronization with the directory is active.

8 Managing the Passphrase

Passphrases are an important security component in the implementation of SecureLogin. Passphrases are unique question and answer combinations created to verify and authenticate the identity of a user. In a directory environment, you can create passphrase questions for users. Users can select one of these questions and provide an answer for it. You can also permit users to provide a question of their choice and the answer for it.

Passphrases protect user credentials from unauthorized use. For example, in a Microsoft Active Directory environment, you can potentially log in to the network by resetting the user's network password.

However, this cannot happen when you are using SecureLogin. If someone other than the actual users tries to reset the network password, SecureLogin triggers the passphrase question. The user must provide the correct answer before successfully logging in. Even an administrator cannot access the user's single sign-on-enabled applications without knowing the user's passphrase answer.

NOTE: In a Microsoft Windows Vista environment, when you log in to SecureLogin in an offline mode with an incorrect password, you are prompted to provide the passphrase answer. If an incorrect passphrase answer is specified, you are prompted to retry the authentication.

However, if you again provide a wrong password, instead of seeing a prompt for the passphrase answer, you are prompted to specify the password (that is, instead of the passphrase dialog box, the password dialog box is displayed).

Close and relaunch SecureLogin to be prompted for the password first, then prompted for the passphrase answer if the incorrect password is specified.

8.1 Creating a Passphrase

The first time log in to your workstation and launch SecureLogin, you are prompted to set up your passphrase question and answer.

If you have installed SecureLogin in the LDAP GINA mode with eDirectory, SecureLogin does not work while setting a passphrase for a new user if the eDirectory user's fully distinguished name (FDN) has 128 characters or more.

1. The Passphrase Setup dialog box is displayed.

   If your administrator has defined a set to question, you must select one of the questions and specify your answer.
2. In the **Enter a question** field, select or specify a passphrase question.
3. In the **Enter the answer** field, specify the new passphrase answer.
4. In the **Confirm the answer** field, retype the new passphrase answer.
5. Click **OK**. The changes are saved.

NOTE: You are re-prompted for the passphrase answer in the following situations:

- If your administrator has changed the **Security** preference from **Hidden** to **Yes**, you are promoted to re-enter your passphrase question and answer.
- If you have logged in through the **Workstation only** when;
  - The eDirectory™ and workstation passwords are different
  - `HKLM/Software/Protocom/ SecureLogin\TryRegcredInOffline` is set to `1`

Specify your passphrase again (after the initial set up) to continue with the login.

8.2 Changing a Passphrase

Passphrases protect your credentials from unauthorized use. For example, in an Active Directory environment, you can potentially log in to the network by resetting the user's network password. You can avoid such occurrences by using a passphrase.

However, this cannot happen if you are using a SecureLogin passphrase. If someone other than the actual user tries to reset the network, SecureLogin triggers the passphrase question. The user must provide the correct answer before successfully logging in.

Even an administrator cannot access the user's single sign-on-enabled applications without knowing the user's passphrase answer.

1. Right-click the SecureLogin icon in the notification area, then select **Advanced** > **Change Passphrase**. The Passphrase dialog box is displayed.
2. Specify the existing passphrase response in the field.
3. Click **OK**. The Passphrase Setup dialog box is displayed.
4. In the **Enter a question field**, select or specify a passphrase question.
5. In the **Enter the answer field**, specify the new passphrase answer.
6. In the **Confirm the answer** field, retype the new passphrase answer.
7. Click **OK**. The changes are saved.

NOTE: If you do not have access to the SecureLogin icon in the notification area, you cannot change your passphrase answer. You administrator has disabled access to the SecureLogin icon in the notification area.