

SecureLogin CE 24.3 (v9.2)

Overview Guide

April, 2024

Legal Notice

Copyright 2009 - 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see <https://www.microfocus.com/en-us/> (<https://www.microfocus.com/en-us/>).

Contents

| | |
|---|-----------|
| About This Guide | 5 |
| 1 About SecureLogin | 7 |
| 2 SecureLogin Interface | 9 |
| 2.1 SecureLogin Client Utility | 9 |
| 2.2 Administrative Management Utilities | 10 |
| 2.2.1 SLManager | 10 |
| 2.2.2 Microsoft Management Console Snap-In | 10 |
| 2.3 SecureLogin Icon | 11 |
| 2.4 Application Types and Descriptions | 12 |
| 2.5 The Applications Pane | 13 |
| 2.5.1 The Details Tab | 14 |
| 2.5.2 The Definition Tab | 14 |
| 2.5.3 The Settings Tab | 15 |
| 2.6 The Logins Pane | 15 |
| 2.7 The Preferences Properties Table | 16 |
| 2.7.1 Configuring Preferences Introduced In SecureLogin Version 6 | 16 |
| 2.8 The Password Policy Properties Table | 31 |
| 2.9 The Advanced Settings Pane | 34 |
| 2.10 The Passphrase Policy Properties Table | 36 |
| 2.11 The Distribution Pane | 40 |
| 3 SecureLogin Components | 41 |
| 3.1 SecureLogin Management Utilities | 41 |
| 3.2 Application Definition Wizard | 42 |
| 3.3 Add New Login Wizard | 43 |
| 3.4 Terminal Launcher | 43 |
| 4 Enabling Applications and Websites for Single Sign-On | 45 |
| 4.1 Applications Excluded for SSO | 46 |
| 4.1.1 Modifying the List | 46 |
| 5 Operational Environment | 49 |
| 5.1 Supported Environments | 49 |
| 5.2 Windows | 49 |
| 5.3 Terminal Emulators | 50 |
| 5.4 Web or Internet | 51 |
| Glossary | 53 |

About This Guide

This guide provides an overview of SecureLogin, its features, and its components.

Additional Documentation

For the latest version of SecureLogin guides, see the [SecureLogin Documentation](#) portal.

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.

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

1 About SecureLogin

In large enterprises and organizations, employees require to interact with multiple applications and access sensitive information. Each application has its authentication methods. Users need to manage different user names and passwords for each application, which is inconvenient and difficult.

A solution is needed to help users avoid remembering numerous passwords while simultaneously providing users access to the required sensitive data without compromising the security.

SecureLogin is a single sign-on (SSO) product that provides this kind of ease for password management. SecureLogin utilities and components enable SSO for Windows, web, Java, and terminal emulator applications.

In addition to username and password authentication, it supports multi-factor authentication, such as smart card, token, or biometric authentication at the network and application levels.

It also supports SSO to enterprise workstations and applications from Azure Active Directory. The **SecureLogin Advanced Edition** component serves this purpose. This feature extends advanced capabilities such as public cloud adoption, hybrid deployments, and multi endpoint support. For more information, see [SecureLogin CE 24.3 \(v9.2\) Advanced Edition Installation and Configuration Guide](#).

SecureLogin has the following features:

- ♦ 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 SSO details and, if permitted, enable SSO applications.
- ♦ Eliminates the requirement for users to remember multiple user names and passwords beyond their initial login. It stores user names and passwords and automatically specifies them for users when required. Users do not need to remember and manually provide their credentials to log in to an application.
- ♦ Quickly retrieves and specifies user credentials, which results in faster login.
- ♦ Helps reduce Help Desk calls for locked accounts and forgotten user names and passwords.
- ♦ Makes use of multiple integrated security systems that provide authentication and SSO 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.

- ♦ Stores and encrypts user credentials in the directory: eDirectory, Active Directory, or other LDAP-compliant directories. It optionally caches them in an encrypted format on the local workstation.

With this level of encryption, no one can 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.

- ♦ Client Login Extension provides password recovery for network login credentials. The password recovery support through Client Login Extension tool is also available for locked workstations and for workstations in which user operations are controlled by Desktop Automation Services (DAS).
- ♦ Provides fault tolerance by using the following methods:
 - ♦ Local encrypted caching: To ensure that the network downtime does not affect SSO performance. If the corporate network is down, caching enables application logins to continue uninterrupted.
 - ♦ Application definitions: To cater to different login conditions and errors during the login.

It maintains SSO integrity for all mobile and remote users by locally encrypting the cache regardless of the network connectivity. If permitted, mobile users can update their SSO credentials when they are disconnected from the network and update the directory with these details when they attach later.

SecureLogin is a directory-enabled product and enables users to perform the following actions:

- ♦ 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.
- ♦ 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.
- ♦ Use a shared, kiosk-type workstation securely where many people log in temporarily for quick work, then log out.

2 SecureLogin Interface

In this Chapter

- ♦ [SecureLogin Client Utility](#)
- ♦ [Administrative Management Utilities](#)
- ♦ [SecureLogin Icon](#)
- ♦ [Application Types and Descriptions](#)
- ♦ [The Applications Pane](#)
- ♦ [The Logins Pane](#)
- ♦ [The Preferences Properties Table](#)
- ♦ [The Password Policy Properties Table](#)
- ♦ [The Advanced Settings Pane](#)
- ♦ [The Passphrase Policy Properties Table](#)
- ♦ [The Distribution Pane](#)

2.1 SecureLogin Client Utility

SecureLogin Client 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.

The navigation tree in the left pane contains the following items:

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

Changes made by using SecureLogin Client Utility on the local workstation apply only to the currently logged-in user's single sign-on (SSO) and they override the settings made in the directory.

SecureLogin Client Utility is used for the following activities:

- ♦ Providing the users with the capability to configure the SecureLogin environment and view their credentials.
- ♦ Testing SecureLogin configuration before mass deployment.
- ♦ Creating and modifying the application definitions for testing.
- ♦ Managing credentials and applications when installed in Standalone mode.
- ♦ Troubleshooting.

For more information, see the [NetIQ SecureLogin CE 24.3 \(v9.2\) Administration Guide](#).

2.2 Administrative Management Utilities

SecureLogin consists of an administrative management utility and plug-ins for integration with NetIQ and Microsoft directory management utilities.

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

IMPORTANT: The NetIQ iManager product is discontinued and reached end-of-life. Therefore, SecureLogin has stopped the iManager support. If eDirectory is deployed as part of OES deployment, refer to the OES support cycle of iManager.

It is recommended to use SLManager in place of iManager for administering SecureLogin. Limitations of SLManager over iManager: SLManager does not support concurrent connections and configured groups.

For any references of iManager on previous versions of NetIQ SecureLogin, see [NetIQ SecureLogin 8.8 Documentation](#).


The following are the directory administration tools:

- ♦ [SLManager](#)
- ♦ [Microsoft Management Console Snap-In](#)

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

2.2.1 SLManager

- 1 Click **Start > Programs > SecureLogin > SecureLogin Manager**.
- 2 In **Object**, select the object or specify the full DN of the user object, container, or 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.

2.2.2 Microsoft Management Console Snap-In




Use the Microsoft Management Console (MMC) snap-in for Active Directory deployments.

- 1 On the Windows **Start** menu, click **Programs > Administrative Tools > Active Directory Users and Computers**.
- 2 Browse or search for the desired directory object and open its properties. A new tab with the SecureLogin icon is displayed. Use this tab to configure SecureLogin information for this object.

2.3 SecureLogin Icon

The SecureLogin icon appears on the workstation's notification area (system tray) and provides quick access to common functions in the management utilities and wizards. When you click the icon, the list of applications available for SSO is displayed.

Table 2-1 SecureLogin Icon Status

| Scenario | Icon |
|--|---|
| SecureLogin is active. |  |
| SecureLogin is inactive. |  |
| NOTE: In this case, SecureLogin does not perform SSO functions, such as decrypting and passing credentials to applications. | |
| SecureLogin caches applications |  |

The following are the options available when you right-click the SecureLogin icon in the system tray:

Table 2-2 SecureLogin Icon Menu Options

| Option | Function |
|------------------------|--|
| Add Application | Launches the Add Application Wizard. |
| Manage Logins | Launches SecureLogin Client Utility. |
| New Login | Launches the Add New Login Wizard. |
| Advanced | Has some advanced SecureLogin management options. See Table 2-3 on page 11 . |
| Active | Displays a check (✓) mark when SecureLogin is active on the workstation. |
| About | Displays information about SecureLogin and your system. |
| Log Off User | Allows to shut down all programs including SecureLogin, and log out a user from the workstation. |
| Close | Closes SecureLogin on the workstation. |

The following are the options available in the **Advanced** menu:

Table 2-3 SecureLogin Advanced Menu Options







| Option | Function |
|---------------------------|---|
| Change Preferences | Launches SecureLogin Client Utility with the Preferences properties table displayed. |
| Change Passphrase | Displays the Passphrase window and enables users to change their passphrase answers. |

| Option | Function |
|----------------------------|---|
| Refresh Cache | Executes the synchronization of data between the local cache and directory data manually. |
| Backup User Information | Enables a user to backup the SecureLogin information to an encrypted XML file. The backup can include applications, credentials, and settings that are defined for the currently logged in user. |
| Restore User Information | Allows the restoration of a user's SecureLogin information from an encrypted XML file generated with the Backup User Information option. |
| Work Offline / Work Online | Toggles between offline and online network access. Displays whether a user is connected to the network or not. NOTE: This is not displayed in the standalone mode. |

2.4 Application Types and Descriptions



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

Table 2-4 Application Types and Description

| Icon | Application Type | Description |
|---|-------------------|--|
|  | Generic | The name of the application executable. |
|  | Java | <ul style="list-style-type: none"> ♦ The web page URL containing the JavaScript login. For example, <code>http://javaboutique.internet.com/KiserPassword</code>. ♦ The class name of the application (if it is a stand-alone Java application). |
|  | Startup | This must be configured in the application definition editor. For more information, see the NetIQ SecureLogin CE 24.3 (v9.2) Application Definition Guide . |
|  | Terminal Emulator | The name of the emulator. For example, <code>PLAY3270.A3D</code> . |
|  | Web | <p>All or part of the URL of the web page or an application. The name can apply to an entire website or a specific web page.</p> <p>For example, the domain name <code>www.novell.com</code> activates SecureLogin application definition on any page on the NetIQ website. Alternatively, <code>www.novell.com/</code> activates the application definition solely on the specified web page.</p> |
|  | Windows | The ID of the application that will define whether the application definition applies to the .Net or Windows executable. For example, the Windows executable displays the ID as <code>notepad.exe</code> and the .Net application displays the ID as <code>notepad</code> . |

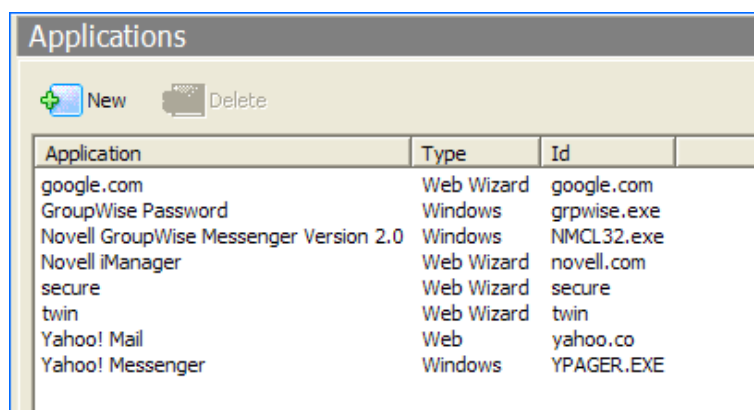
The following table describes the application details icons as available in SecureLogin Manager:

Table 2-5 Application Details

| Icon | Description |
|---|--|
|  | Indicates that the application definition is inherited from some other object in the directory. For example the users organization unit. |
|  | An application definition or a predefined application that is not inherited from a higher-level object. |

2.5 The Applications Pane

Figure 2-1 The Applications Pane in SecureLogin Manager



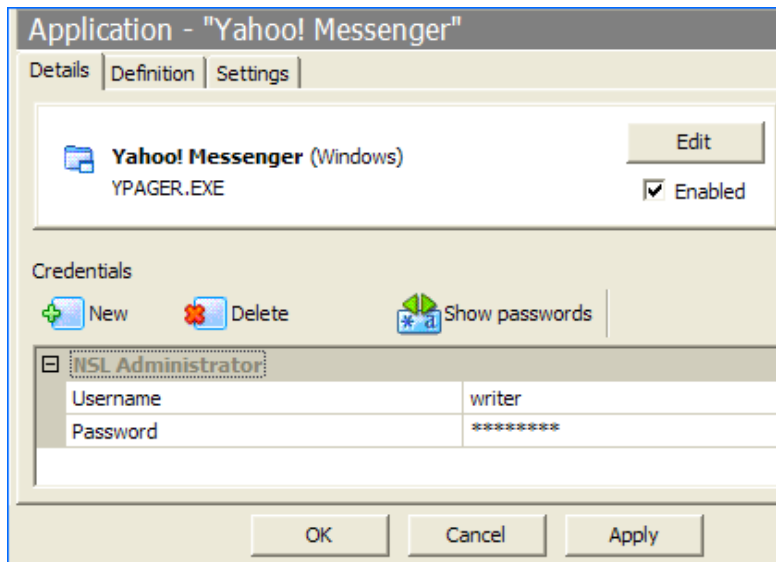
From the applications pane, users can create and modify SecureLogin application definitions that enable SSO. For details, see the [NetIQ SecureLogin CE 24.3 \(v9.2\) Application Definition Guide](#).

To display a specific application, double-click an application in the navigation tree or in the Application pane. The Application pane contains the following tabs:

- ♦ [The Details Tab](#)
- ♦ [The Definition Tab](#)
- ♦ [The Settings Tab](#)

2.5.1 The Details Tab

Figure 2-2 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 SecureLogin or the name specified by the user.
- Identity of the Application. The identity differs depending on the application definition type (.NET type, JAVA class name, URL or application name).
- The credentials (login) linked to the application and tools to create, edit, and delete these credentials.

2.5.2 The Definition Tab

The Definition tab contains the application definition. An application definition directs how SecureLogin responds to various screens (dialog boxes, web pages, etc.) returned by the application. The details displayed vary depending on the type of application definition. For applications generated by the SecureLogin add application wizard the wizard details and parameters will be displayed. For pre-built, converted wizard, or manually created definitions, the application script will be displayed.

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.

2.5.3 The Settings Tab

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

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

Table 2-6 Settings for the Windows Applications

| Item | Description |
|--|---|
| 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 re-authenticate against an advanced authentication device. For example a smart card. |

The following table describes the settings for web applications:

Table 2-7 Settings for Web Applications

| Item | Description |
|--|---|
| Allow web page to load while Application Definition is running (Web applications only) | <p>This applies to Microsoft Internet Explorer and the application definitions created for web pages and JavaScript logins that are executed in a web page.</p> <p>By default, this option is set to No. This suspends the completion of any other Internet Explorer tasks until the login is completed.</p> <p>If this option is set to Yes, then the Internet Explorer continues to function while SecureLogin is executing the login.</p> |
| Password field must exist on Internet Explorer page for Application Definition to run (Web applications only) | <p>This applies to the Microsoft Internet Explorer and application definitions created for the web pages and JavaScripts within the web pages.</p> <p>If Yes is selected, it ensures that SecureLogin does not execute the automated login on pages without the password field.</p> <p>If No is selected, SecureLogin will continually scan all pages when loaded regardless of whether there is a password field or not. This allows for the ability to script for automation of status messages or other user related activities. For example, a change password successful or failure message.</p> |

2.6 The Logins Pane

The **My Logins** pane in SecureLogin Client 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.

2.7 The Preferences Properties Table

The **Preferences** properties table provides settings to configure the parameters of the user's SecureLogin environment. This table includes the applications that are permitted to be enabled for SSO and includes access to SecureLogin management and administration tools.

For information about various preferences available for SecureLogin Client Utility and SecureLogin Manager, see [Table 2-9](#) to [Table 2-13](#).

2.7.1 Configuring Preferences Introduced In SecureLogin Version 6

Prior to configuring preferences, see [Configuration Tasks Before Deploying SecureLogin](#) in the *NetIQ SecureLogin CE 24.3 (v9.2) Administration Guide* for important information regarding SecureLogin functionality using different datastore versions.

SecureLogin provides many security features and preferences, including storage of SSO credentials on the user's smart card, encryption of the data store using Public Key Infrastructure (PKI)-based credentials, and support for the Advanced Encryption Standard (AES) encryption algorithm.

Viewing and modifying application definitions

Preferences are displayed in the right pane when **Preferences** is clicked in the Management utility. Click the plus (+) icon next to the names of the preferences to expand the preference options.

In previous versions of 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 SecureLogin to the latest version, if you are using the legacy directory data (that is, data from 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 the latest SecureLogin 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.

Preferences has the following categories:

- ♦ [Table 2-8, “The .Net Preferences,” on page 17](#)
- ♦ [Table 2-9, “The General Preferences Properties Table,” on page 18](#)
- ♦ [Table 2-10, “The Java Preferences Properties Table,” on page 27](#)
- ♦ [Table 2-11, “The Web Preferences Properties Table,” on page 28](#)
- ♦ [Table 2-12, “The Windows Preferences Properties Table,” on page 30](#)

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

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

NOTE: The **Security** preferences are not available in SecureLogin Client Utility.

Table 2-8 *The .Net Preferences*

| Preference | Possible Values | Description | Default Value |
|---|-----------------|---|---------------|
| Allow single sign-on to WindowsAutomation (DotNet) applications | Yes/No/Default | This preference allows SSO to .Net applications. If this preference is set to No then, the application will not be available for SSO. | Yes |
| Add application prompts for WindowsAutomation (DotNet) applications | Yes/No/Default | This preference prompts to add a .Net application for defining the application definition. If this preference is set to No then, the Add Application window is not launched when you launch any .Net application. | Yes |
| Start the WindowsAutomation (DotNet) monitor/automation worker | Yes/No/Default | This preference will start the DotNetSSO process. The Start the WindowsAutomation (DotNet) monitor/automation worker preference replaces the DISABLE_DOTNETSSO registry setting. | Yes |

Table 2-9 The General Preferences Properties Table

| Preference | Possible Values | Description | Default Value |
|--|-----------------|--|---------------|
| Allow "Close" option via system tray | Yes/No/Default | <p>This preference controls whether users can access the Close option from SecureLogin icon on the notification area (system tray).</p> <p>If the option is set to No, the Close option is shown as disabled in the SecureLogin notification area (system tray) icon.</p> <p>If this option is set to Yes or Default, the Close option is displayed and accessible in the SecureLogin notification area (system tray) icon.</p> <p>NOTE: This preference requires SecureLogin 6.0 datastore if the value is changed.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Allow "Refresh Cache" option via system tray | Yes/No/Default | <p>This preference controls whether users can refresh cache using the Advanced > Refresh Cache option from the SecureLogin icon on the notification area (system tray).</p> <p>If this option is set to Yes, the Refresh Cache option is displayed and accessible in the notification area (system tray) icon.</p> <p>If this option is set to No or Default, the Refresh Cache option is not displayed in the notification area (system tray) icon.</p> <p>NOTE: This preference requires SecureLogin 6.0 datastore if the value is changed.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | No |
| Allow "Log Off" option via system tray | Yes/No/Default | <p>This preference controls if users can log out from a session using Log Off User option from the SecureLogin icon on the notification area (system tray).</p> <p>If this option is set to No, the Log Off User option is not displayed and accessible in the SecureLogin notification area (system tray) icon.</p> <p>If this option is set to Yes or Default, the Log Off User option is displayed and accessible in the SecureLogin notification area (system tray) icon.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |

| Preference | Possible Values | Description | Default Value |
|--|-----------------|---|---------------|
| Allow "Work Offline" option via system tray | Yes/No/Default | <p>This preference controls whether users can work in offline cache mode using the Advanced > Work Offline option.</p> <p>If this option is set to Yes or Default, the Work Offline option is displayed in the notification area (system tray) icon.</p> <p>If this option is set to No, the Work Offline option is not displayed in the notification area (system tray) icon.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Allow application definition to be modified by users | Yes/No/Default | <p>This preference controls whether users can modify application definitions using the Definitions tabs in the Applications pane of the SecureLogin Client Utility.</p> <p>If this option is set to Yes or Default, the end user can view and modify their application definitions.</p> <p>If this option is set to No, the end user cannot change their application definitions.</p> <p>NOTE: If the Allow application definition to be viewed by users is set to No, then this option is cannot be edited.</p> <p>Disabling this preference does not disable the users from creating new applications through the wizards.</p> <p>This preference requires SecureLogin 6.0 datastore if the value is changed.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Allow application definition to be viewed by users | Yes/No/Default | <p>This preference controls whether users can view application definitions using the Definitions tabs in the Applications pane of the SecureLogin Client Utility.</p> <p>If this option is set to Yes or Default, users can view the application definition.</p> <p>If this option is set to No, users cannot view the application definition.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |

| Preference | Possible Values | Description | Default Value |
|---|-----------------|---|---------------|
| Allow credentials to be deleted by users through the GUI | Yes/No/Default | <p>This preference controls whether users can delete their credentials using the SecureLogin Client Utility available from Manage Logins from the SecureLogin icon in the notification area (system tray).</p> <p>NOTE: If Allow credentials to be modified by users through the GUI is set to No, then this option is automatically set to No and not editable.</p> <p>This preference requires SecureLogin 6.0 datastore if the value is changed.</p> <p>If this option is set to Yes or Default, users can delete their credentials through the GUI.</p> <p>If this option is set to No, users cannot delete their credentials.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Allow credentials to be modified by users through the GUI | Yes/No/Default | <p>This preference controls whether users can modify their credentials using the SecureLogin Client Utility available from Manage Logins from the SecureLogin icon in the notification area (system tray).</p> <p>If this option is set to Yes or Default, users can modify their credentials through the GUI.</p> <p>If this option is set to No, users cannot modify their credentials through the GUI. They can only view the credentials.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |

| Preference | Possible Values | Description | Default Value |
|--|-----------------|--|---------------|
| Allow users to (de) activate SSO via system tray | Yes/No/Default | <p>This preference controls whether users can activate or deactivate SecureLogin through the SecureLogin icon in the notification area (system tray).</p> <p>If this option is set to Yes or Default, users can switch between active and inactive modes of SecureLogin.</p> <p>If this option is set to No, users cannot switch between active and inactive modes.</p> <ul style="list-style-type: none"> ♦ If SecureLogin status was active when this preference was applied, it remains as active and the user cannot de-activate SecureLogin. ♦ If SecureLogin status was inactive when this preference was applied, it remains as inactive and the user cannot change SecureLogin status to Active. <p>This preference requires SecureLogin 6.0 datastore if the value is changed.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Allow users to backup/restore | Yes/No/Default | <p>This preference controls whether users can backup and restore their information from the Advanced menu of the SecureLogin icon on the notification area (system tray).</p> <p>If this option is set to Yes or Default, users can back up and restore their SSO information.</p> <p>If this option is set to No, users cannot back up and restore their SSO configuration.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Allow users to change passphrase | Yes/No/Default | <p>This preference controls whether users can change their passphrase question and answer. The Change Passphrase option is available from the Advanced menu of the SecureLogin icon on the notification area (system tray).</p> <p>If this option is set to Yes or Default, users can change their passphrase through the notification area (system tray) icon.</p> <p>If this option is set to No, users cannot change their passphrase through the notification area (system tray) icon.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |

| Preference | Possible Values | Description | Default Value |
|--|-----------------|--|---------------|
| Allow users to modify names of Applications and Logins | Yes/No/Default | <p>This preference controls whether users can edit the names of their Application login credentials using the Details tab > Edit function in the SecureLogin Client Utility.</p> <p>If this option is set to Yes or Default, the user can edit the names of their credentials (either by right-clicking on the credential and selecting Rename, or by a slow double-click on the credential name).</p> <p>If this option is set to No, the use cannot edit the names of the credentials.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | No |
| Allow users to view and change Preferences | Yes/No/Default | <p>This preference controls whether users can view and update their preferences.</p> <p>If this option is set to Yes or Default, users can view and change their preferences.</p> <p>If this option is set to No, users cannot view and change their preferences.</p> <p>NOTE: Create a separate ou for administrators to ensure that they are not adversely affected by the general user configuration preferences at the ou level.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Allow users to view and modify API preferences | Yes/No/Default | <p>This preference controls whether users can view and modify API options using the Preferences pane of the SecureLogin Client Utility.</p> <p>The API preference defines the following options for users to:</p> <ul style="list-style-type: none"> ♦ Enter an API license key(s). ♦ Provide API access. <p>If this option is set to Yes or Default users can view and modify the API preference.</p> <p>If this option is set to No, users cannot view and modify the API preference.</p> <p>NOTE: This preference affects what is displayed in the SecureLogin Client Utility using Change Preferences from the Advanced menu.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |

| Preference | Possible Values | Description | Default Value |
|--|-----------------|---|---------------|
| Allow users to view passwords | Yes/No/Default | <p>This preference controls whether users can view their passwords using Show Passwords in the Application pane > Details of the SecureLogin Client Utility.</p> <p>If this option is set to Yes or Default, users can view their passwords.</p> <p>If this option is set to No, users cannot view their passwords.</p> <p>NOTE: Allowing users to view their passwords gives them an opportunity to view and record passwords if they need to reset the SecureLogin configuration.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Change the cache refresh interval (in minutes) | 5 | <p>This preference defines the time in minutes the synchronization of user data and directory on the local workstation.</p> <p>This preference is available in both the SecureLogin Client Utility and the administrative management utilities (SLManager and MMC snap-ins).</p> | 5 minutes |
| Detect incorrect passwords | Yes/No/Default | <p>Predefined applications generally include commands to respond to incorrect password dialogs. This preference enables SecureLogin to respond to incorrect passwords for web applications. SecureLogin will monitor the time period between successive attempts to enter the credential information into the same application. If the time period is too short SecureLogin assumes that the login is failing due to bad credentials.</p> <p>If this option is set to Yes or Default, incorrect passwords for web applications are detected.</p> <p>If this option is set to No, incorrect passwords for web applications are not detected.</p> <p>This preference is available in both SecureLogin Client Utility and administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Disable single sign-on | Yes/No/Default | <p>This preference controls the users access to running SecureLogin.</p> <p>If this option is set to Yes, access to SecureLogin is disabled and it will not start when run either automatically at startup or when run manually.</p> <p>If this option is set to No or Default, access to SecureLogin is enabled and will start normally.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | No |

| Preference | Possible Values | Description | Default Value |
|----------------------------------|-----------------|--|---------------|
| Display splash screen on startup | Yes/No/Default | <p>This preference controls the display of the SecureLogin splash screen during startup.</p> <p>If this option is set to Yes or Default, the splash screen appears when SecureLogin startup.</p> <p>If this option is set to No, the splash screen is hidden and users cannot see the splash screen when SecureLogin startup.</p> <p>NOTE: This preference requires SecureLogin 6.0 datastore if the value is changed.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Display the system tray icon | Yes/No/Default | <p>This preference controls the display of SecureLogin icon in the notification area (system tray).</p> <p>If this option is set to Yes or Default, the SecureLogin icon appears on the notification area (system tray).</p> <p>If this option is set to No, the SecureLogin icon does not appear on the notification area (system tray).</p> <p>NOTE: When the SecureLogin icon is visible, users can double-click the icon on the notification area (system tray) to launch the SecureLogin Client Utility.</p> <p>When the SecureLogin is not visible, users can start the SecureLogin Client Utility through Start > Programs > SecureLogin > SecureLogin</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Enable cache file | Yes/No/Default | <p>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.</p> <p>Set this option to Yes or Default, the cache file is saved on the local workstation in the directory that was specified during install.</p> <p>Users with roaming profiles should always have this setting as Yes.</p> <p>Set this option to No if you cannot store cache files locally or if this causes conflicts with your organizational security policy.</p> <p>This preference is available in both the SecureLogin Client Utility and the administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |

| Preference | Possible Values | Description | Default Value |
|---|-----------------|---|---------------|
| Enable logging to Windows Event log | Yes/No/Default | <p>This preference controls sending the log events to Windows Event Log.</p> <p>If set to Yes or Default, log events are sent automatically to Windows Event Log.</p> <p>If set to No, the log events are not sent to Windows Event Log.</p> <p>Only the following events are logged:</p> <ul style="list-style-type: none"> ♦ SSO client started ♦ SSO client exited ♦ SSO client activated by user ♦ SSO client deactivated by user ♦ Password provided to an application by a script ♦ Password changed by the user in response to a change password command ♦ Password changed automatically in response to a change password command. <p>NOTE: This preference requires SecureLogin 6.0 datastore if the value is changed.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Enable the New Login Wizard on the system tray icon | Yes/No/Default | <p>This preference controls whether users can create multiple logins on the same application using the New Login > Add New Login option from the SecureLogin icon on the notification area (system tray).</p> <p>When set to Yes or Default, the New Login menu option is enabled and users can create multiple logins.</p> <p>If this option is set to No, New Login menu option is disabled and users cannot create multiple logins.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Enforce passphrase use | Yes/No/Default | <p>This preference forces users to set up a passphrase question and answer when SecureLogin is launched by a user for the first time.</p> <p>If this option is set to Yes, users must complete setting up their passphrase before they proceed with any other activity on the workstation.</p> <p>When set to No or Default, users can postpone setting up the passphrase. If the users clicks Cancel or closes the dialog, then SecureLogin does not start.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | No |

| Preference | Possible Values | Description | Default Value |
|--|----------------------------|---|-----------------------------|
| Enter API license key(s) | Specify API license key(s) | <p>Specify the API license key(s) provided by SecureLogin to activate the API functionality for an application.</p> <p>You can add more than one API license key.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Specify the API license key |
| Password protect the system tray icon | Yes/No/Default | <p>This preference restricts the users from accessing the SecureLogin icon menu option (from the notification area (system tray) without their network login password.</p> <p>If this option is set to Yes, the SecureLogin icon on the notification area (system tray) is password protected.</p> <p>If this option is set to No or Default, the SecureLogin icon on the notification area (system tray) is not password protected.</p> <p>This preference is available in both the SecureLogin Client Utility and the administrative management utilities (SLManager and MMC snap-ins).</p> | No |
| Provide API Access | Yes/No/Default | <p>This preference controls the API functionality use.</p> <p>If this option is set to Yes, the API access is enabled.</p> <p>When set to No or Default, the API access is disabled.</p> <p>This preference is available in both the SecureLogin Client Utility and the administrative management utilities (SLManager and MMC snap-ins).</p> | No |
| Stop walking here | Yes/No/Default | <p>This preference controls the inheritance of settings from higher level containers or organizational units.</p> <p>If this option is set to Yes, the inheritance of settings from higher level containers or organizational units is disabled.</p> <p>Set the option to Yes during phased upgrades when higher levels might have a different version of SecureLogin implemented.</p> <p>If this option is set to No or Default, the inheritance of settings from higher level containers or organizational units is enabled.</p> <p>This preference does not apply when SecureLogin is installed in eDirectory environment. The Corporate redirection functionality; that is, the inheritance settings from higher level container or organizational units is bypassed in an eDirectory environment.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | No |

| Preference | Possible Values | Description | Default Value |
|-------------|---------------------------------|---|---------------|
| Wizard mode | Administrator/ User/Disabled | <p>This preference controls the access to the application definition wizard.</p> <p>If this option is set to Administrator, it gives users' complete access to the application definition wizard. Users can create their own application definitions.</p> <p>If this option is set to User, users are only allowed to create new login credential sets for new applications using the auto-detection settings.</p> <p>If this option is set to Disabled, the application definition wizard is not launched.</p> <p>NOTE: This preference requires SecureLogin 6.0 datastore if the value is changed.</p> <p>This preference is available in administrative management utilities (SLManager and MMC snap-ins).</p> | Administrator |

Table 2-10 The Java Preferences Properties Table

| Preference | Possible Values | Description | Default Value |
|---|-----------------|--|---------------|
| Add application prompts for Java applications | Yes/No/Default | <p>This preference controls whether SecureLogin detects Java application.</p> <p>If the preference is set to Yes or Default, SecureLogin prompts to create a script when a Java application login page is loaded.</p> <p>If the preference is set to No, SecureLogin will not prompt when Java application login page is loaded.</p> <p>This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Allow single sign-on to Java applications | Yes/No/Default | <p>This preference controls whether SecureLogin allows SSO for Java applications.</p> <p>If the preference is set to Yes or Default, SecureLogin prompts the user to enter credentials (if none already exist), or submits existing credentials on the Java application login page.</p> <p>If this option is set to No, Java applications are not enabled for SSO.</p> <p>This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |

Table 2-11 The Web Preferences Properties Table

| Preference | Possible Values | Description | Default Value |
|---|-----------------|--|---------------|
| Add application prompts for Internet Explorer | Yes/No/Default | <p>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.</p> <p>If you select Yes or Default, the user is initially prompted to enable the application and enter the credentials for the application (if not done previously).</p> <p>NOTE: When you set the preference to Yes, the information that is displayed for the users depend on the settings of the Wizard mode preference.</p> <p>On subsequent runs of the application, the user is not prompted for credentials and SSO occurs seamlessly.</p> <p>If you select No, SecureLogin skips enabling the application for SSO, the user is never be prompted to enable the application.</p> <p>This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Add application prompts for Mozilla Firefox | Yes/No/Default | <p>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.</p> <p>NOTE: When you set the preference to Yes, the information that is displayed to the users depend on the settings of the Wizard mode preference.</p> <p>If you select Yes or Default, the user is initially prompted to enable the application and enter the credentials for the application (if not done previously). On subsequent runs of the application, the user is not prompted for credentials and SSO occurs seamlessly.</p> <p>If you select No, SecureLogin skips enabling the application for SSO to this instance. You are prompted to enable the application when you launch it the next time.</p> <p>This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |

| Preference | Possible Values | Description | Default Value |
|---|-----------------|--|---------------|
| Add application prompts for Google Chrome | Yes/No/Default | <p>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.</p> <p>If you select Yes or Default the specified credentials are saved and the application is enabled for SSO.</p> <p>If you select No, SecureLogin skips enabling the application for SSO to this instance. You are prompted to enable the application when you launch it the next time.</p> <p>This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Allow single sign-on to Internet Explorer | Yes/No/Default | <p>This preference defines SSO access to web application using Internet Explorer.</p> <p>If you select Yes or Default the specified credentials are saved and the application is enabled for SSO.</p> <p>If you select No, SecureLogin does not prompt for credentials (if none exist or are incorrect) and does not submit credentials into the application.</p> <p>This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Allow single sign-on Mozilla Firefox | Yes/No/Default | <p>This preference defines SSO access to web application using Mozilla Firefox.</p> <p>If you select Yes or Default the specified credentials are saved and the application is enabled for SSO.</p> <p>If you select No, SecureLogin does not prompt for credentials (if none exists or are incorrect) and does not submit credentials into the application.</p> <p>This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |

| Preference | Possible Values | Description | Default Value |
|------------------------------------|-----------------|--|---------------|
| Allow single sign-on Google Chrome | Yes/No/Default | <p>This preference defines SSO access to web application using Google Chrome.</p> <p>If you select Yes or Default the specified credentials are saved and the application is enabled for SSO.</p> <p>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.</p> <p>This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |

Table 2-12 The Windows Preferences Properties Table

| Preference | Possible Values | Description | Default Value |
|--|-----------------|---|---------------|
| Add application prompts for Windows applications | Yes/No/Default | <p>This preference controls the display of a Windows login detection and confirmation message when a Windows application is detected and recognized.</p> <p>If you select Yes or Default, the user is prompted to enable the application and to enter the credentials for the application (if not done previously).</p> <p>On subsequent runs of the application, the user is not prompted for credentials and SSO occurs seamlessly.</p> <p>If you select No, SecureLogin does not prompt the user to add the application for SSO skips enabling the application for SSO for this instance. You are prompted to enable SSO for subsequent runs of the application.</p> <p>This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |
| Allow single sign-on to Windows applications | Yes/No/Default | <p>This preference defines SSO access to Windows applications.</p> <p>If you select Yes or Default the specified credentials are saved and the application is enabled for SSO.</p> <p>If you select No, SecureLogin will not prompt for credentials (if none exist or are incorrect) and will not submit credentials into the application.</p> <p>This preference is available in both the SecureLogin Client Utility and all the administrative management utilities (SLManager and MMC snap-ins).</p> | Yes |

2.8 The Password Policy Properties Table

Figure 2-3 The Password Policy Properties Table

| Password Policies | |
|------------------------------------|-------------------------------------|
| Setting Description | Value |
| Minimum length | <input type="text"/> |
| Maximum length | <input type="text"/> |
| Minimum punctuation characters | <input type="text"/> |
| Maximum punctuation characters | <input type="text"/> |
| Minimum uppercase characters | <input type="text"/> |
| Maximum uppercase characters | <input type="text"/> |
| Minimum lowercase characters | <input type="text"/> |
| Maximum lowercase characters | <input type="text"/> |
| Minimum numeric characters | <input type="text"/> |
| Maximum numeric characters | <input type="text"/> |
| Disallow repeated characters | No <input type="button" value="v"/> |
| Disallow duplicate characters | No <input type="button" value="v"/> |
| Disallow sequential characters | No <input type="button" value="v"/> |
| Begins with an uppercase character | No <input type="button" value="v"/> |
| Ends with an uppercase character | No <input type="button" value="v"/> |
| Prohibited characters | <input type="text"/> |
| Begins with any character | No <input type="button" value="v"/> |
| Begins with a Number | No <input type="button" value="v"/> |
| Begins with a special character | No <input type="button" value="v"/> |
| Ends with any character | No <input type="button" value="v"/> |
| Ends with a Number | No <input type="button" value="v"/> |
| Ends with a special character | No <input type="button" value="v"/> |

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 2-13 The Password Policy Properties Table

| Policy | Value | 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. This should be a whole number. |
| Maximum punctuation characters | Punctuation characters | Defines the maximum number of punctuation characters allowed in a password. This should be a whole number. |
| 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 | <p>Disallows the use of repeated characters, or the use of the same successive characters.</p> <p>When set to No, characters can be repeated. This is the default value.</p> <p>When set to Yes, same alphabetic characters in a different cases are considered as different characters. For example, A and a are different.</p> <p>If this option is set to Yes, case insensitive, the successive use of the same alphabetic characters in a different case is not allowed.</p> |
| Disallow duplicate characters | No/Yes/Yes, case insensitive | <p>Disallows the use of the same non-successive characters.</p> <p>If this option is set to No, duplicate characters are allowed. This is the default value.</p> <p>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.</p> <p>If this option is set to Yes, case insensitive, duplication of the same alphabetic characters in a different case is not allowed.</p> |

| Policy | Value | Description |
|-----------------------------------|------------------------------|--|
| Disallow sequential characters | No/Yes/Yes, case insensitive | <p>Disallows the use of successive characters in an alphabetical order.</p> <p>If this option is set to No, sequential characters are allowed. This is the default value.</p> <p>When set to Yes, sequential characters in a different case are considered as non-sequential. For example, a and B are non-sequential.</p> <p>If this option is set to Yes, case insensitive, sequential characters in different cases is disallowed.</p> |
| Begin with an uppercase character | No/Yes | <p>Enforces the use of an uppercase alphabetic character as the beginning character of a password. The default value is No.</p> <p>When set to Yes, all other policies that indicate that a password must begin with a particular character or in a specific manner are disabled.</p> <p>IMPORTANT: Only one type of character can be designated as the first value of a password.</p> |
| End with an uppercase character | No/Yes | <p>Enforces the use of an uppercase letter at the end of a password. The default value is No.</p> <p>When set to Yes, all other policies that indicate a password must end with a specific character or in a specific manner are disabled.</p> |
| Prohibited characters | Keyboard characters | <p>Defines a list of characters that cannot be used in a password.</p> <p>NOTE: There is no need of a separator in the list of prohibited characters. For example, @#\$%&</p> |
| Begin with any Alpha character | No/Yes | <p>Enforces the use of an alphabetic character at the beginning of a password. The default value is No.</p> <p>When set to Yes, it automatically disables all other policies that specify what the first character of the password should be.</p> |
| Begin with any number | No/Yes | <p>Enforces the use of a numeric character as the first character of the password. The default value is No.</p> <p>When set to Yes, it automatically disables all other policies that specify what the first character of the password should be.</p> |
| Begin with any symbol | No/Yes | <p>Enforces the use of a symbol character as the first character of the password. The default value is No.</p> <p>When set to Yes, it automatically disables all other policies that specify what the first character of the password should be.</p> |
| End with any Alpha character | No/Yes | <p>Enforces the use of an alphabetic character as the last character of the password. The default value is No.</p> <p>If this option is set to Yes, it automatically disables all other policies that specify what the password should end with.</p> |

| Policy | Value | Description |
|---------------------|--------|---|
| 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. |

2.9 The Advanced Settings Pane

Figure 2-4 The Advanced Settings Pane with the Passphrase Option

The screenshot displays the 'SecureLogin SSO' interface with the 'Advanced Settings' tab selected. The 'Passphrase' section is active, showing a list of 'Corporate passphrase questions' (currently empty) with buttons for 'New...', 'Edit...', and 'Delete...'. Below this, the 'User-defined passphrase questions' are set to 'Default'. The 'Customized Passphrase Prompt' section has a checkbox for 'Modify the passphrase prompt window text' which is unchecked. The 'Passphrase Policy' section has a checkbox for 'Use a passphrase policy' which is also unchecked, with an 'Edit Policy' button to its right. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

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

Table 2-14 *The Advanced Settings Pane*

| Tab Name | Description |
|------------------------------|---|
| Passphrase | This page contains fields for: <ul style="list-style-type: none">♦ Creating, editing, and deleting corporate passphrase questions.♦ Customizing passphrase prompts.♦ Editing passphrase policies. |
| Datastore | This is used for: <ul style="list-style-type: none">♦ Selecting directory data version details (for mixed mode environments by using the earlier versions of the client software).♦ Deleting 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 SecureLogin environment. |

NOTE: The **Advanced Settings** option is not available in SecureLogin Client Utility.

2.10 The Passphrase Policy Properties Table

Figure 2-5 The Passphrase Policy Properties Table

| Passphrase Policy | |
|------------------------------------|-------------------------------------|
| Setting Description | Value |
| Minimum length | <input type="text"/> |
| Maximum length | <input type="text"/> |
| Minimum punctuation characters | <input type="text"/> |
| Maximum punctuation characters | <input type="text"/> |
| Minimum uppercase characters | <input type="text"/> |
| Maximum uppercase characters | <input type="text"/> |
| Minimum lowercase characters | <input type="text"/> |
| Maximum lowercase characters | <input type="text"/> |
| Minimum numeric characters | <input type="text"/> |
| Maximum numeric characters | <input type="text"/> |
| Disallow repeated characters | No <input type="button" value="v"/> |
| Disallow duplicate characters | No <input type="button" value="v"/> |
| Disallow sequential characters | No <input type="button" value="v"/> |
| Begins with an uppercase character | No <input type="button" value="v"/> |
| Ends with an uppercase character | No <input type="button" value="v"/> |
| Prohibited characters | <input type="text"/> |
| Begins with any character | No <input type="button" value="v"/> |
| Begins with a Number | No <input type="button" value="v"/> |
| Begins with a special character | No <input type="button" value="v"/> |
| Ends with any character | No <input type="button" value="v"/> |
| Ends with a Number | No <input type="button" value="v"/> |
| Ends with a special character | No <input type="button" value="v"/> |

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.

Table 2-15 The Passphrase Policy Properties Table

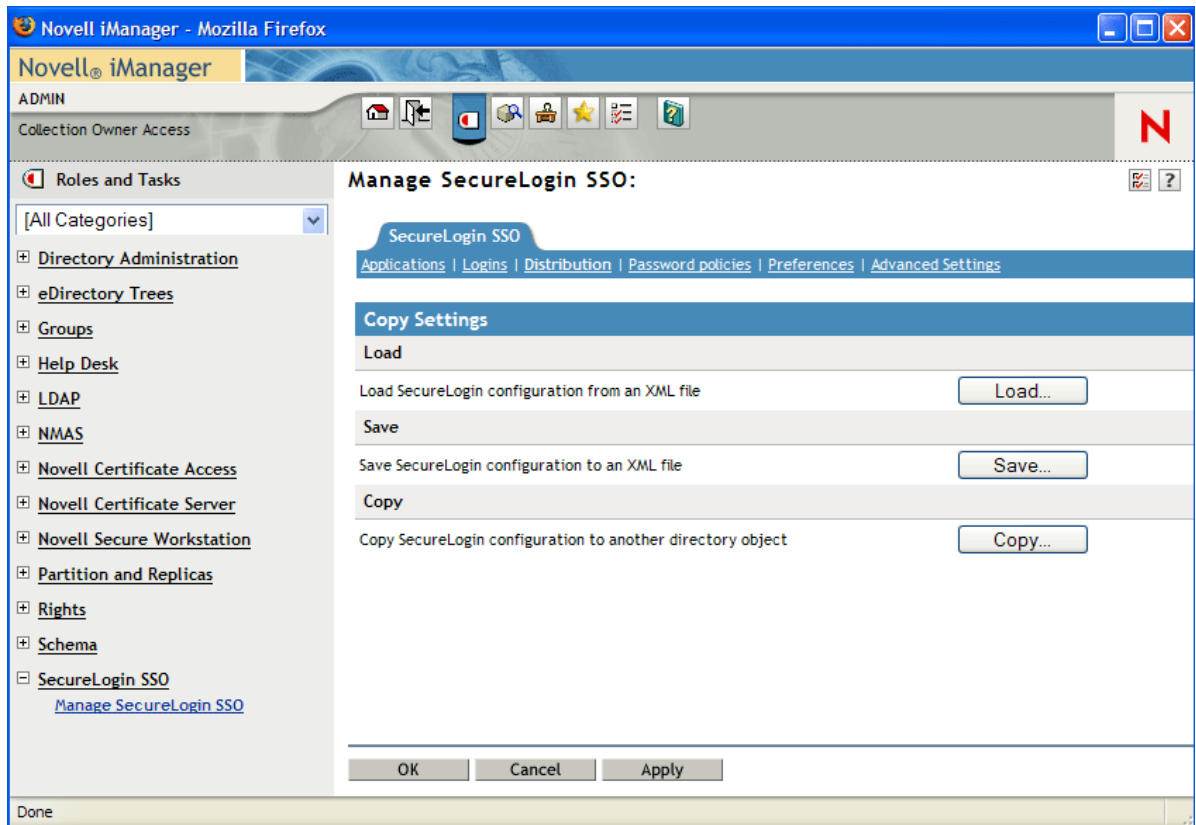
| Policy | Value | Description |
|--------------------------------|------------------------------|--|
| Minimum length | Whole number | Defines the minimum length of the passphrase. |
| Maximum length | Whole number | Defines the maximum length of the passphrase. |
| Minimum punctuation characters | 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 | <p>Disallows the use of repeated characters, or the use of the same successive characters.</p> <p>If this option is set to No, characters can be repeated. This is the default value.</p> <p>When set to Yes, the same alphabetic characters in a different case are considered as different characters. For example, A and a are different.</p> <p>If this option is set to Yes, case insensitive, the successive use of the same alphabetic characters in a different case is not allowed.</p> |
| Disallow duplicate characters | No/Yes/Yes, case insensitive | <p>Disallows the use of the same non-successive characters.</p> <p>If this option is set to No, duplicate characters are allowed. This is the default value.</p> <p>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.</p> <p>If this option is set to Yes, case insensitive, duplication of the same alphabetic characters in a different case is not allowed.</p> |

| Policy | Value | Description |
|-----------------------------------|------------------------------|---|
| Disallow sequential characters | No/Yes/Yes, case insensitive | <p>Disallows the use of successive characters in an alphabetical order.</p> <p>If this option is set to No, sequential characters are allowed. This is the default value.</p> <p>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.</p> <p>If this option is set to Yes, case insensitive, sequential characters in different cases is disallowed.</p> |
| Begin with an uppercase character | No/Yes | <p>Enforces the use of an uppercase alphabetic character as the beginning character of a passphrase.</p> <p>The default value is No.</p> <p>When set to Yes, all other policies that indicate that a passphrase must begin with a particular character or in a specific manner are disabled.</p> <p>IMPORTANT: Only one type of character can be designated as the first value of a passphrase.</p> |
| End with an uppercase character | No/Yes | <p>Enforces the use of an uppercase letter at the end of a passphrase.</p> <p>The default value is No.</p> <p>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.</p> |
| Prohibited characters | Keyboard characters | <p>Defines a list of characters that cannot be used in a passphrase.</p> <p>NOTE: There is no need of a separator in the list of prohibited characters. For example, @\$%&</p> |
| Begin with any Alpha character | No/Yes | <p>Enforces the use of an alphabetic character at the beginning of a passphrase.</p> <p>The default value is No.</p> <p>If this option is set to Yes, it automatically disables all other policies that specify what the first character of the passphrase should be.</p> |
| Begin with any number | No/Yes | <p>Enforces the use of a numeric character as the first character of the passphrase.</p> <p>The default value is No.</p> <p>If this option is set to Yes, it automatically disables all other policies that specify what the first character of the passphrase should be.</p> |

| Policy | Value | Description |
|------------------------------|--------|--|
| Begin with any symbol | No/Yes | <p>Enforces the use of a symbol character as the first character of the passphrase.</p> <p>The default value is No.</p> <p>If this option is set to Yes, it automatically disables all other policies that specify what the first character of the passphrase should be.</p> |
| End with any Alpha character | No/Yes | <p>Enforces the use of an alphabetic character as the last character of the passphrase.</p> <p>The default value is No.</p> <p>If this option is set to Yes, it automatically disables all other policies that specify what the passphrase should end with.</p> |
| End with any number | No/Yes | <p>Enforces the use of a numeric character as the last character of the passphrase.</p> <p>The default value is No.</p> <p>If this option is set to Yes, it automatically disables all other policies that specify what the passphrase should end with.</p> |
| End with any symbol | No/Yes | <p>Enforces the use of a symbol character as the last character of the passphrase.</p> <p>The default value is No.</p> <p>If this option is set to Yes, it automatically disables all other policies that specify what the passphrase should end with.</p> |

2.11 The Distribution Pane

Figure 2-6 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. For more information, see [Copying a Configuration Across Organizational Units](#)

The Copy dialog box help the administrator to copy an object's SecureLogin configuration from one object to another. For more information, see [Managing Configurations](#)

NOTE: The **Distribution** pane is not available for SecureLogin Client Utility.

3 SecureLogin Components

In this Chapter

- ♦ [SecureLogin Management Utilities](#)
- ♦ [Application Definition Wizard](#)
- ♦ [Add New Login Wizard](#)
- ♦ [Terminal Launcher](#)

3.1 SecureLogin Management Utilities

Table 3-1 SecureLogin Management Utilities

| Use This Utility | To Manage These Users |
|--|---|
| SecureLogin Manager (SLManager) | This tool can be used in any supported SecureLogin environment to globally manage SecureLogin information on user objects, groups, policies, containers, or organizational objects at the tree/domain level. |
| SecureLogin Client Utility (manage logins) | <p>The manage logins interface of the SecureLogin client allows users to modify the SecureLogin applications, credentials, and settings for the currently logged in user. This utility has similar functionality as the SecureLogin management utility, excluding some preference options that relate to only the directory environment. Administrators can disable users from accessing this utility and or limit the capabilities provided by default within this user interface.</p> <p>For example, Allow users to view application definitions set to No would restrict the user from viewing the application definition from within the client utility.</p> <p>For more information, see SecureLogin Client Utility</p> |
| MMC snap-in | This tool extends the capabilities of Microsoft Management Console (MMC) to include management of the SecureLogin information when running within an Active Directory environment. |

| Use This Utility | To Manage These Users |
|--|---|
| Active Directory Users and Computers Snap-in | <p>Using the Active Directory users and computer snap-in you can manage users in the Microsoft Active Directory environment.</p> <p>If during the installation of the SecureLogin client in Active Directory mode, the option Install Directory Administration Tools was selected, then the installation routine copies and registers the SecureLogin Snap-In for Active Directory Users and Computers. In addition to the MMC snap-in being installed, the SecureLogin Administrative Management utility is also copied to the SecureLogin program folder.</p> <p>NOTE: If you select the Enable Microsoft Active Directory Group Policies option during the installation, you can administer SecureLogin by using the Group Policy object.</p> |

3.2 Application Definition Wizard

Application definitions specify how SecureLogin interacts with an application using your single sign-on (SSO) credentials. The Application Definition Wizard assists you in creating an application definition.

IMPORTANT: You can use the Application Definition Wizard only if the administrator has given you permission. The administrator can restrict users' access to the Application Definition Wizard. Depending on the preferences set by the administrator, you might be allowed to create application definitions for new applications or you might not have access at all.

In most instances, the Application Definition Wizard opens automatically when it detects a new logon screen, but you can also choose to create or modify application definitions using the wizard to automate the handling of notification screens including prompts to change your password and error messages.

For information about using the Application Definition Wizard to create application definitions and enabling applications for SSO, see [NetIQ SecureLogin CE 24.3 \(v9.2\) Application Definition Wizard Administration Guide](#)

This wizard helps you to create and change the application definition responses for the following:

- ♦ The Login Screen
- ♦ The Login Notification Screen
- ♦ The Change Password Screen
- ♦ The Change Password Notification Screen
- ♦ Application windows or pages that are not recognized by the Application Definition Wizard automatically.

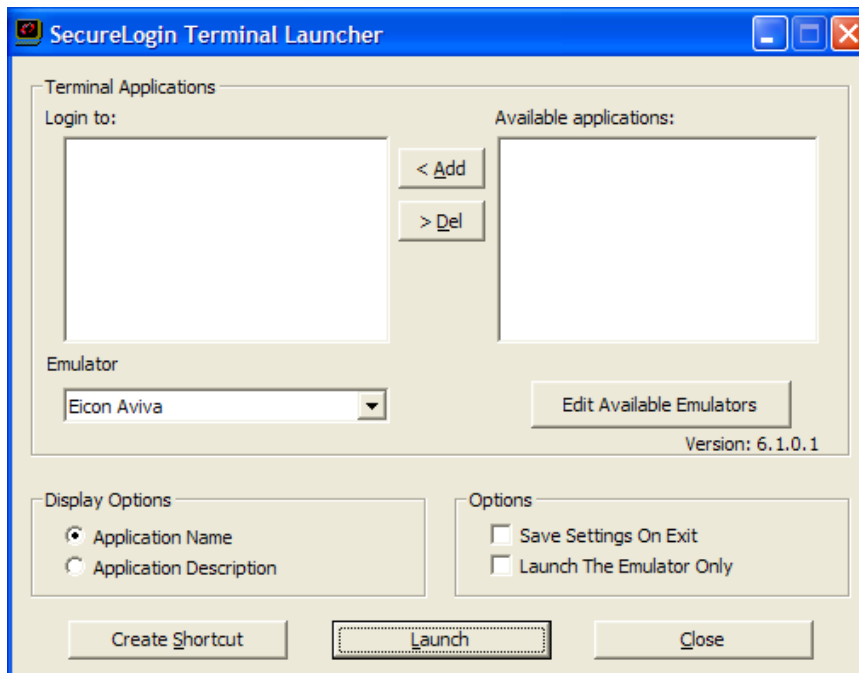
3.3 Add New Login Wizard

The Add New Login Wizard helps users to create multiple logins for the same application. The wizard contains a list of available credential sets from which users can choose the desired login.

An alternative to using the wizard to add a new login, the script commands `PickListAdd` and `PickListDisplay` can be used within an application script to prompt the user for the desired login. For example, if all users in an IT group require three different logins for a help desk application, the administrator can modify the script for the help desk application to include the `PickList` commands. This way all users of the help desk application are prompted to choose one of the three valid logins before the application login occurs.

3.4 Terminal Launcher

Figure 3-1 The Terminal Launcher



Terminal emulator application definitions are invoked by the utility called Terminal Launcher (tlaunch.exe or tlaunch64.exe). Configuration of SecureLogin to provide Single Sign-on to terminal sessions is typically implemented in one of three ways:

- Users launch the emulator via the tlaunch utility (GUI)
- A shortcut is created on the users desktop that will execute tlaunch with the correct parameters to start the emulator with the desired terminal emulator application definition.
- A windows application definition is created for the emulator executable that will invoke tlaunch with the proper parameters to connect to the emulator session and Terminal Emulator application definition

For more information about enabling SSO for terminal services, see [“Enabling Terminal Emulator Applications”](#) in the *NetIQ SecureLogin CE 24.3 (v9.2) Administration Guide*.

4 Enabling Applications and Websites for Single Sign-On

SecureLogin has predefined applications for single sign-on (SSO) access to a wide range of commercially available applications.

SecureLogin detects applications for which a predefined application exists. For example, if SecureLogin detects Novell GroupWise Messenger dialog box, then it prompts the user to allow SecureLogin to enable SSO for the application.

Predefined applications for some commonly used applications are incorporated with SecureLogin, and with each new version, more applications are developed and made available to the customers.

SecureLogin provides application definition wizard to facilitate SSO to almost any new or proprietary application, if a predefined application is unavailable. For information, see the [NetIQ SecureLogin CE 24.3 \(v9.2\) Application Definition Wizard Administration Guide](#).

SecureLogin also supports enabling SSO for terminal emulator applications.

- ♦ Users can enable SSO for terminal emulators by using the terminal launcher tool.
- ♦ SecureLogin has additional tools such as, `Window Finder` and `LoginWatch`, which help the user to enable SSO for even the most difficult applications. For information, see the [NetIQ SecureLogin CE 24.3 \(v9.2\) Application Definition Guide](#).

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 SecureLogin can enable an application for SSO 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 Identity Manager.

When a user starts an application for the first time after it is enabled for SSO, 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 SSO is achieved by using the proprietary application definitions. The application definitions are managed in directory environments through SecureLogin administrative management utilities. In local and standalone deployments, the application definitions are managed in SecureLogin Client Utility or distributed by using the advanced offline signed and encrypted method.

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

4.1 Applications Excluded for SSO

Although SecureLogin facilitates you to enable SSO for Windows, web, and Java applications; some applications cannot be enabled for SSO. The applications that cannot be enabled include certain installers, SecureLogin and Windows system files. Enabling these applications might affect your computer's performance or create a security risk.

These applications are hard-coded and are excluded from SSO.

Table 4-1 Applications excluded from SSO

| | | |
|--------------|----------------|---------------------|
| setup.exe | Nwadm95.exe | acsagent.exe |
| _isdel.exe | loginw95.exe | adamconfig.exe |
| msiexec.exe | NWTray.exe | rdbgwiz.exe |
| MSDEV.exe | loginw32.exe | ProtocomSysTray.exe |
| devenv.exe | scrnlock.scr | ac.aac.run.exe |
| SLBroker.EXE | MMC.EXE | SLBroker64.EXE |
| tlaunch.exe | slwinsso.exe | slwinsso64.exe |
| SLProto.exe | SLManager.exe | SLManager64.exe |
| nswebsso.exe | sllock.scr | tlaunch64.exe |
| Nwadm32.exe | ConsoleOne.exe | SLProto64.exe |
| Nwadmnt.exe | SLLauncher.exe | |

4.1.1 Modifying the List

Although the applications disabled for SSO are hardcoded, you can modify the behavior by creating a text file at the SecureLogin installation path. For example, at `C:\Program Files\Novell\SecureLogin\` and name it `exclude.ini`.

NOTE: Despite its extension, the `exclude.ini` file is not in an `.ini` file format.

You can open this file in any text editor and make the changes. You can extend or modify the list.

You can modify the file in the following ways:

- ♦ “Extending the List of Applications” on page 47
- ♦ “Including Applications for SSO” on page 47
- ♦ “Disabling the Default Behavior” on page 47

Extending the List of Applications

If you want to disable more applications apart from the hardcoded applications, add the names of the application to the `exclude.ini` file. For example, you can add `grpwise.exe` to the `exclude.ini` file. With this, GroupWise is also disabled for SSO.

NOTE: If you add an existing application to the list of applications in the `exclude.ini` file, it does not impact the original list. For example, if you add `SLProto.exe` to the `exclude.ini` file, it does not impact the function although it is listed twice.

Including Applications for SSO

If you want to enable only a set of applications for SSO, use `Include` keyword in `exclude.ini` file

In the `exclude.ini` file add the `Include` keyword to enable an executable for SSO. By including the `Include` keyword, the list is converted to an include list.

For example, when you add

```
Include
Trillian.exe
```

Trillian application is enabled for SSO. The next time you log in, you are prompted to enable SSO.

If you use the `include` keyword you must list all of the desired applications you want to use SecureLogin with. All other applications will be ignored. For more information, see [TID 7009238](http://www.novell.com/support/kb/doc.php?id=7009283) (<http://www.novell.com/support/kb/doc.php?id=7009283>)

Disabling the Default Behavior

If you want to define a custom list for disabling the applications for SSO, include the `NoDefault` keyword. When you include the `NoDefault` keyword, the hardcoded applications are overridden.

For example, if you modify the list as:

```
NoDefault
NMCL32.exe
```

the hardcoded applications that are disabled for SSO is not read by SecureLogin. Instead, the executables listed with the `NoDefault` keyword in the `exclude.ini` file are considered and all the applications listed in the file are disabled for SSO.

5 Operational Environment

In this Chapter

- ♦ [Supported Environments](#)
- ♦ [Windows](#)
- ♦ [Terminal Emulators](#)
- ♦ [Web or Internet](#)

5.1 Supported Environments

For supported environments and platforms, see [NetIQ SecureLogin CE 24.3 \(v9.2\) System Requirements](#).

5.2 Windows

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

- ♦ ActiveSync
- ♦ Cisco VPN
- ♦ Citrix Program Neighborhood
- ♦ Citrix Program Neighborhood - Farm Login Failure
- ♦ Citrix Program Neighborhood - Server
- ♦ Citrix Program Neighborhood - Agent
- ♦ Citrix Program Neighborhood - Agent v10.x
- ♦ GroupWise Windows Application v5.5, v6.0, v7.0, and v8.0
- ♦ Lotus Notes R8
- ♦ MEDITECH x and 4.x

NOTE: The support for MEDITECH 3.x and 4.x is dependent 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 Internet Explorer 6, 7, and 8
- ♦ Microsoft Networking Client
- ♦ Microsoft Outlook
- ♦ Microsoft Outlook Express
- ♦ Microsoft SQL
- ♦ Microsoft Windows Live ID

- ♦ MSN Messenger 4.5 and 4.7
- ♦ Novell Groupwise Messenger 2.0
- ♦ Novell Groupwise Notify Client
- ♦ Novell Groupwise 7.0 Web Login
- ♦ Quick Finder
- ♦ SAP - SAPlogon.exe
- ♦ SAP R/3 Login
- ♦ Trillian
- ♦ VNC 3.0 and 4.0
- ♦ Windows Live Messenger 5.0, 6.0, 7.5, 8.1, and 2009
- ♦ Windows Remote Desktop 6
- ♦ Yahoo! Messenger 8.1
- ♦ Yahoo! Messenger 8.1 Alternate

If SecureLogin does not prompt to enable single sign-on (SSO) for applications, use the Application Definition Wizard to build an application.

5.3 Terminal Emulators

SecureLogin provides SSO support for the applications running on any backend 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 9x
- ♦ 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
- ♦ Attachmate EXTRA X-treme
- ♦ Microsoft Telnet Vista

5.4 Web or Internet

SecureLogin provides the following sample 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

SecureLogin prompts you if a predefined application is available. You can also use the Application Definition Wizard to build an application definition for the application.

Glossary

administrative management utility. The utility available in SecureLogin to manage the users in a directory environment. The slmanagertool.exe provides additional functionality that is not available in SecureLogin Client Utility.

application programming interface. Enables programmatic communication with the application.

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

User data includes credentials, preferences, password policies, and application definitions. By default, 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. Object in a directory environment that contains other objects.

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

credentials. User names, 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 SecureLogin.

management utility. SecureLogin's management utility. It generically refers to the administrative management utilities and SecureLogin Client 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.

SecureLogin Client 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.

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

SecureLogin Attribute Provisioning (SLAP). The tool that enables 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, SecureLogin transparently manages the login process.