SecureLogin 8.5

Application Definition Wizard Administration Guide

October, 2016

Legal Notice

Contents

About This Guide 5

1 Introduction 7

What is an Application Definition? . . . 7
The Application Definition Wizard . . . 7

2 Understanding the Application Definition Wizard Interface 9

The Application Screens Pane . . . 10
Logon . . . 10
Login Notification . . . 26
Change Password . . . 34
Change Password Notification . . . 44
Other . . . 53
Attributes Pane . . . 59
General Controls and Messages . . . 59
Help . . . 60
Test . . . 60
OK . . . 60
Apply . . . 60
Cancel . . . 60
Selecting and Identifying Screens and Controls . . . 60
Recording Keystrokes . . . 61
Using Regular Expressions . . . 62

3 Using the Application Definition Wizard 63

Launching the Application Definition Wizard . . . 63
Automatically Launching the Wizard . . . 64
Launching the Wizard through the Add Application Menu . . . 64
Creating an Application Definition for a Web Application . . . 65
Prerequisites . . . 65
Using the Default Selections for an Application Definition . . . 65
Manually Defining the Attributes for an Application Definition . . . 67
Creating an Application Definition for a Windows Application . . . 74
Prerequisites . . . 74
Using the Default Selections to Create an Application Definition . . . 74
Manually Defining the Attributes for an Application Definition . . . 75
Creating an Application Definition for a Java Application or an Oracle Form . . . 82
Prerequisites . . . 82
Using the Default Selections to Create an Application Definition . . . 83
Manually Defining the Attributes for an Application Definition . . . 84
Using a Predefined Application Definition . . . 89
Using a Predefined Application Definition to Enable a Web Application for Single Sign-On . . . 90
Using a Predefined Application Definition to Enable Windows Application for Single Sign-On . . . 92
Testing Application Definitions . . . 94
Deploying Application Definitions . . . 96
Configuring Notifications . . . 96

Creating an Application Definition for Login Notification 96
Creating an Application Definition for Change Password 101
Creating an Application Definition for Change Password Notification 108

4 Modifying Application Definitions 113

Using the Application Definition Wizard to Modify an Application Definition 113
Using the Manage Logins Menu to Modify the Application Definition 115

5 Setting the Wizard Mode Preference 119

6 Deploying Application Definitions 121

7 Compatibility with Earlier Versions 123

8 Limitations, Tips, and Troubleshooting 125

Limitations 125
Support for .NET Framework 125
Support for Non-Natively Supported UI Framework 125
Defining Password Notification 126
Specifying Reauthentication Rules 126
Incorrect Login Notifications in Mozilla Firefox 126
Single Sign-On For Microsoft Windows Vista Remote Desktop Client 126
Tips 126
Detecting Multiple Controls 126
Using Dynamic Controls 128
Citrix Published Applications 128
COM Applications 128
Troubleshooting 129
Redirecting to Login Page 129
Remote Desktop Connection 131

About This Guide

This guide provides information about the interface of the Wizards, the layout of the Wizards, using the Wizards to enable applications for single sign-on.

Additional Documentation

For the latest version of SecureLogin guides, see www.netiq.com/documentation/securelogin/

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Introduction

This section contains an overview of application definition and introduces the Application Definition Wizard.

- “What is an Application Definition?” on page 7
- “The Application Definition Wizard” on page 7

What is an Application Definition?

An application definition is a set of instructions that SecureLogin follows to perform tasks on Windows applications, Java applications, or Web pages. For example, you can use an application definition to save user login credentials, so users don’t need to type a username and password every time they want to access an application.

NOTE: Throughout the document, we refer to all the Web, Windows, and Java applications as applications.

An application definition is a collection of instructions that handle multiple operations associated with credentials of the application such as login, change password, application prompts, application notifications. It contains specific instructions that allow the software client to analyze an application after it is launched and determine whether some specific actions need to be performed.

Application definitions specify how SecureLogin interacts with an application to use a single sign-on credential. SecureLogin comes with predefined application definitions for many commercial applications.

You can use the predefined application definitions or create new application definition to enable single sign-on for applications. You can also use application definitions to assign instructions for each dialog box or screen that an application displays. You can choose to define actions for a selected window, a login screen, or an entire application. Application definitions can also include commands to automate password changes on behalf of users and to request user input when required.

Application definitions are stored and secured within the directory to ensure maximum security, support for single-point administration, and for manageability.

The Application Definition Wizard

The Application Definition Wizard provides an easy and intuitive interface to create new user-specific application definitions. It also manages the user-specific credentials and tasks that SecureLogin performs on multiple applications, including the following:

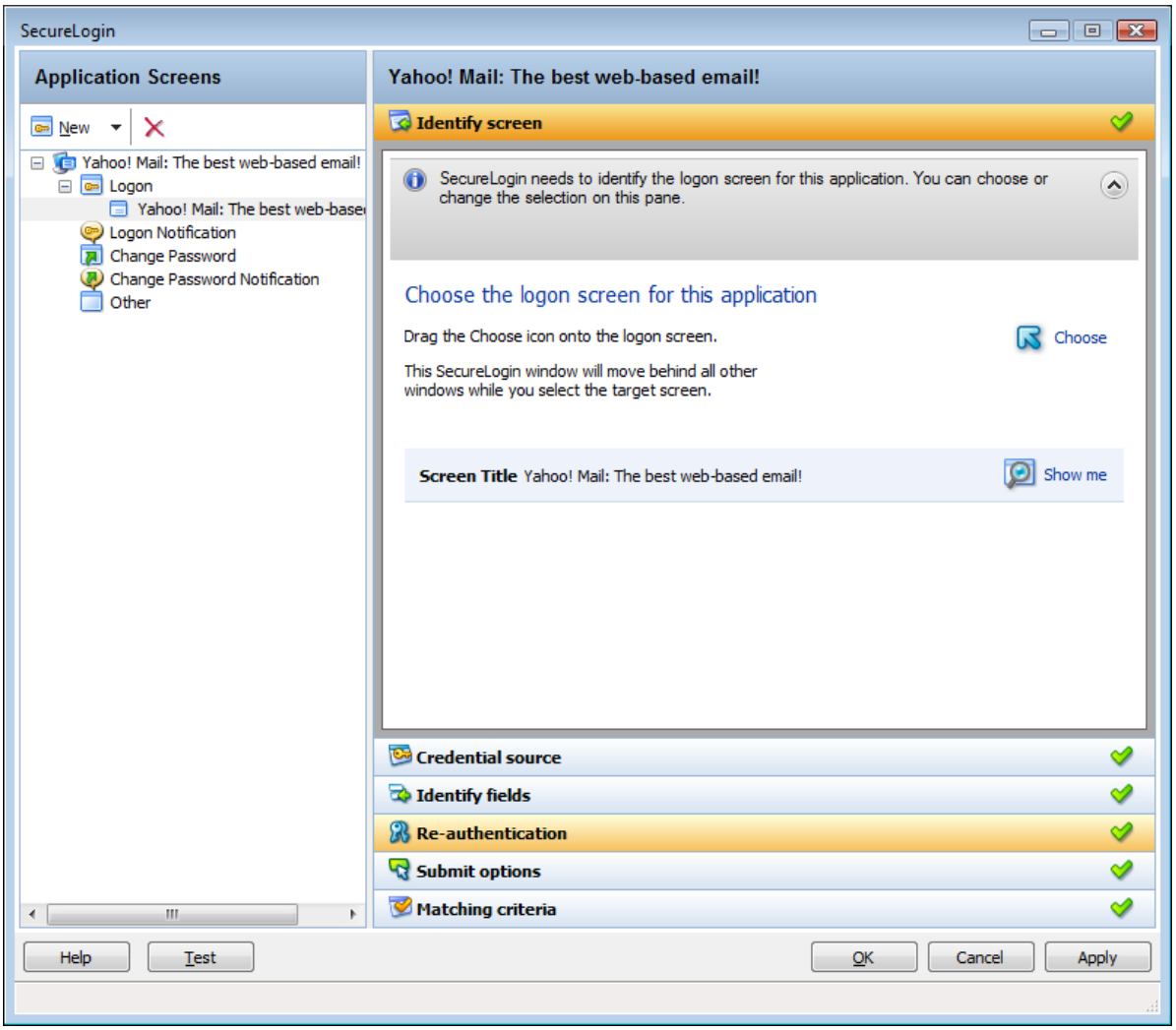
- Retrieving and entering login details.
- Automating many login processes, including multi-page logins and login panels that require miscellaneous information such as surnames, telephone numbers, or IP addresses. These can also be stored in the directory.

When you log in to an application for the first time if you have permission to create an application definition, you are prompted to create an application definition if SecureLogin is active on your workstation.

Although you can enable various types of application for single sign-on using the application definition wizard, some specific applications cannot be enabled for single sign-on. For information on such applications, read Chapter 8, “Limitations, Tips, and Troubleshooting,” on page 125.

2 Understanding the Application Definition Wizard Interface

Figure 2-1 *The Application Definition Wizard Interface*



The user interface of SecureLogin Application Definition Wizard includes various forms that help in managing the application definitions.

After you launch the Application Definition Wizard, the wizard page has the following main components on the interface:

- “The Application Screens Pane” on page 10
- “Attributes Pane” on page 59
- “General Controls and Messages” on page 59
- “Selecting and Identifying Screens and Controls” on page 60

- “Recording Keystrokes” on page 61
- “Using Regular Expressions” on page 62

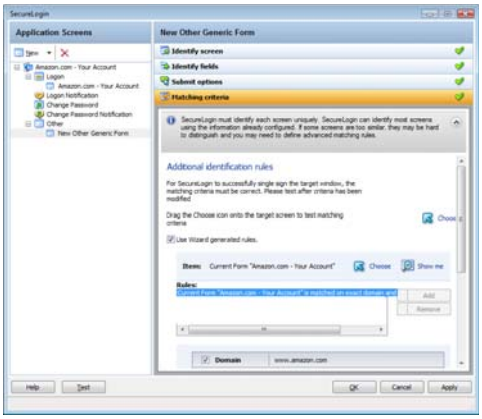
The Application Screens Pane

The **Application Screens** pane is shown on the left side of the Application Definition Wizard interface.

The **Applications Screens** pane has a list of the application forms enabled for single sign-on, change password, notifications, and others.

The advanced options are displayed only if you select them.

Figure 2-2 *The Application Screens Pane*



The **Application Screens** pane contains the following menus:

- “Logon” on page 10
- “Login Notification” on page 26
- “Change Password” on page 34
- “Change Password Notification” on page 44
- “Other” on page 53

Logon

You can create application definitions for a login screen, through the **Logon** screen. For this, you must complete the following tasks:

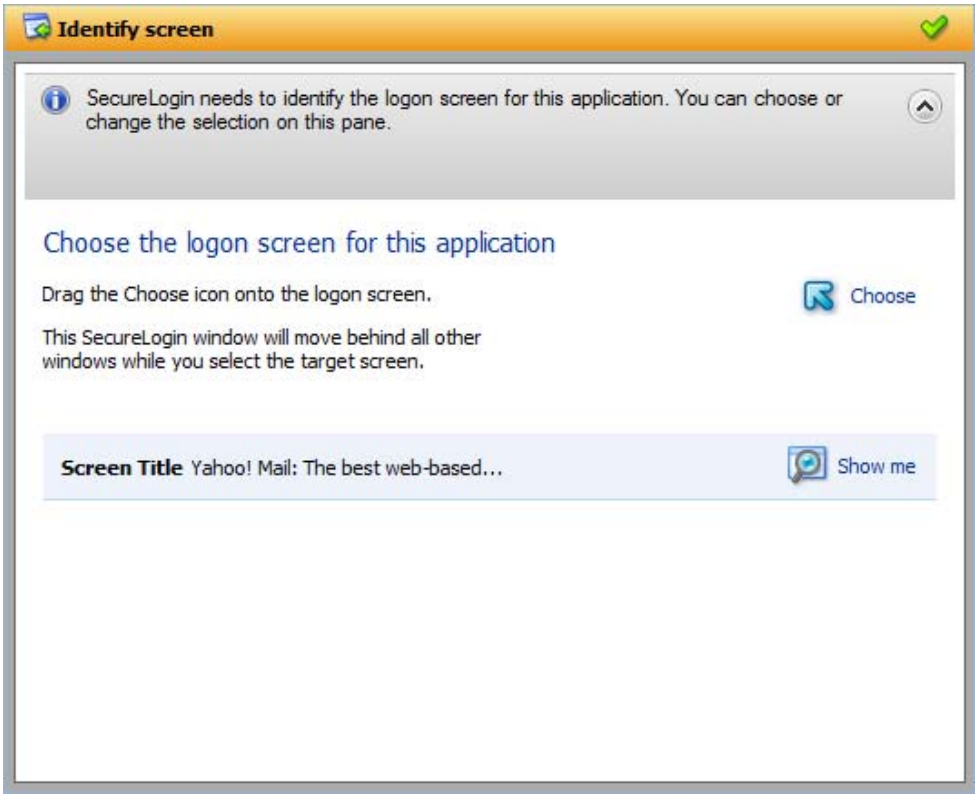
- “Identifying the Screen” on page 11
- “Selecting the Credential Source” on page 11
- “Identifying the Fields” on page 14
- “All Fields” on page 17
- “Specifying Re-authentication” on page 19
- “Selecting the Submit Options” on page 21
- “Determining the Matching Criteria” on page 25

These are displayed in the “Attributes Pane” on page 59.

Identifying the Screen

SecureLogin identifies the login screen of the application for which you want to enable single sign-on. You can use the **Identify screen** attribute to select or change the login screen of the application.

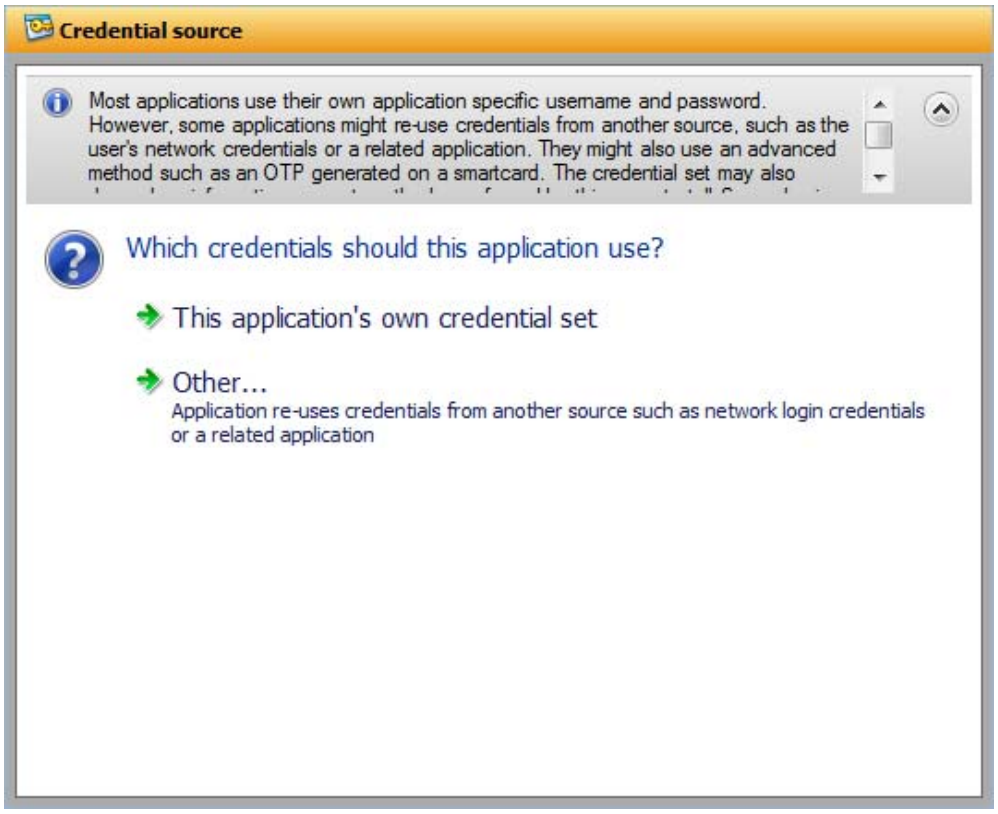
Figure 2-3 *The Identify Screen*



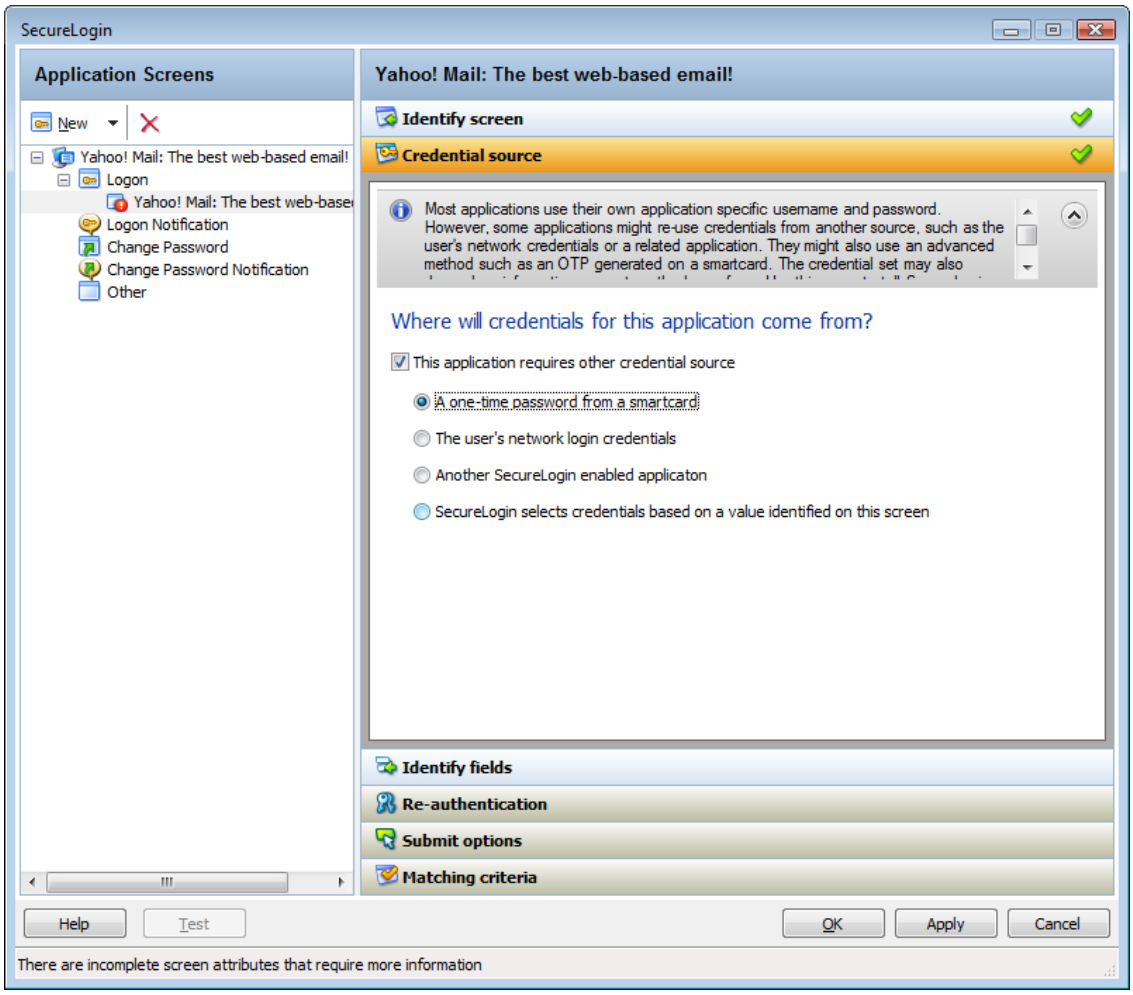
1. In the Application Screens pane of the wizard, select the login screen by dragging the **Choose** icon to the login screen.
2. Click the **Show me** icon to highlight the selection made by the wizard.

Selecting the Credential Source

1. Use the **Credential source** menu to select the credentials that SecureLogin must use in an application. Typically, you can have only one credential set for an application. If a second login is enabled with different credential set, it replaces the first set of credentials.



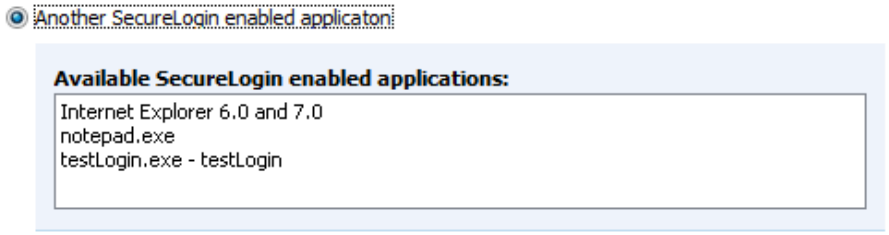
2 Select **This application's own credential set** to allow SecureLogin create a discrete set of credentials for the application. The credential set is recognized by the name of the application.



3 Select **Other** to choose another source of credentials for the application. You choose from the following sources.

- **A one-time password from a smart card:** Select this option to use a one-time password from a smart card to log in to the application.
- **The user's network logon credentials:** Select this option to use the user's directory credentials to log in to the application.
- **Another SecureLogin enabled application:** Select this option to use the credentials of another application that is already enabled for single sign-on. Select a credential set from the list of applications displayed under **Another SecureLogin enabled application**.

Figure 2-4 *Selecting Another Application's Credentials*



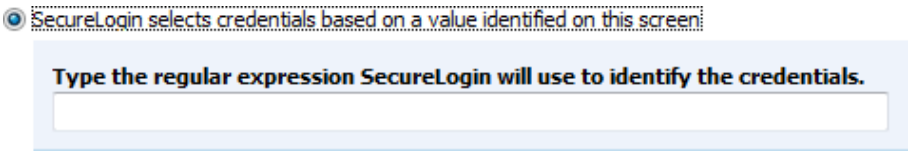
- **SecureLogin selects credentials based on a value identified on this screen:** Select this option when the login information for an application is determined by the presence of a particular value in the login screen. You can specify a text value in the field.

  Regular expressions are supported. For example, you can specify a regular expressions such as:

  ```
  Connecting to server (.*)
  ```

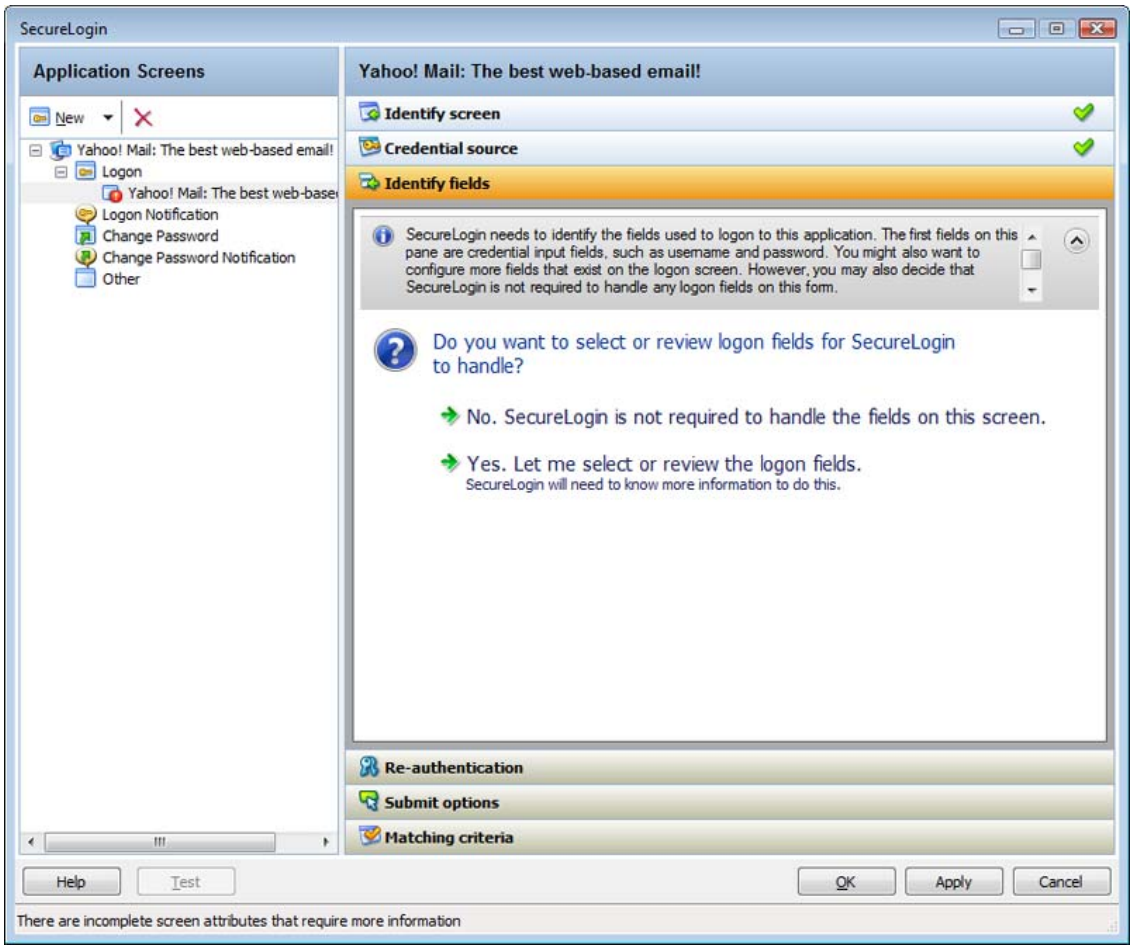
  The `(.*)`specifies the value that must be captured to define the credentials. You can have one credential set for each regular expression value.

Figure 2-5 *Selecting Credentials Based on a Value*



Identifying the Fields

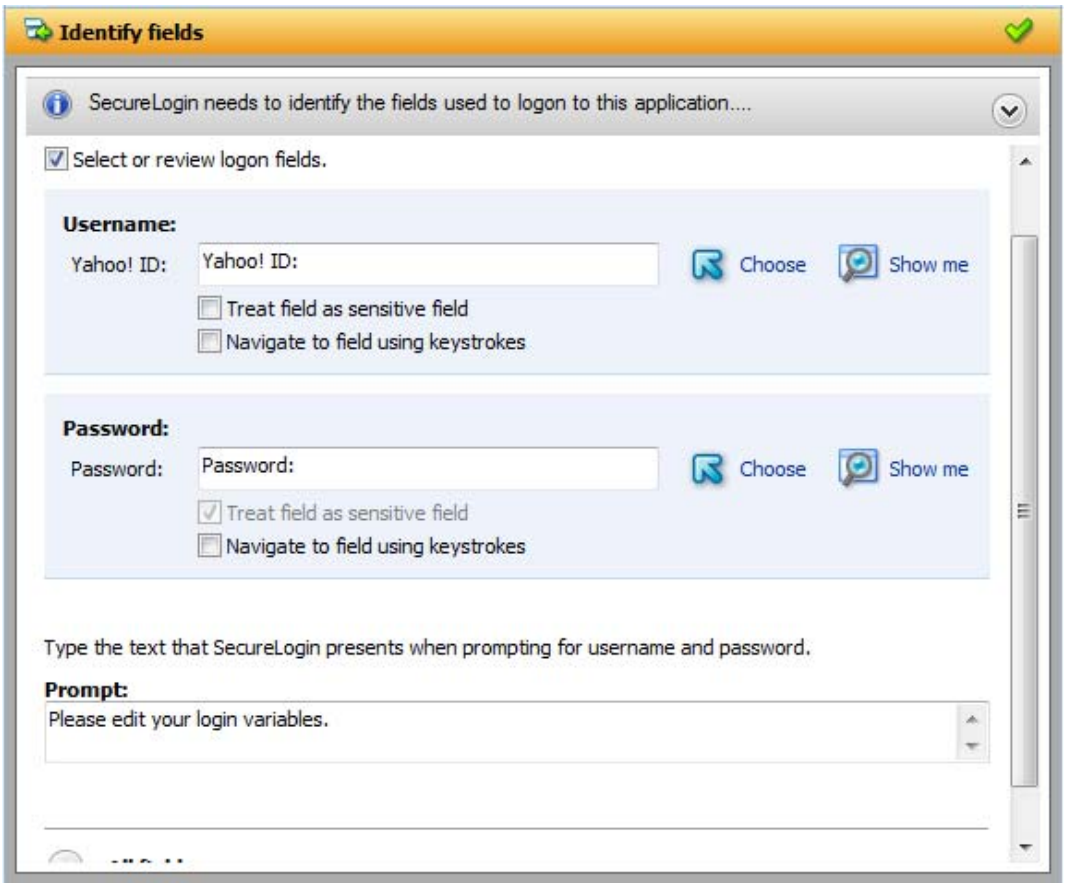
1. Use the **Identify fields** menu to review or change the selection of fields recognized by the wizard.
2. If you select **No. SecureLogin is not required to handle the fields on this screen**, SecureLogin does not handle any fields detected on the application. Use this option to create a common credential set that you can use with several applications. You can link other application definitions to this common credential set.



3 If you select **Yes. Let me select or review the logon fields**, you can review and confirm if the fields are selected correctly by the wizard.

By default, SecureLogin uses the field names as the prompts in its dialog boxes. You can edit the field names for more clear and user-friendly names.

4 If the fields are not identified correctly, drag the **Choose** icon to the fields and click **Show me**. The identified fields are highlighted.

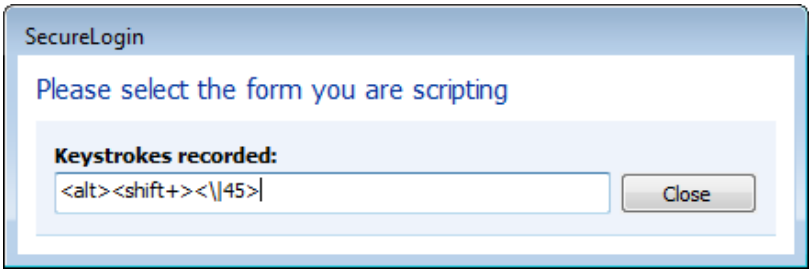


5 Select **Treat text field as a sensitive field** to hide the characters with asterisks. This choice is optional for a username, but selected by default for a password.

6 Select **Navigate to field using keystrokes**, if you cannot identify the correct field through other methods.

6a Click **Start**.

6b Specify the keystrokes.



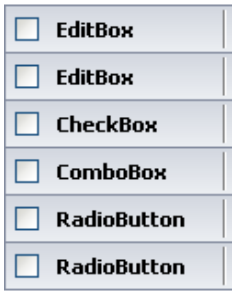
6c Click **Close** to return to the **Identify fields** menu.

6d Click **Stop** to stop the recording.

SecureLogin begins using the specified keystrokes at the subsequent login.

All Fields

1 Click **All Fields** to show other fields detected by the wizard on the login screen. Each control is listed by type and name (if known).



When the Application Definition Wizard retrieves the default controls such as the username and password fields, they are identified as primary controls and identified in **Identify Fields** menu. See Figure 2-8 on page 28.

These controls are also listed with all other controls in the **All Fields** menu. By default, they are selected and dimmed. However, if you use the **All Fields** menu to set the control definitions for primary controls selected in **Identify Fields** menu, the selections made in the **Identify Fields** menu is updated.

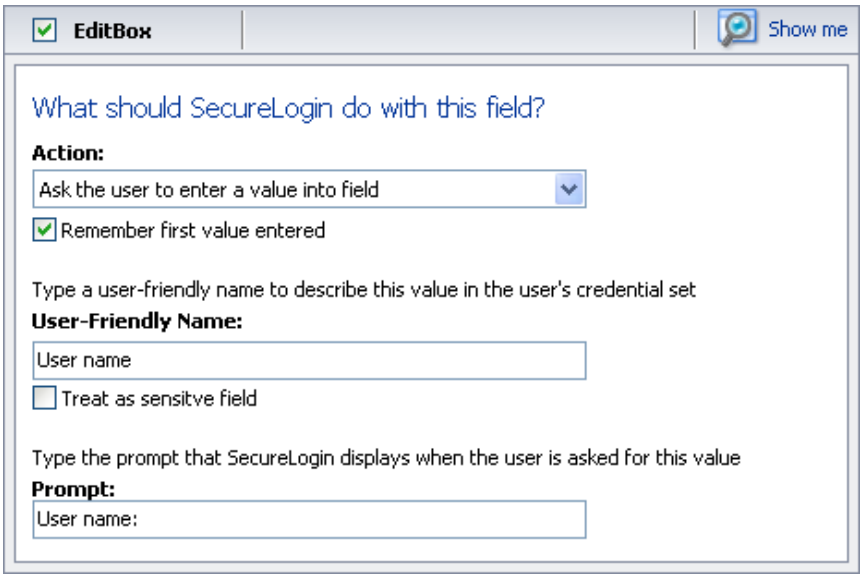
The other fields are:

- “Edit Box” on page 17
- “Check Box” on page 18
- “Combo Box” on page 18
- “Radio Button” on page 19

Edit Box

1 If an edit box is detected, use the **Action** drop-down list to configure SecureLogin to:

- **Ask the user to enter a value into field:** If you select this option, specify a user-friendly name and the message to prompt users to specify a value.



NOTE: If you select **Remember first value entered**, SecureLogin saves the first value entered in this field and automatically enter it on all subsequent logins.

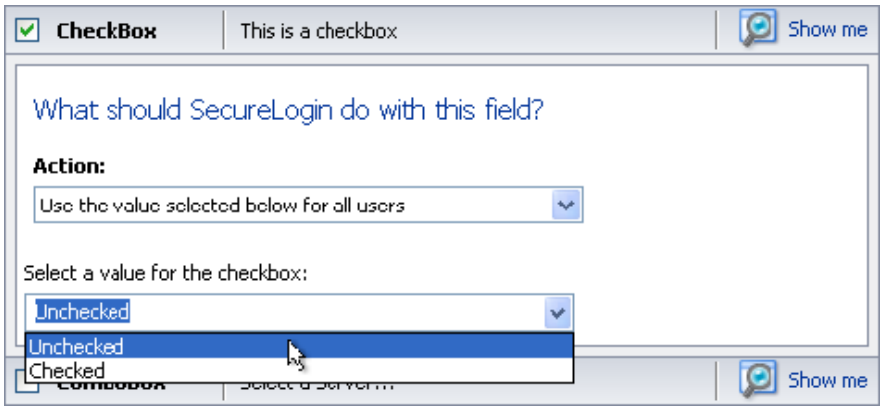
The **User-Friendly Name** is also used as the variable name in the SecureLogin Client Utility.

Select **Treat as sensitive field** to treat the username field like a password field and hide the characters with asterisks.

- **Use the value selected below for all users:** If you select **Use the value selected below for all users**, specify the message that SecureLogin displays.

Check Box

1 If a check box is detected, use the action **Use the value selected below for all users** to select whether the check box is to be selected or deselected.



Combo Box

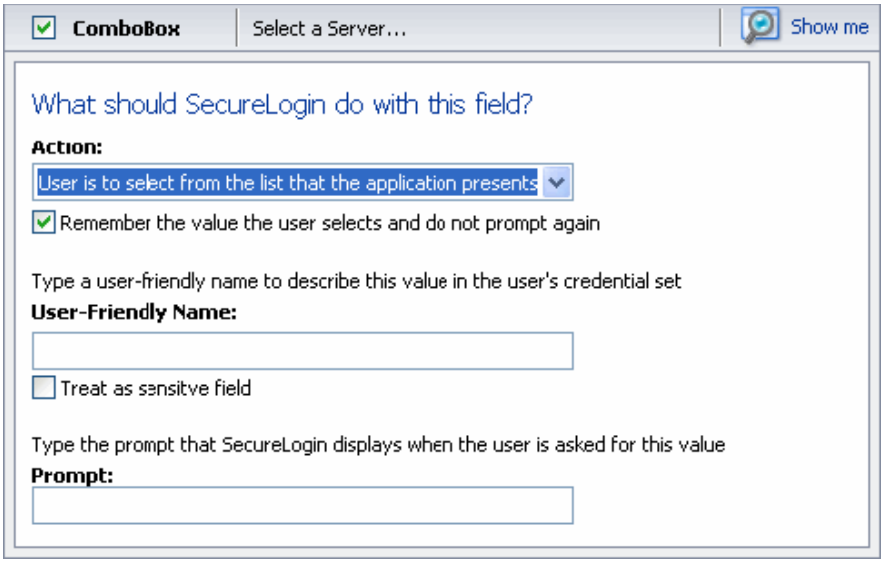
1 If a drop-down list box or any other kind of combination box is detected, use the **Action** drop-down list to configure SecureLogin to:

- **Use the value selected below for all users:** If you select **Use the value selected below for all users**, specify the option SecureLogin selects. This is the only option available for combo boxes in Web applications.

- **Ask the user to select from the list that the application presents:** If you select **User is to select from the list the application presents**, specify a name for the value and the text used to prompt users. This option is not available for Web applications.

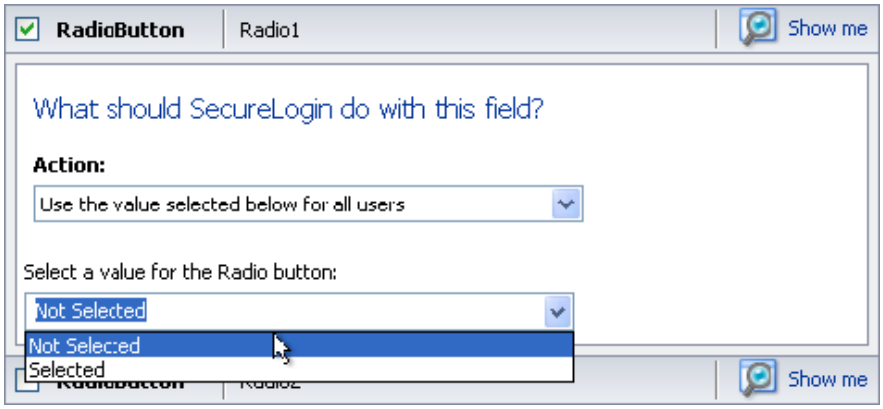
  If you select **Remember the value the user selects and do not prompt again**, SecureLogin stores and automatically enter this value into this screen in the future.

Figure 2-6 *Specifying Values for a Combo Box*



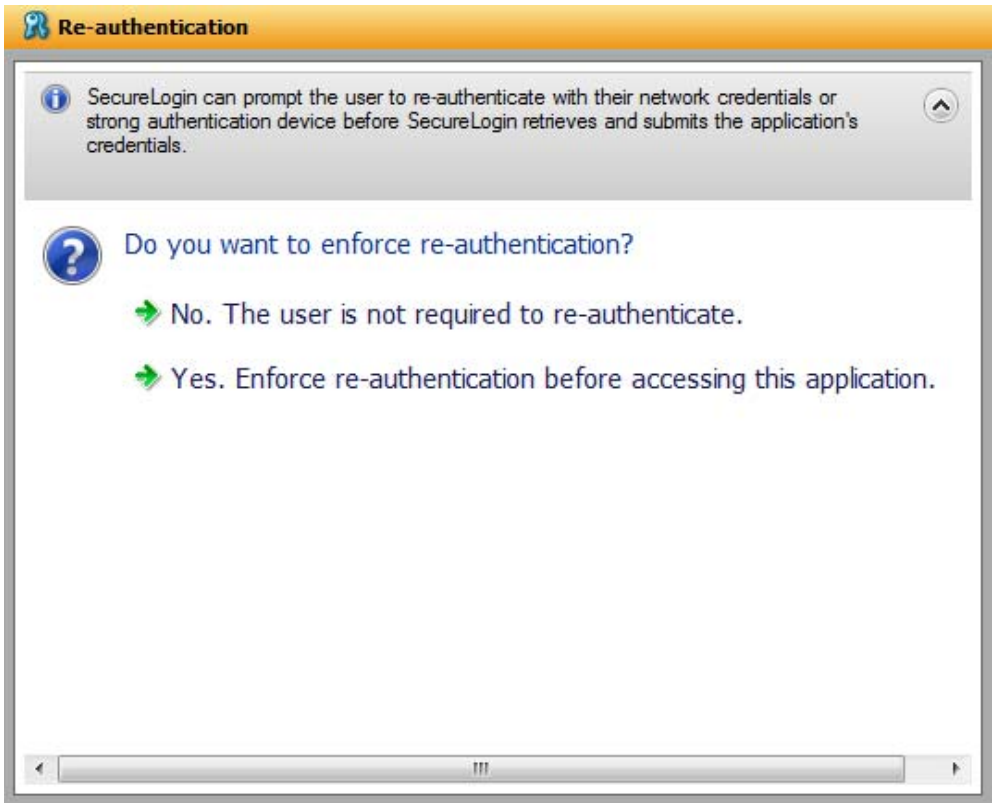
Radio Button

1 If a radio button is detected, use the **Use the value selected below for all users** action to select whether the radio button is selected or not.



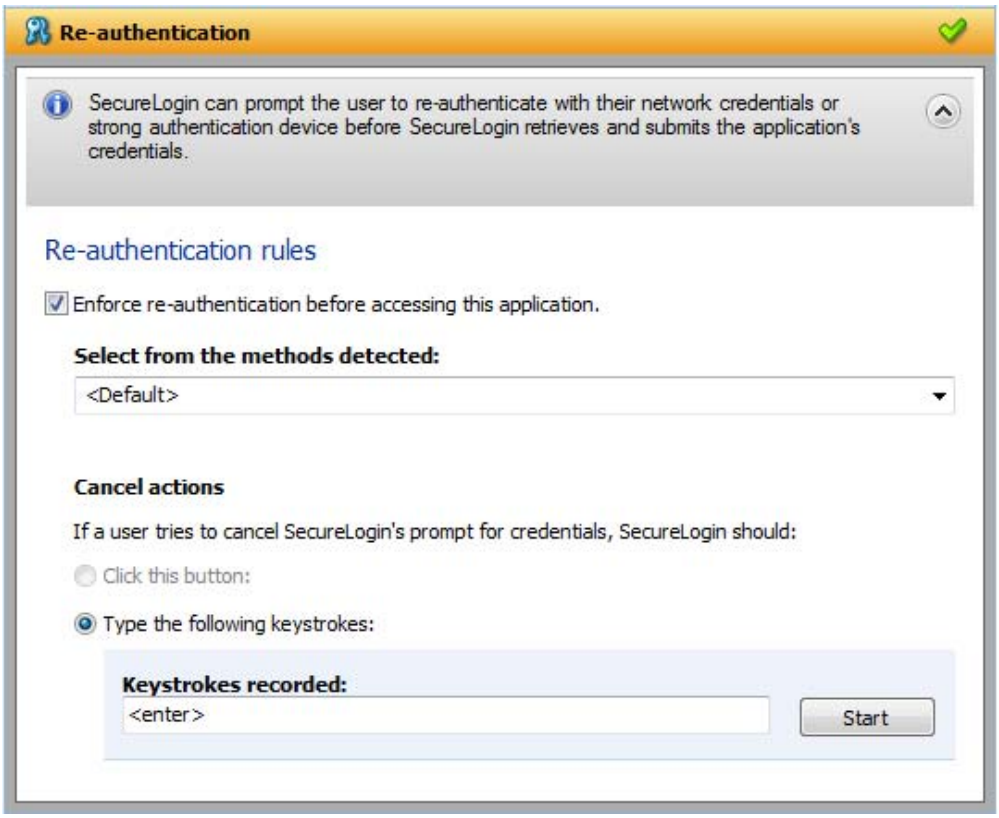
Specifying Re-authentication

1 Use the **Re-authentication** menu to specify how users must reauthenticate. Specify whether they must reauthenticate with their network credentials or by using an authentication device.



2 If you select **No. The user is not required to re-authenticate**, SecureLogin does not prompt users to reauthenticate before providing the credentials to the application.

If you select **Yes. Enforce re-authentication before accessing this application**, users must specify the credentials that SecureLogin uses to reauthenicate the user's identity.



3 From the **Select from the methods detected** drop-down list, select the method SecureLogin must use to authenticate the credentials. You can select one of the following options:

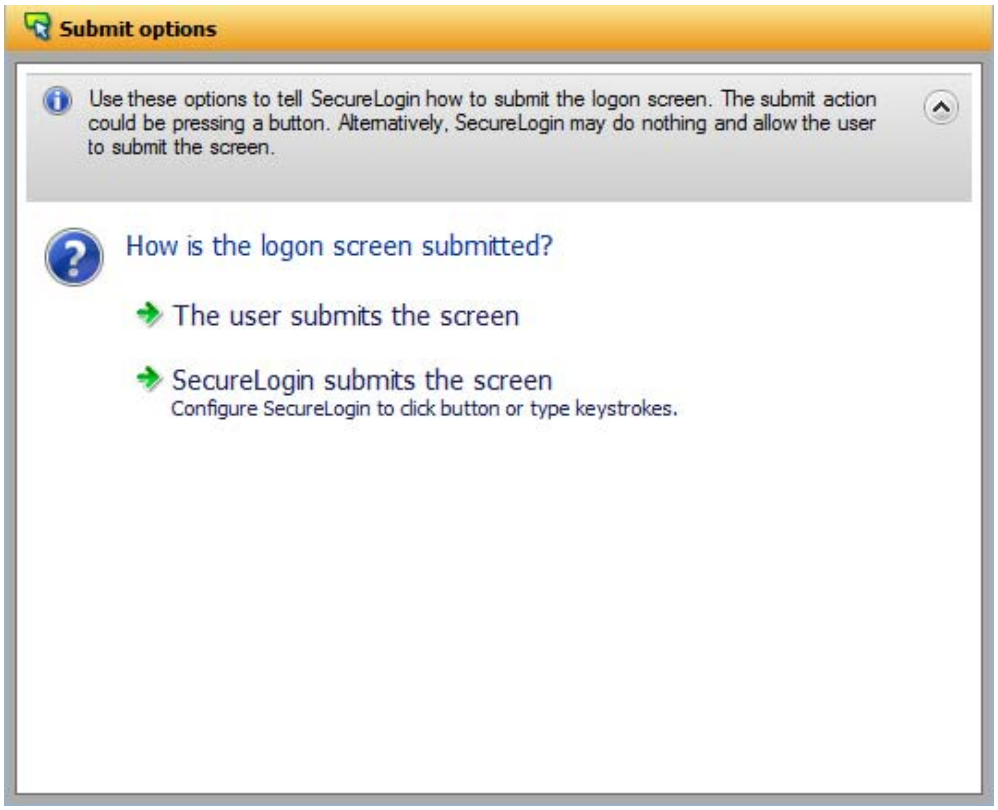
- **Default:** The method the user used to log in to the application.
- **Use same credentials as network login:** Use the network login credentials.
- **Password:** The network password.
- **Smart card:** After the PIN is verified, SecureLogin checks to see if the smart card is available to the user.

You must also specify the action for SecureLogin to take when the user cancels reauthentication. You can define one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user cancels the reauthentication dialog box. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes that SecureLogin enters when a user clicks **Cancel** on the reauthentication dialog box. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.

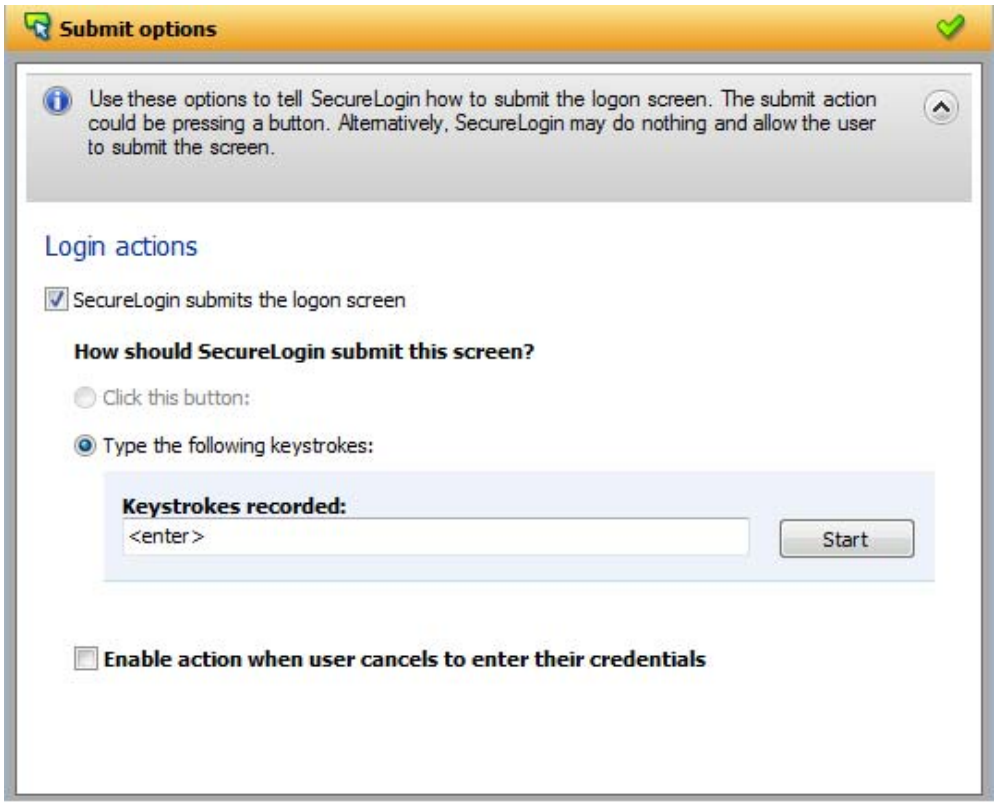
Selecting the Submit Options

1 Use the **Submit options** menu to define how SecureLogin submits the login screen.



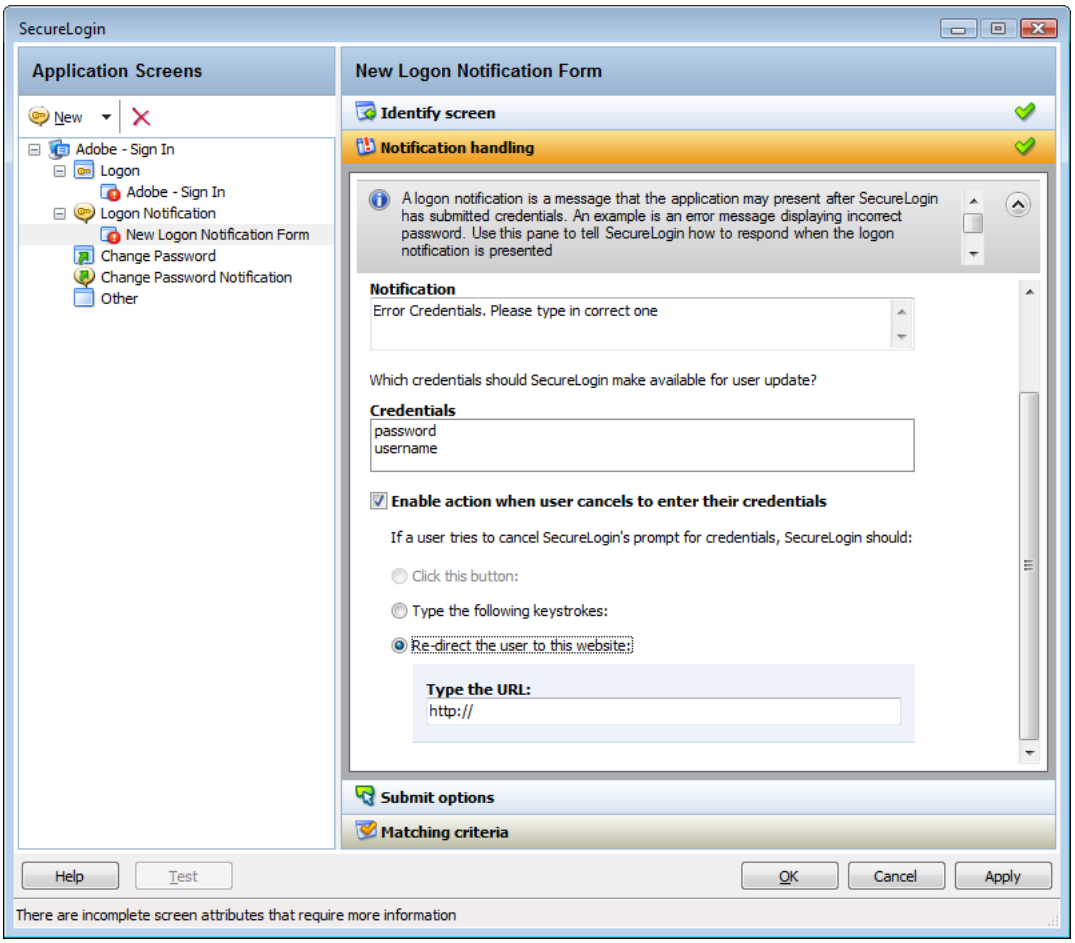
2 If you select **The user submits the screen**, SecureLogin does nothing and the user must manually submit the login screen.

3 If you select **SecureLogin submits the screen**, specify the action that SecureLogin must take to submit the login screen.



You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes that SecureLogin enters to submit the login screen. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Enable action when user cancels to enter their credentials:** If you select this option, specify the action SecureLogin takes when a user cancels credential entry.

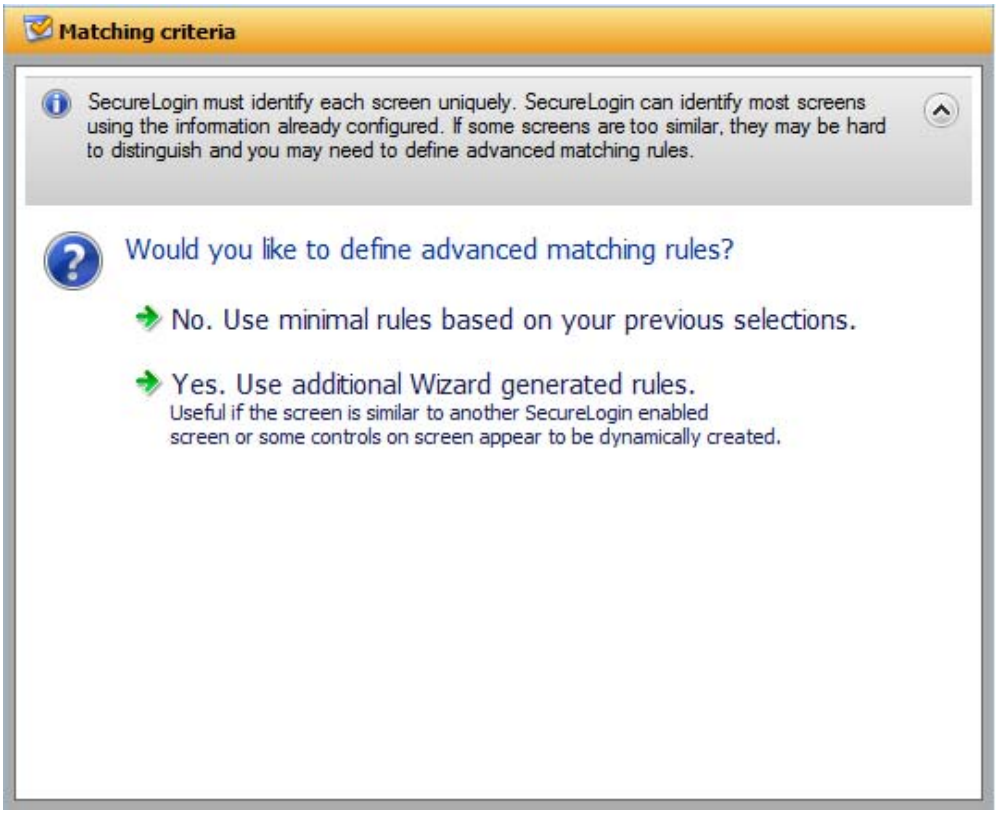


You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user cancels the prompt for credentials. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes that SecureLogin enters when a user cancels the prompt for credentials. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct the user to this website:** Specify a URL to go to when a user cancels the prompt for credentials. You can redirect users to the login screen and force them to specify the login credentials again.

Determining the Matching Criteria

1 SecureLogin must uniquely identify each application screen in order to run an application definition. If SecureLogin cannot uniquely identify a particular application screen, you can manually define the matching criteria.



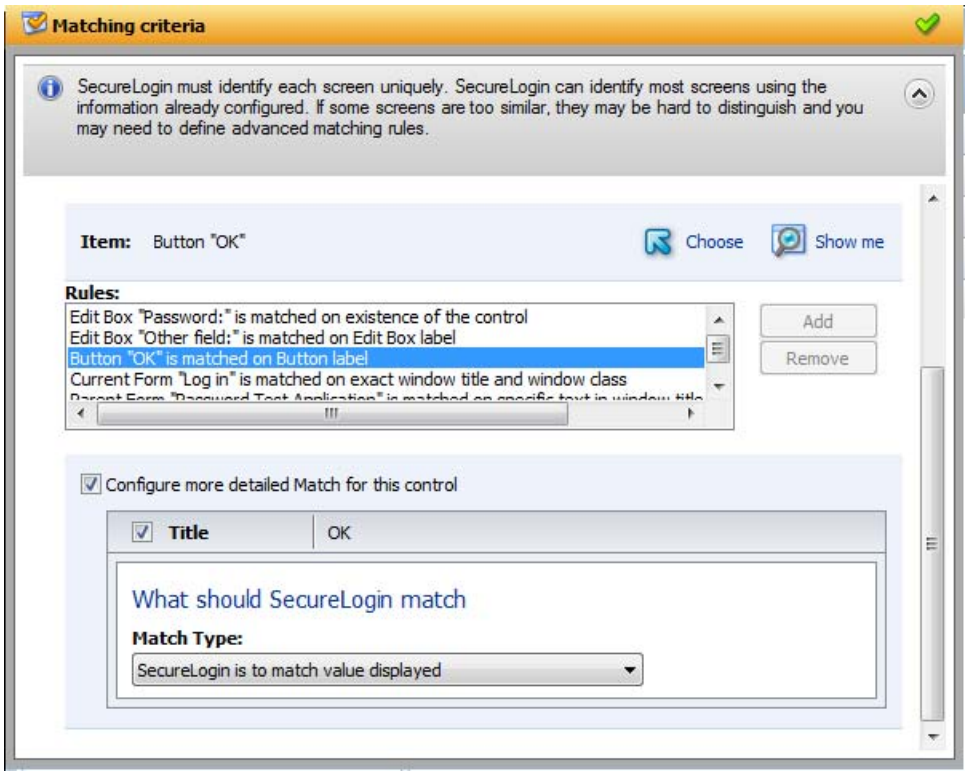
1 If you select **No. Use minimal rules based on your previous selections**, SecureLogin uses the rules defined in previous attribute panels to identify and handle an application.

2 If you select **Yes. Use additional Wizard generated rules**, you can add, modify, or remove rules. Your matching criteria must include at least one rule. After you have selected this option, the following screen appears:

By default, **Use Wizard generated rules** is selected. The **Rules** text box lists the controls detected by SecureLogin. You can add a new rule by dragging the **Choose** icon to a specific control and clicking **Show me** to confirm that SecureLogin has identified the correct control.

To modify a rule for a control:

1 Select the rule you want to edit, then select **Configure more detailed match for this control**



2 Define what SecureLogin must match. You can set one of the following matching rules:

- **SecureLogin is to match value displayed:** If you select this option, SecureLogin only matches those screens that exactly match the displayed text and rules identified.
- **SecureLogin is to match specific part of the identified ctrl:** If you select this option, you must use a regular expression to define and match the screen features. You cannot use special characters in a regular expression.

To test a regular expression:

1 To verify if your regular expression is correct, click **Test Match**.

If a regular expression does not match any control on the application screen, SecureLogin prompts you to verify your regular expression and select the correct control.

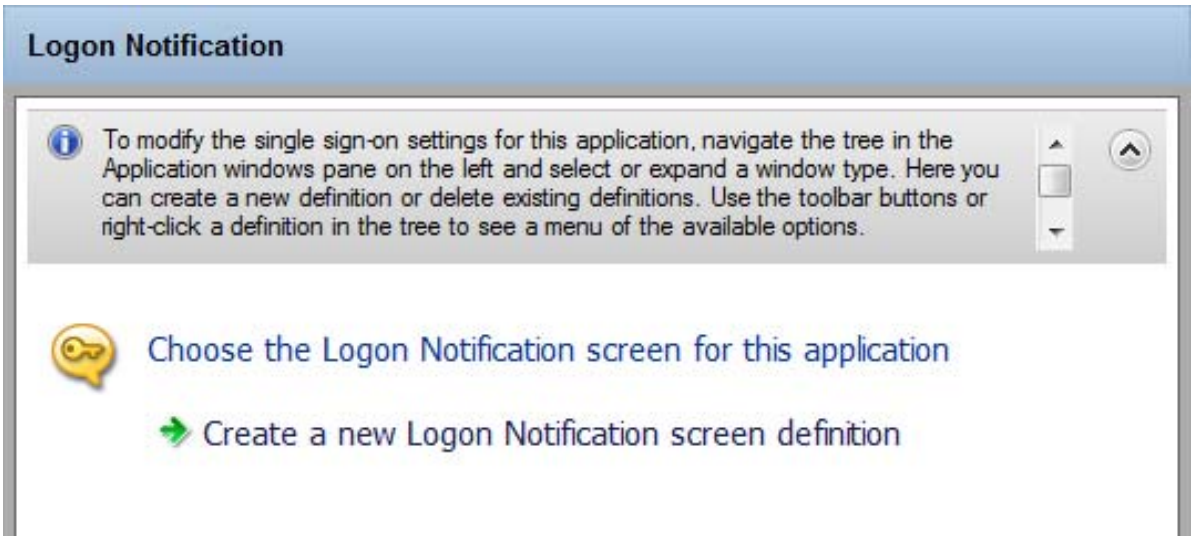
To delete a rule:

1 Select the rule, then click **Remove**.

Login Notification

A login notification is a message that the application displays after SecureLogin has submitted the credentials, such as an error message indicating an incorrect password. Use the **Logon Notification** options to define how SecureLogin handles notifications in your application definition.

Figure 2-7 *Login Notification Screen*



To define an application definition or login notifications, You must complete the following tasks:

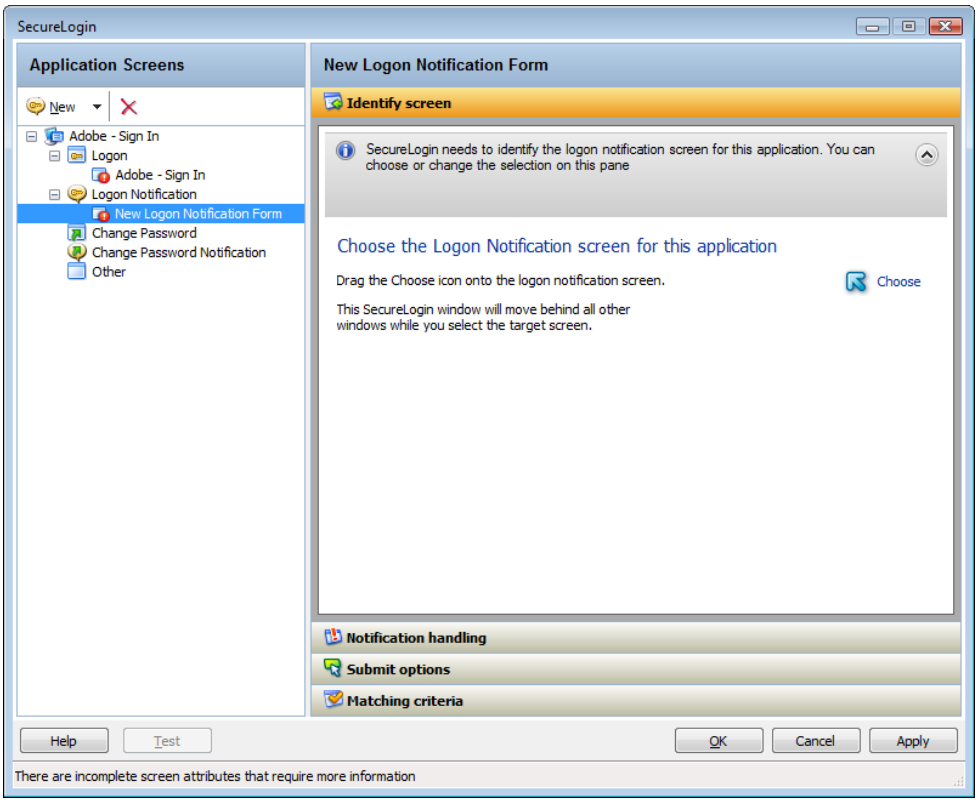
- “Identifying the Screen” on page 27
- “Defining Notification Handling” on page 28
- “Defining the Submit Options” on page 31
- “Defining the Matching Criteria” on page 33

These are displayed in the “Attributes Pane” on page 59.

Identifying the Screen

SecureLogin identifies a login screen for which you want to create an application definition. You can use the **Identify screen** attribute to select or review the login screen selected by the wizard.

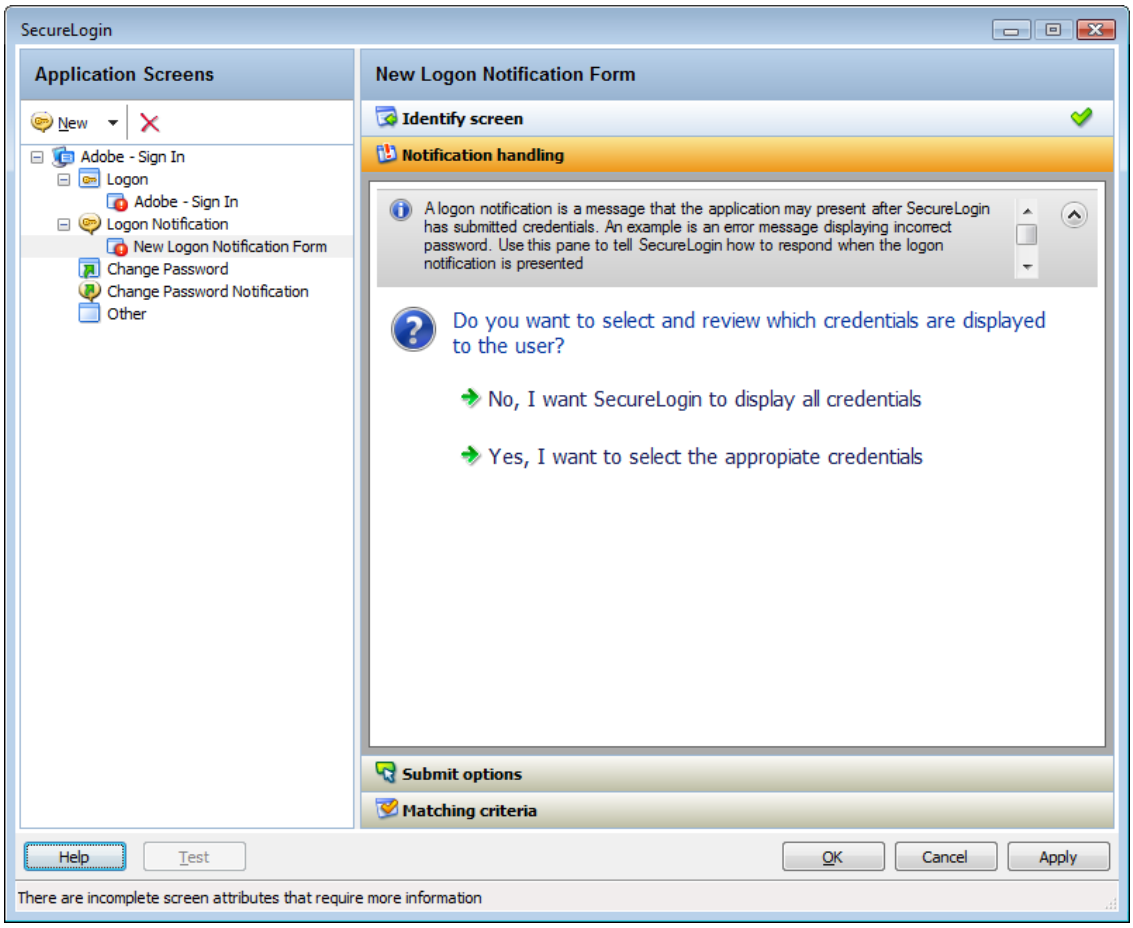
Figure 2-8 *The Identify Screen*



1 Select the login screen by dragging the **Choose** icon to the login screen or by recording keystrokes. The title of the login screen is displayed. Click the **Show me** icon to highlight the selection made by the wizard.

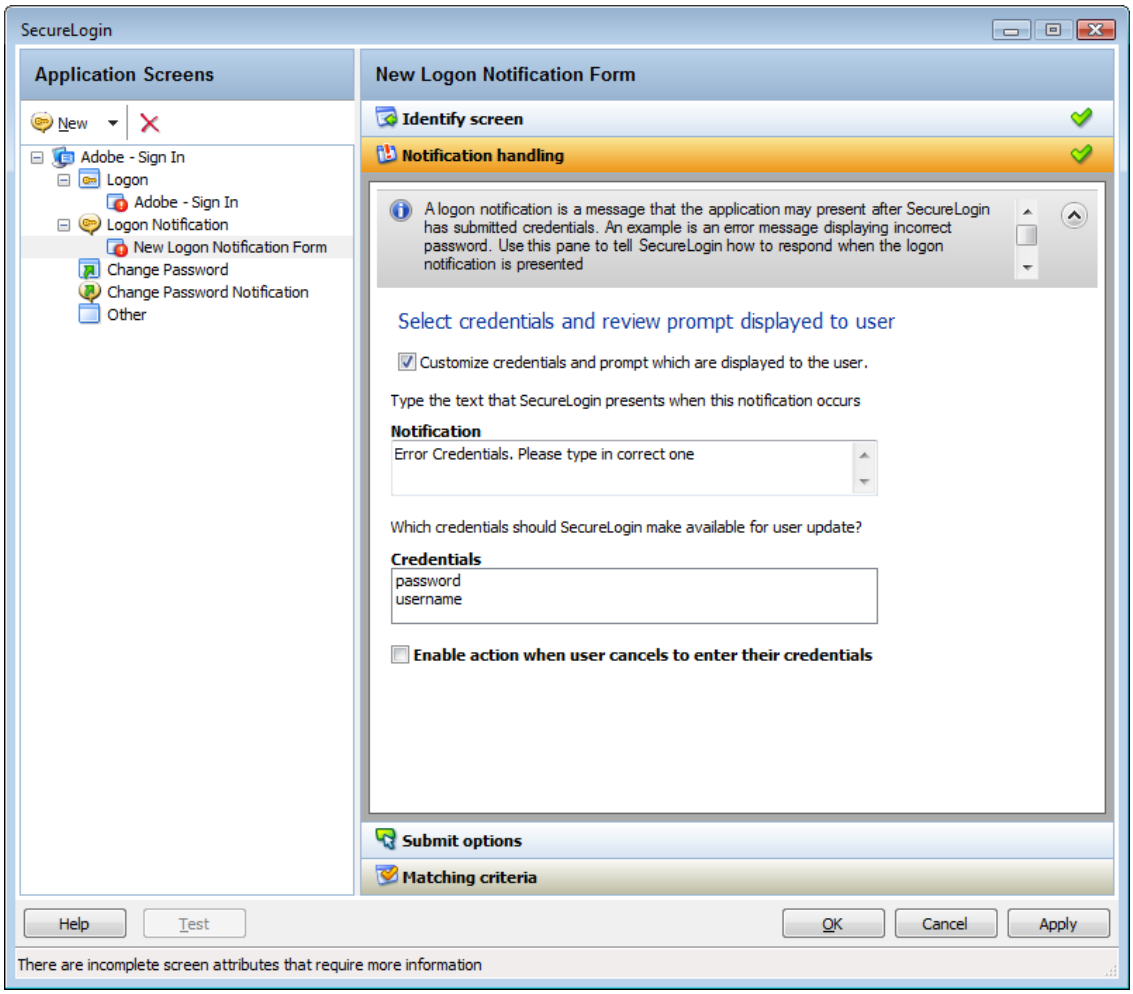
Defining Notification Handling

1 Through the **Notification handling** menu, specify how SecureLogin must respond when a login notification screen is displayed.

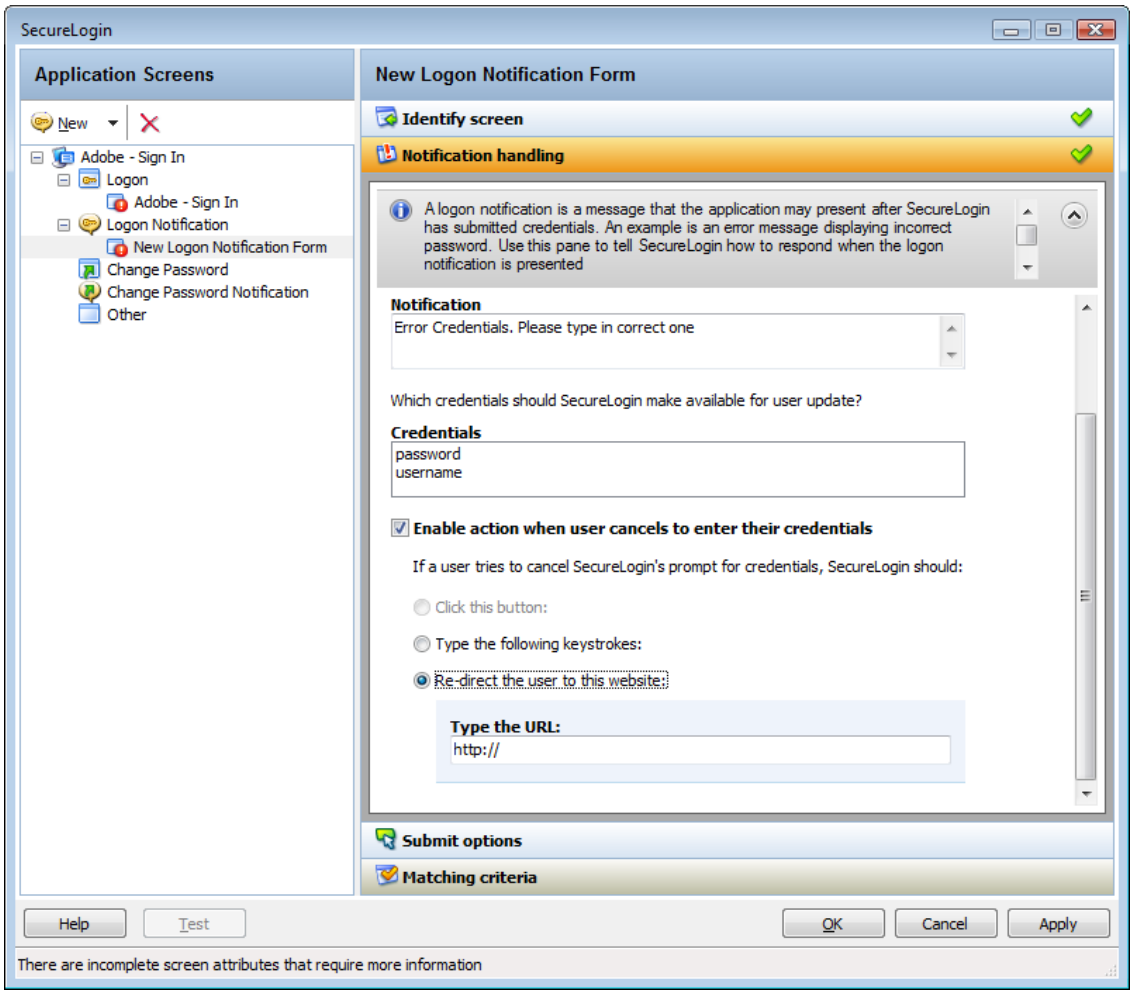


2 Click **No, I want SecureLogin to display all credentials** to prompt the users to enter their credentials again. SecureLogin uses the notification from the application.

3 Click **Yes, I want to select the appropriate credentials** to select the credentials to display to the user for updating. If you select this option, you must specify the prompt displayed to the users. You can select an existing prompt, or you can specify a cutomized prompt and error message. You must also specify the credential that users provide for the application.



4 If you select **Enable action when user cancels to enter their credentials**, specify the action that SecureLogin must take when a user cancels credential entry



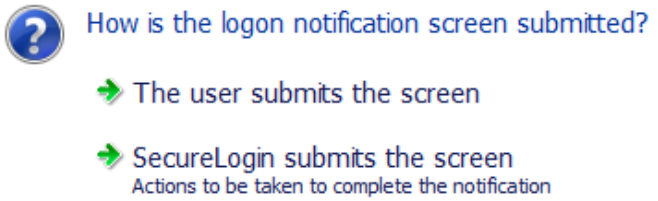
You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user cancels the prompt for credentials. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes that SecureLogin enters when a user cancels the prompt for credentials. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct the user to this website:** Specify a URL to go to when a user cancels the prompt for credentials. You can redirect users to the login screen and force them to specify the login credentials again.

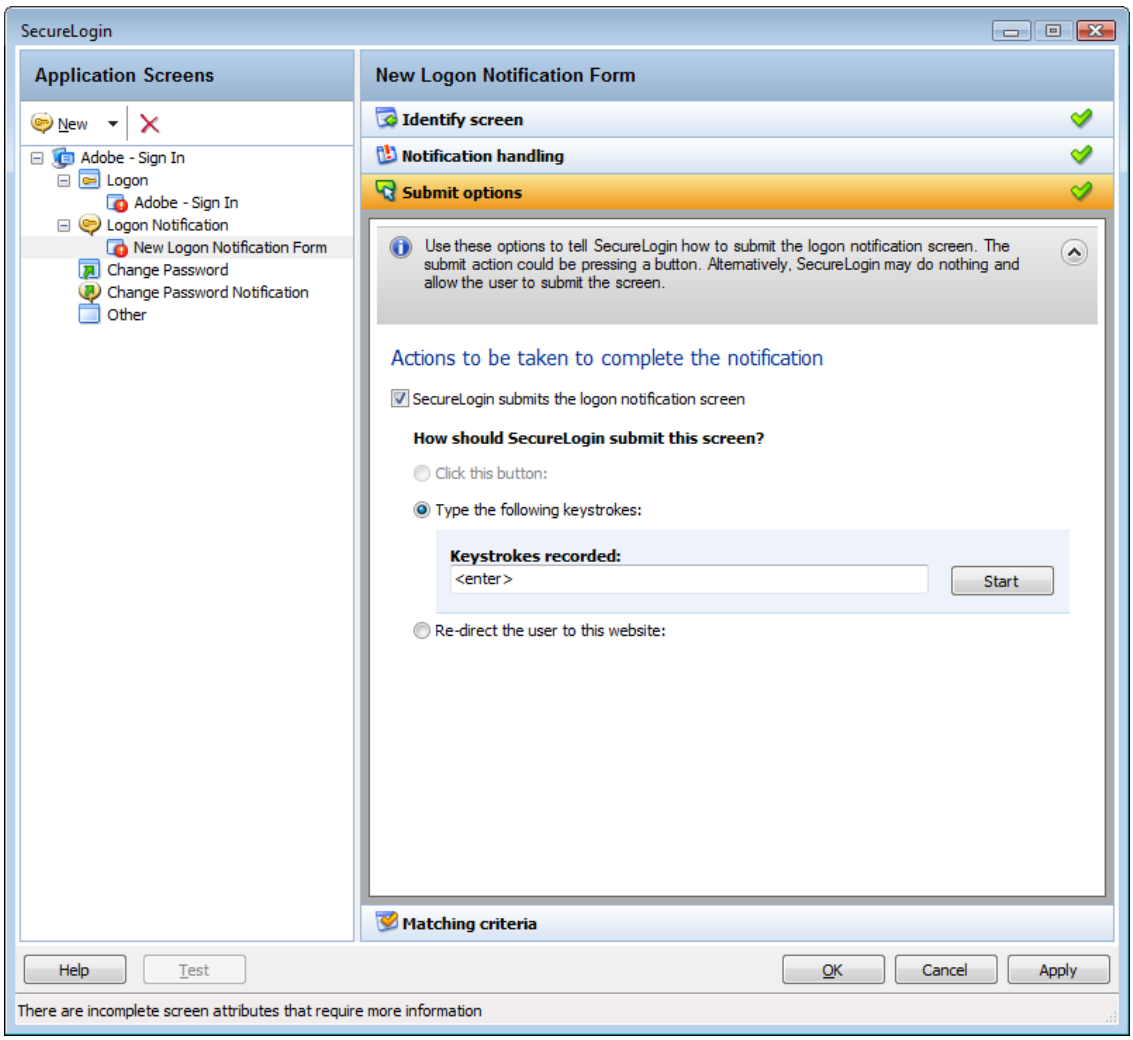
Defining the Submit Options

1 Use the **Submit options** menu to define how SecureLogin submits the login notification screen.

2 If you select **The user submits the screen**, SecureLogin does nothing and the user must manually submit the login screen.



3 If you select **SecureLogin submits the screen**, specify the action that SecureLogin takes to submit the login notification screen.



You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes that SecureLogin enters to submit the login notification screen. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.

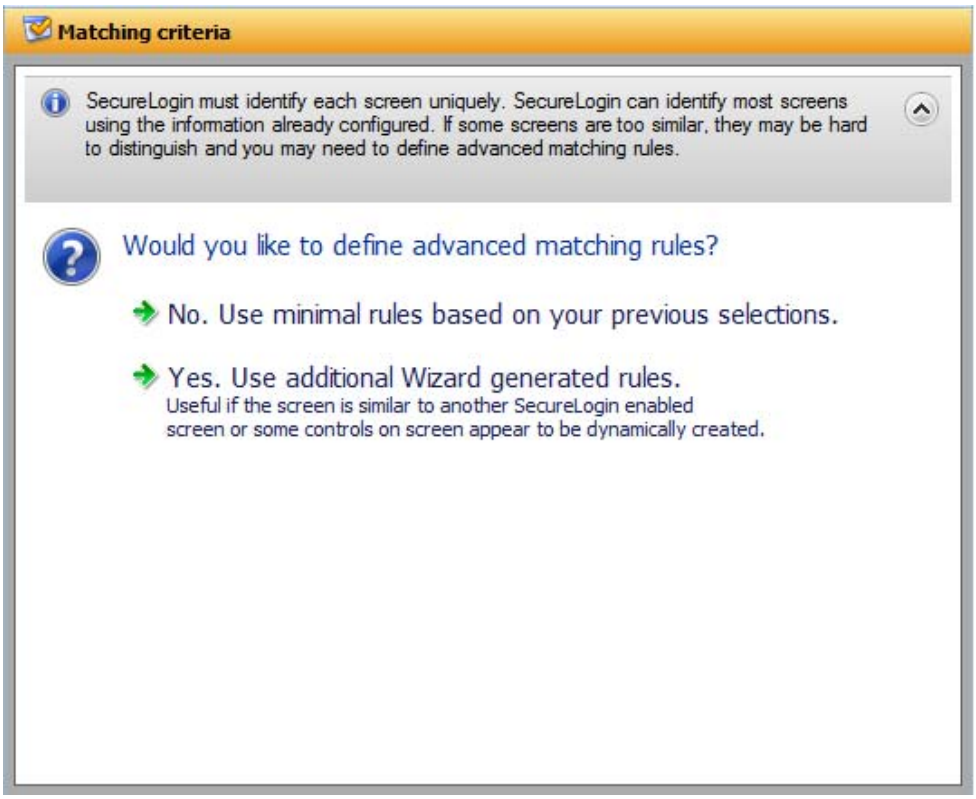
- **Re-direct the user to this website:** Specify a URL to go to when a user submits the login notification screen.

Defining the Matching Criteria

SecureLogin must uniquely identify each application screen in order to run an application definition. If SecureLogin cannot uniquely identify a particular application screen, you can manually define the matching criteria.

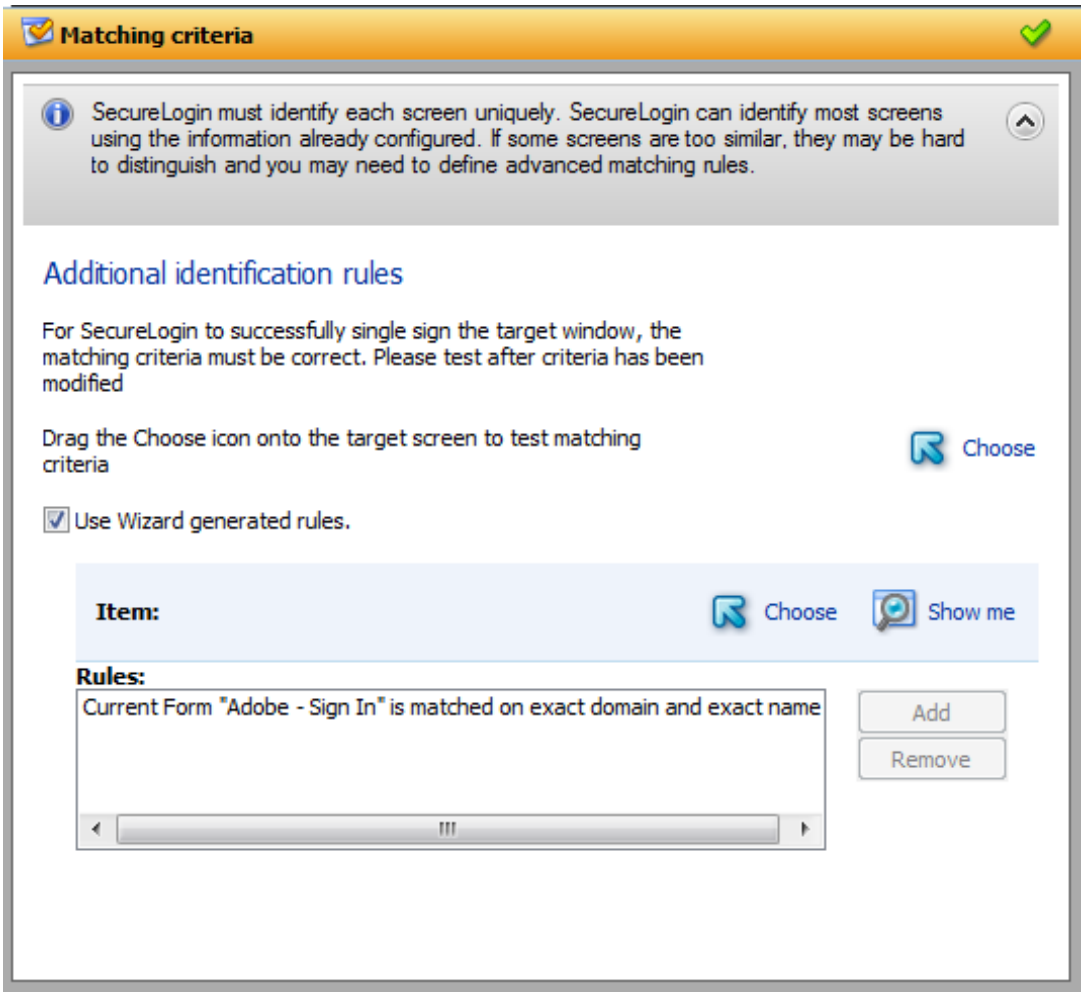
If you select **Use additional Wizard generated rules**, you can add, modify, or remove rules. Your matching criteria must include at least one rule. After you have selected this option, the following screen appears:

Figure 2-9 *Setting the Matching Criteria*



If you select **No. Use minimal rules based on your previous selections**, SecureLogin uses the rules defined in previous menus to identify and handle an application.

Figure 2-10 *Defining Additional Rules*



By default, **Use Wizard generated rules** is selected. The **Rules** text box lists the controls detected by SecureLogin. You can add new rule by dragging the **Choose** icon to a specific control. Click **Show me** to confirm that SecureLogin has identified the correct control.

To delete a rule, select the rule, then click **Remove**.

Change Password

You can use the **Change Password** menu of the Application Definitions Wizard to create an application definition to include instructions for changing the password for an application.

You can allow SecureLogin to generate new passwords that match your password policies or let users choose their passwords. You can also customize the change password prompts displayed to the users.

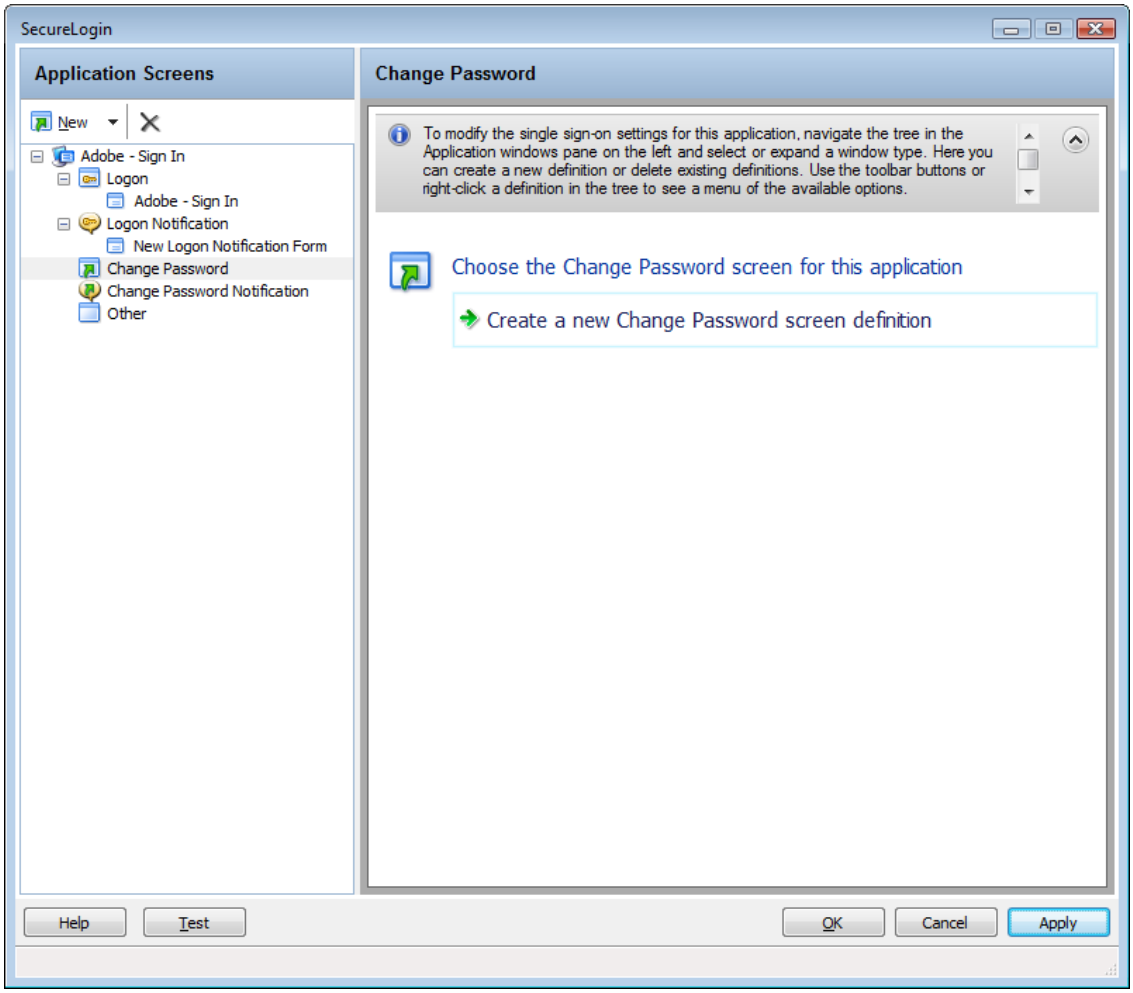
To define an application definition for changing passwords, complete the following tasks:

- “Identifying the Change Password Screen” on page 35
- “Identifying the Change Password Fields” on page 35
- “Generating Password” on page 36

- “Selecting a Password Policy” on page 37
- “Defining the Submit Options” on page 42
- “Defining the Matching Criteria” on page 44

Identifying the Change Password Screen

1 In the Application Screens pane of the wizard, click **Create a Change Password screen definition** to create an application definition for changing a password.



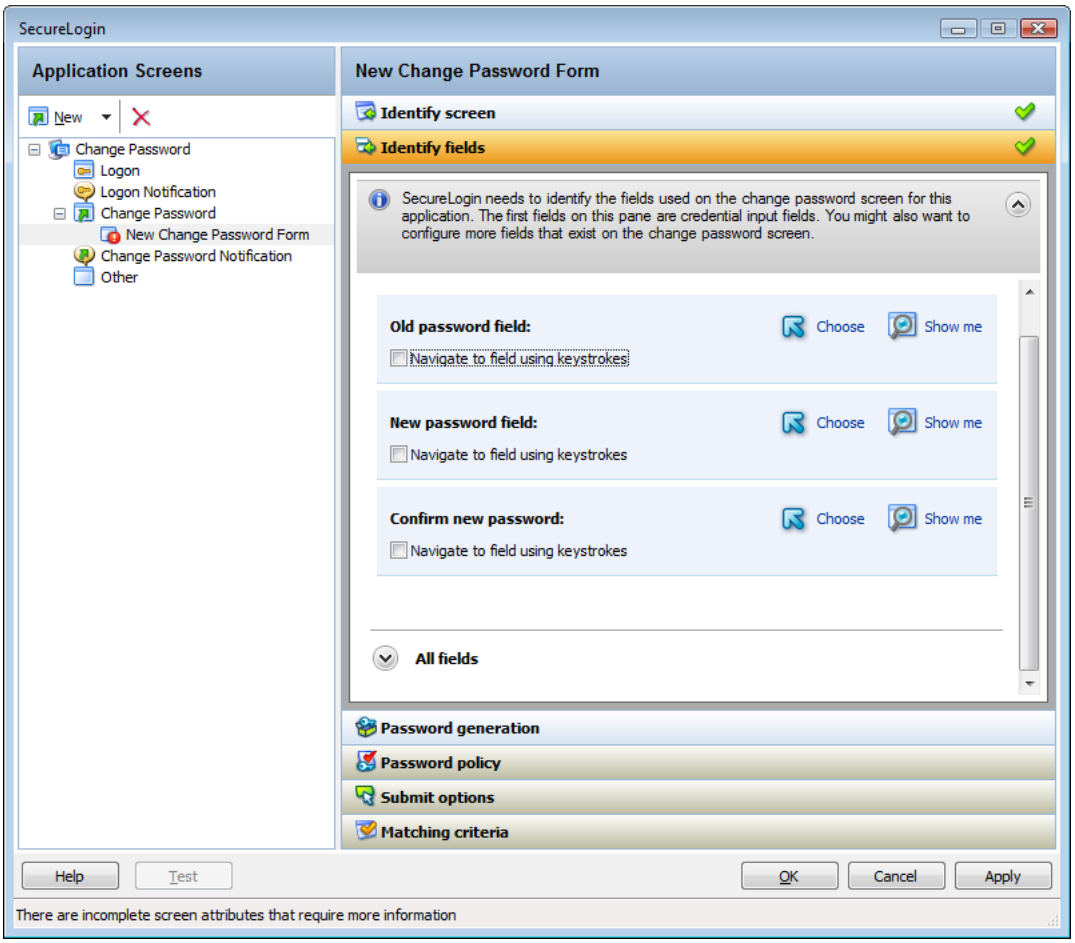
Identifying the Change Password Fields

1 Through the **Identify Fields** menu, select or change the selection of fields for changing a password. Depending on the application, there might be one or more fields.

If the label text for a particular control is empty or incorrect;

1a Click **Show me** to verify if the selected control is correct.

1b If **Show me** does not highlight the correct control, use the **Choose** icon to drag and drop to identify the correct control. If an application is built without ordering the labels in accordance with the controls, the **Choose** icon does not update the label.



Alternatively, you can use the **Navigate to field using keystrokes** to select the correct fields. To record keystrokes:

1b1 Click **Start**.

1b2 Specify the keystrokes.

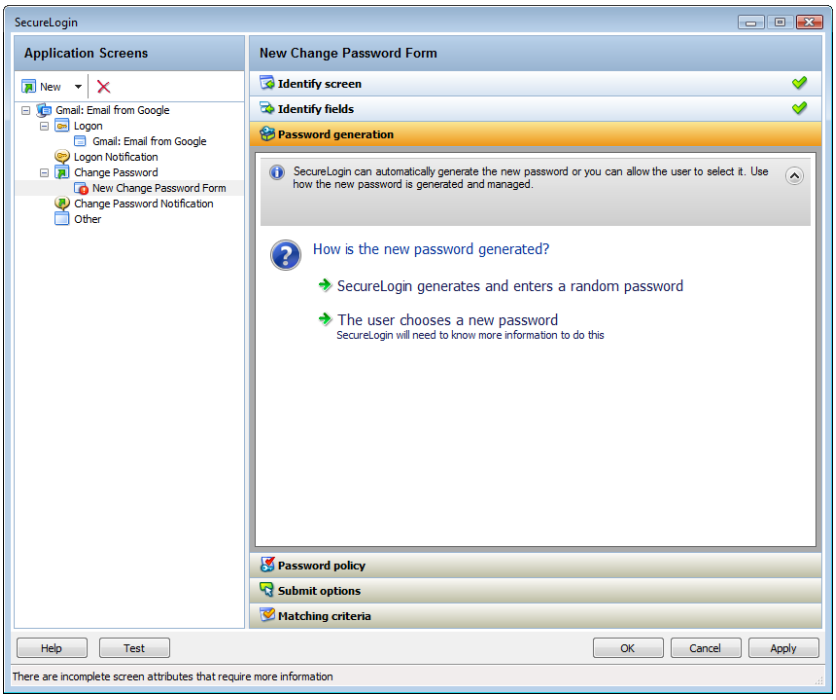
1b3 After you have recorded the keystrokes, click **Close**.

If necessary you can also define the other fields on the screen. You can define how SecureLogin handles the any radio buttons or edit boxes displayed on the **Identify fields** screen.

Generating Password

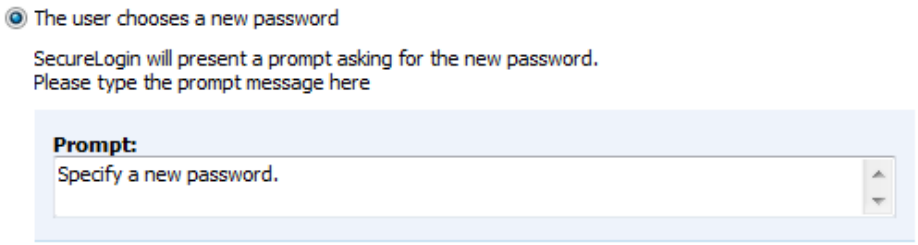
SecureLogin can generate a random password or you can allow users to specify a new password.

Figure 2-11 *The Password Generation Options*



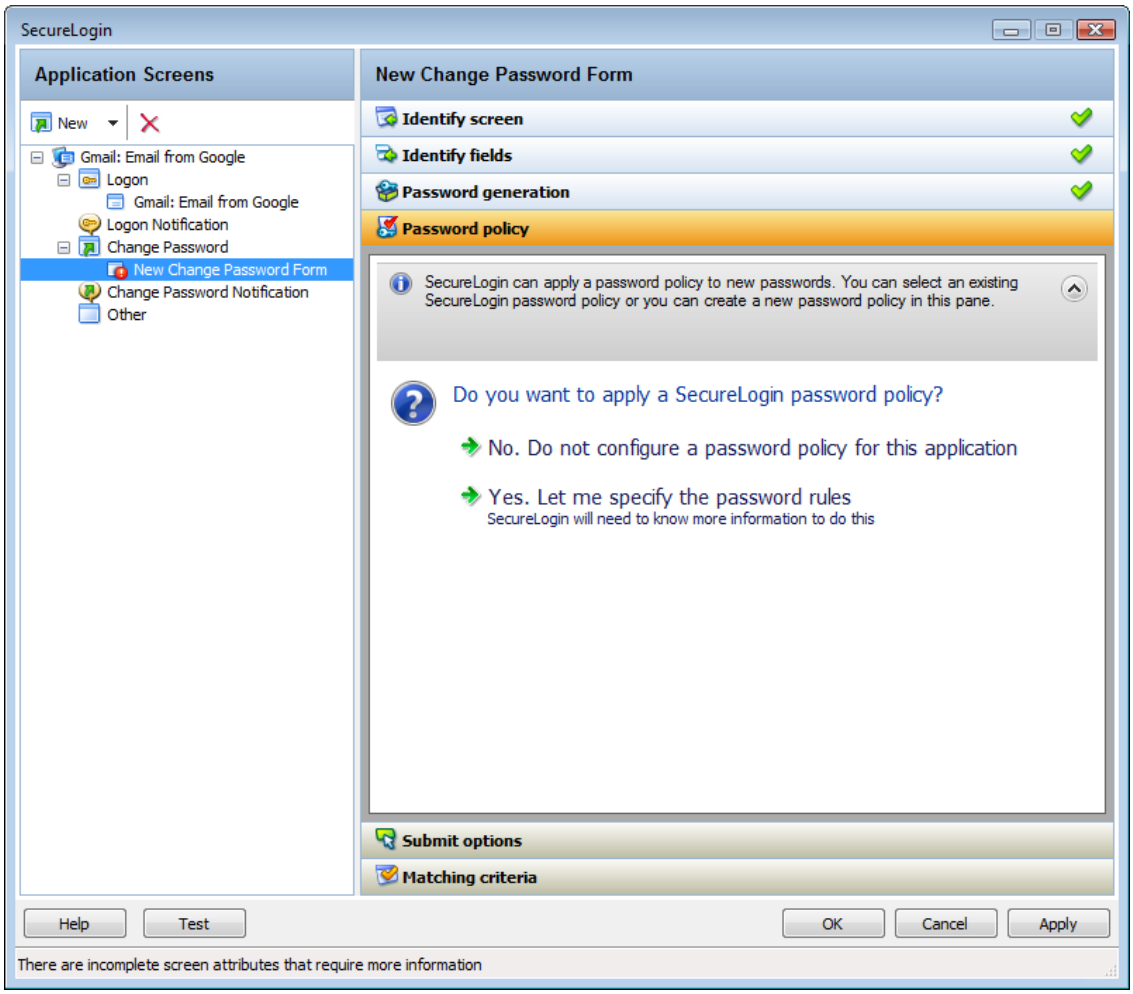
1 If you select **SecureLogin generates and enters random password**, SecureLogin generates a random password.

2 If you select **The user chooses a new password**, specify how to manage the password generation. SecureLogin prompts the user to for a new password. You must specify the prompt that is displayed to the user.



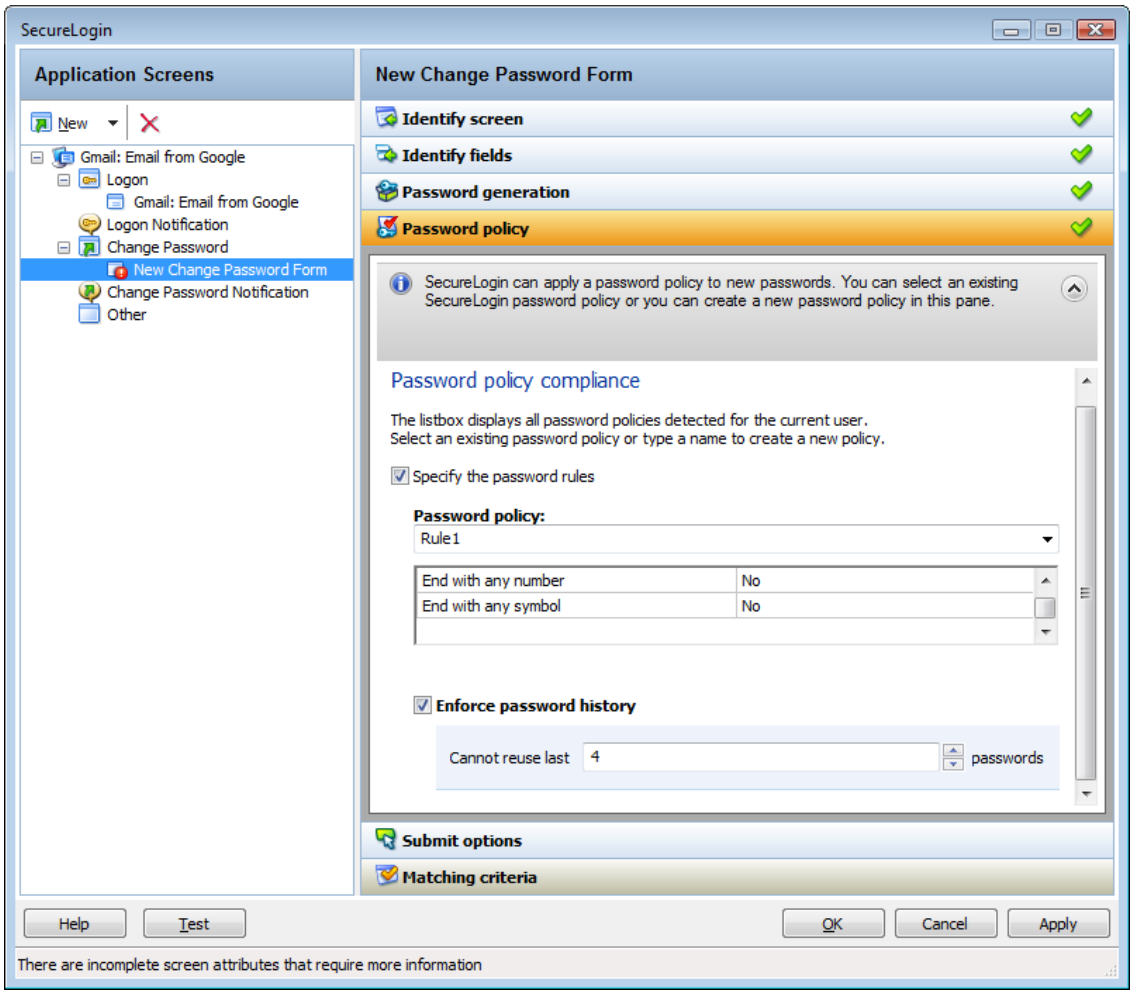
Selecting a Password Policy

1 Use the **Password Policy** menu to apply a password policy to an application. You can create a new policy or apply an existing password policy.



2 If you select **No. Do not configure a password policy for this application**, SecureLogin does not validate the password specified by the user.

3 If you select **Yes. Let me specify the password rules**, you can define any or all of the following options:



- **Create a New Password Policy:** Creates a new password policy.
  1. In the **Password policy** field, specify a name for the policy.
  2. Specify the rules for the policy.

     Refer Table 2-1, “Setting Password Policy,” on page 39 for information on setting the password policy rules.
- **Select an Existing Policy:** If you have previously configured a password policy, select the policy in the **Password Policy** drop-down list.
- **Enforce Password History:** Select this option to stop users from reusing a previous password. You can specify the number of previous passwords that must not be used.

Table 2-1 *Setting Password Policy*

Rule	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.

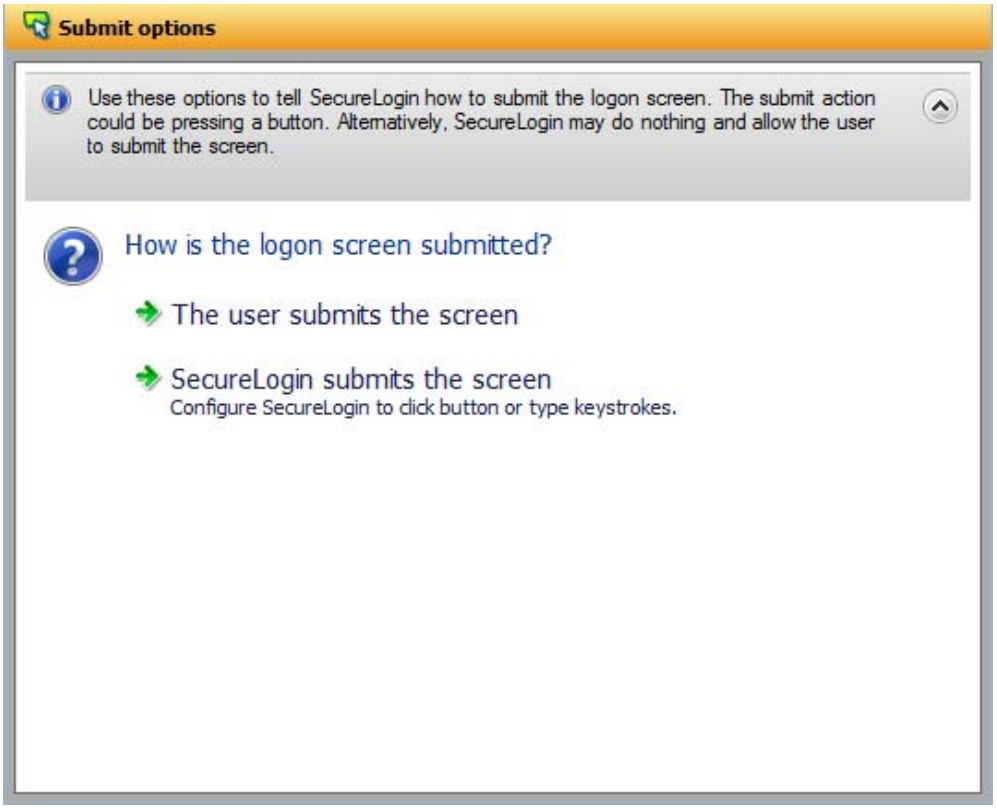
Rule	Value to Be Provided	Description
Minimum punctuation characters	Punctuation characters	Defines the minimum number of punctuation characters allowed in a password. Value to be provided should be a whole number.
Maximum punctuation characters	Punctuation characters	Defines the maximum number of punctuation characters allowed in a password. Value to be provided 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**	Disallows the use of repeated characters, or the use of the same character in succession. If this option is set to **No**, characters can be repeated. 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 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**	**No**/**Yes**/**Yes, case insensitive**
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.

Rule	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 all other policies that specify what the first character of the password should be.
Begin with any number	**No**/**Yes**	Enforces the use of a numeric character as the first character of the password. The default value is **No**. If this option is set to **Yes**, it automatically disables all other policies that specify what the first character of the password should be.
Begin with any symbol	**No**/**Yes**	Enforces the use of a symbol character as the first character of the password. The default value is **No**. If this option is set to **Yes**, it automatically disables all other policies that specify what the first character of the password should be.
End with any Alpha character	**No**/**Yes**	Enforces the use of an alphabetic character as the last character of the password. The default value is **No**. If this option is set to **Yes**, it automatically disables all other policies that specify what the password should end with.

Rule	Value to Be Provided	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.

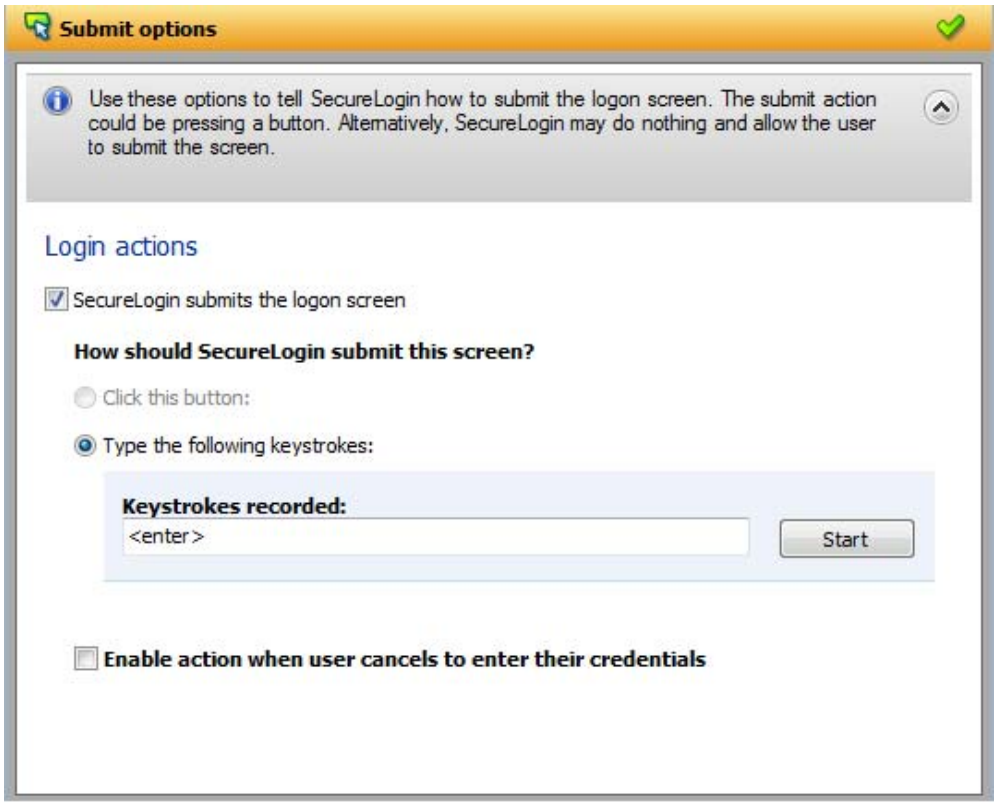
Defining the Submit Options

1 Use the **Submit options** menu to define how SecureLogin submits the change password screen.



1 If you select **The user submits the screen**, SecureLogin does nothing and the user must manually submit the screen.

2 If you select **SecureLogin submits the screen**, specify the action that SecureLogin must take to submit the screen.



You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the change password screen. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes that SecureLogin enters to submit the change password screen.

  To record keystrokes:

  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct users to this website:** Specify a URL to go to after users submit the change password screen.

  You can also specify the SecureLogin action when users cancel saveing their credentials. For this, select **Enable action when user cancels to change their password**. You can specify one of the following actions:

  - **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
  - **Type the following keystrokes:** Define the commands or keystrokes that SecureLogin enters to submit the login screen.

    To record keystrokes:

    1. Click **Start**.

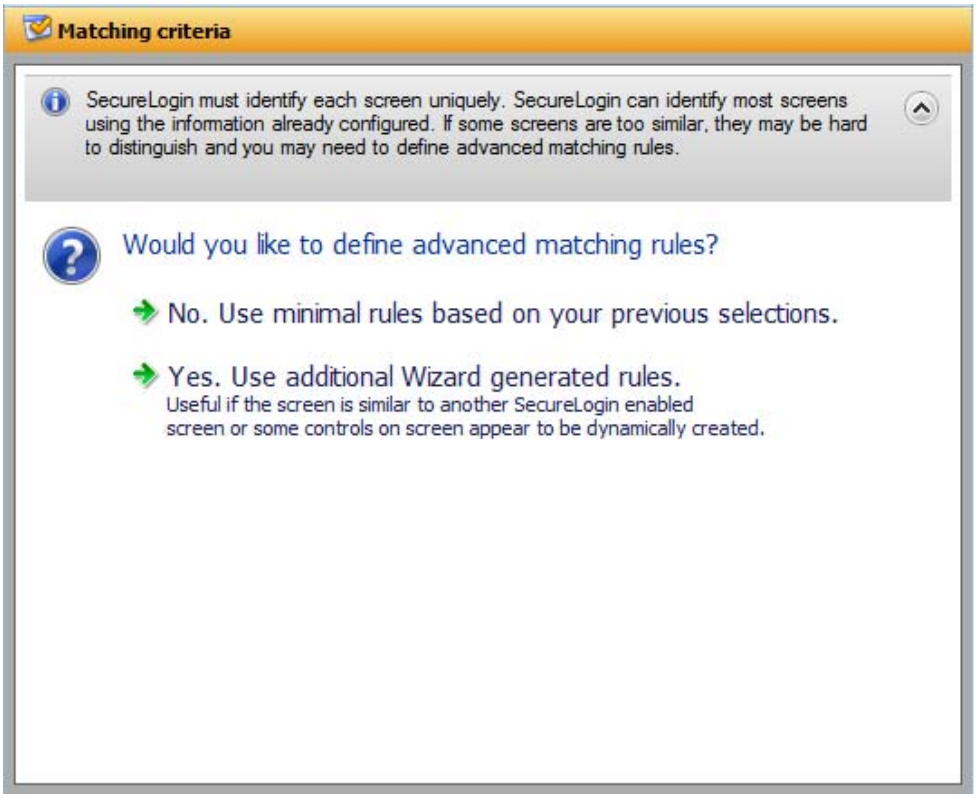
2. Specify the keystrokes.
3. After you have recorded the keystrokes, click **Close**.

Re-direct users to this website: Specify a URL to go to when users cancel the change password prompt.

Defining the Matching Criteria

SecureLogin must uniquely identify each application screen in order to run an application definition. If SecureLogin cannot uniquely identify a particular application screen, you can manually define the matching criteria.

Figure 2-12 *Setting the Matching Criteria*



1 If you select **No. Use minimal rules based on your previous selections**, SecureLogin uses the rules defined in previous attribute panels to identify and handle changing a password.

2 If you select Use additional Wizard generated rules, you can add, modify, or remove rules. Your matching criteria must include at least one rule.

3 By default, **Use Wizard generated rules** is selected. The **Rules** text box lists the controls that are detected by SecureLogin. You can add new rule by dragging the **Choose** icon to a specific control and clicking **Show me** to confirm that SecureLogin has identified the correct control.

Change Password Notification

A change password notification is a message that an application displays after the user submits the new password. This might be either a confirmation or error message.

IMPORTANT: A change password notification cannot be created if a change password form is not defined.

The change password notification lets users know whether the password is successfully changed. If a change password notification is not defined, SecureLogin prompts the user to verify if the password is changed successfully.

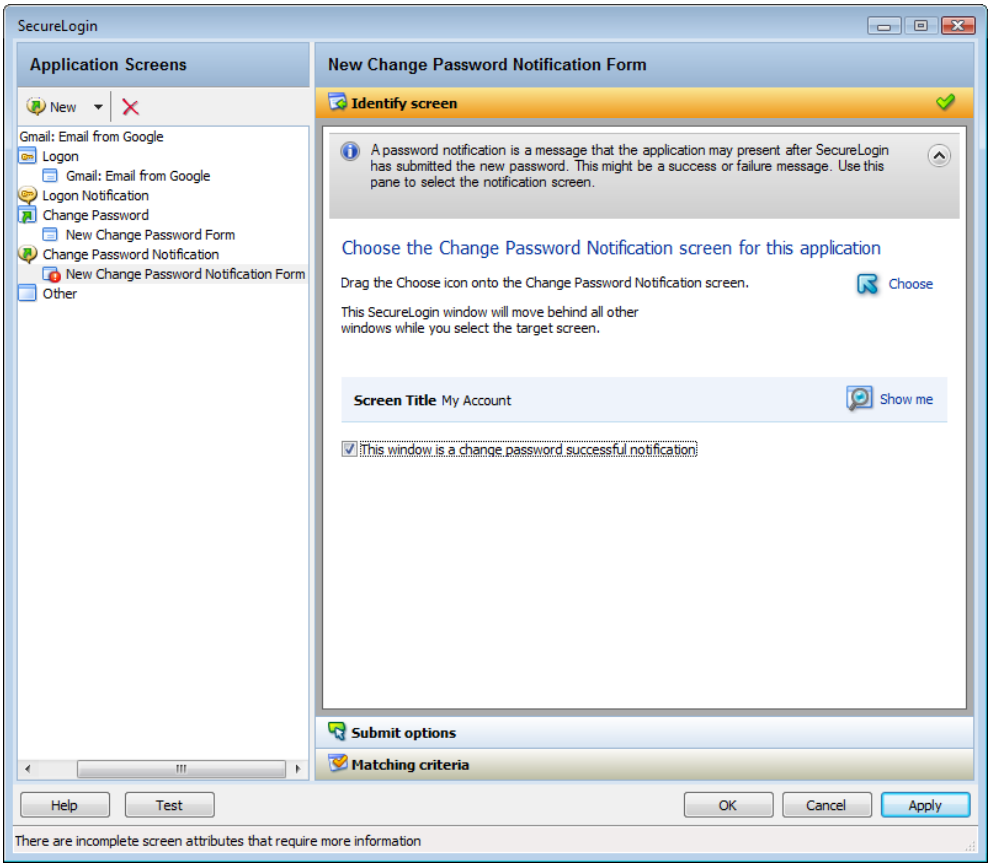
To handle change password notifications, You must complete the following tasks:

- “Identifying the Screens” on page 45
- “Defining the Submit Options” on page 46
- “Handling Errors” on page 49
- “Defining Matching Criteria” on page 50

Identifying the Screens

SecureLogin must uniquely identify the change password notification screen to handle the notification. You can the **Identify screen** attribute to select or change the notification screen.

Figure 2-13 *The Change Password Notification Screen*



1 Select the Change Password Notification screen by dragging the **Choose** icon to the screen. The title of the screen is displayed.

2 Click the **Show me** icon to highlight the selection made by the wizard.

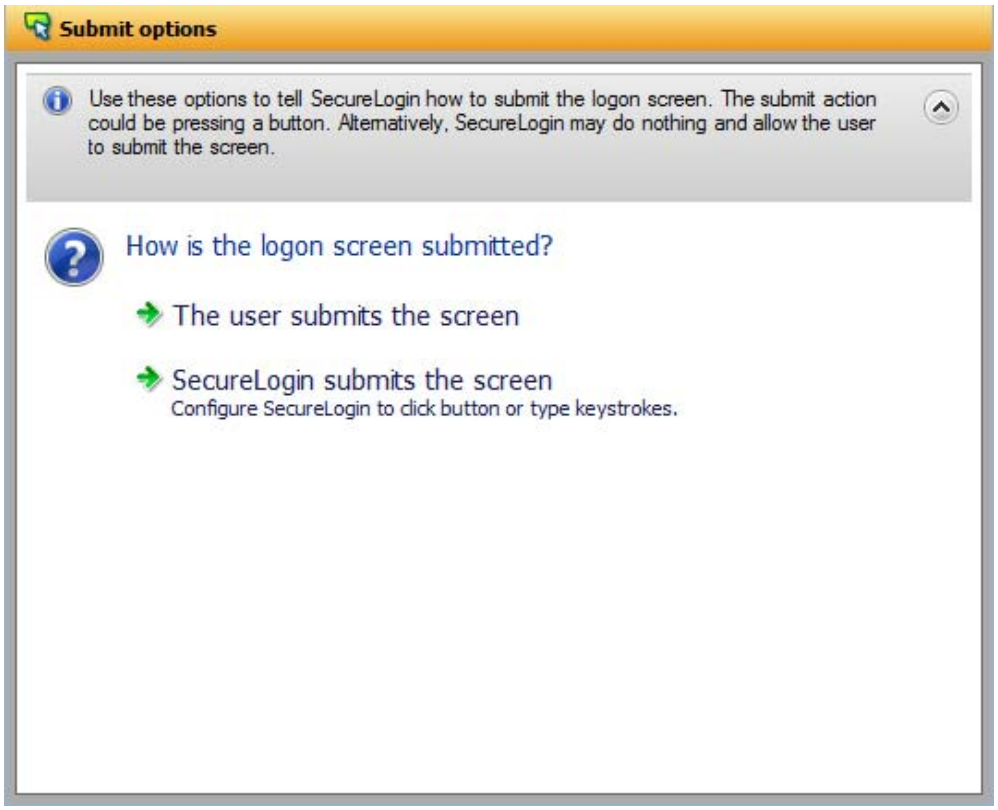
3 If you select **This window is a change password successful notification**, you must next define the submit options. See “Defining the Submit Options” on page 46.

4 If you do not select **This window is a change password successful notification**, define “Handling Errors” on page 49.

SecureLogin updates the credentials for the application immediately after a password is changed successfully. It does it either automatically or by asking the user.

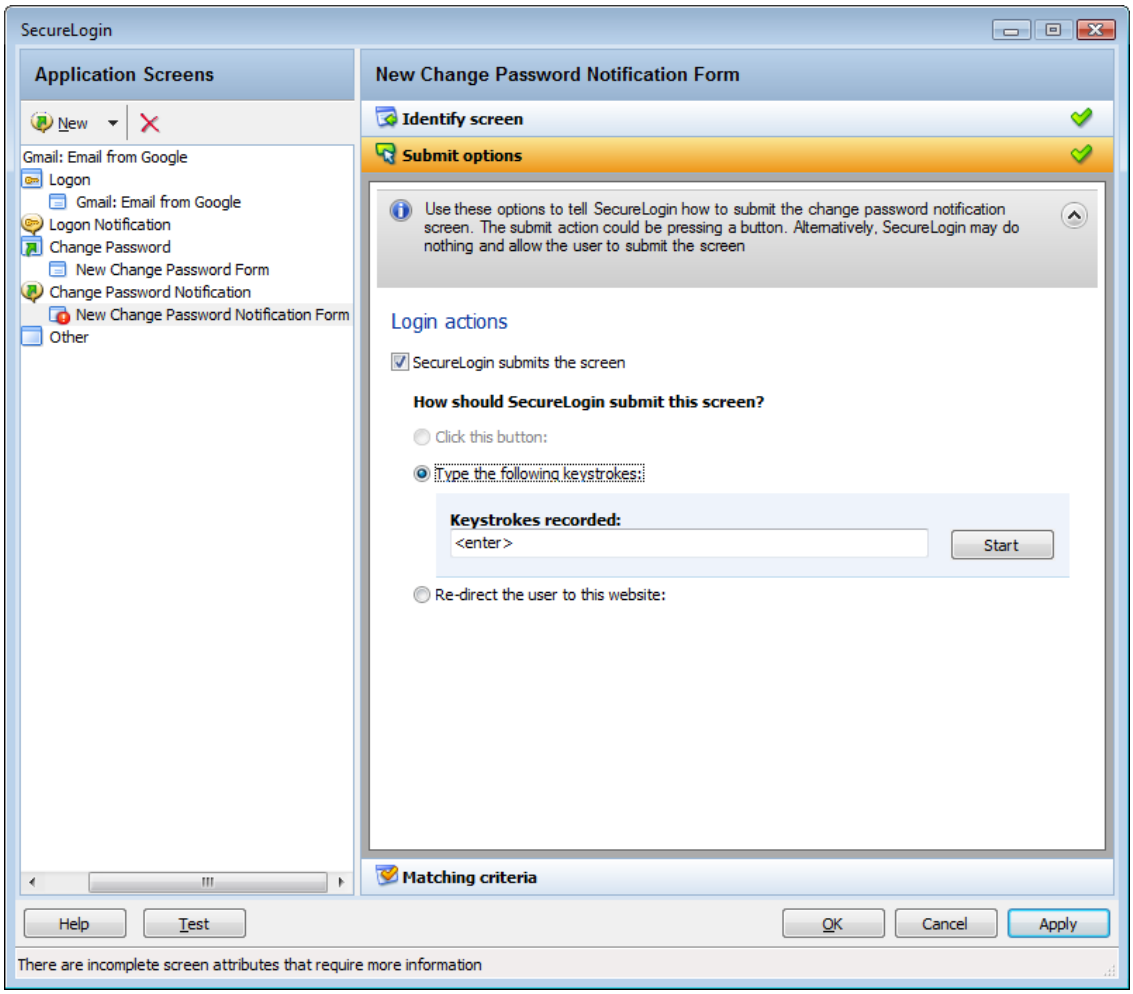
Defining the Submit Options

1 Use the **Submit options** to define what to do when the change password notification is displayed.



2 Select **The user submits the screen** to allow users to handle any change password notification screens.

3 If you select **SecureLogin submits the screen**, specify what SecureLogin must do to handle a change password notification screen.



You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes that SecureLogin enters to submit the login screen.

  To record keystrokes:

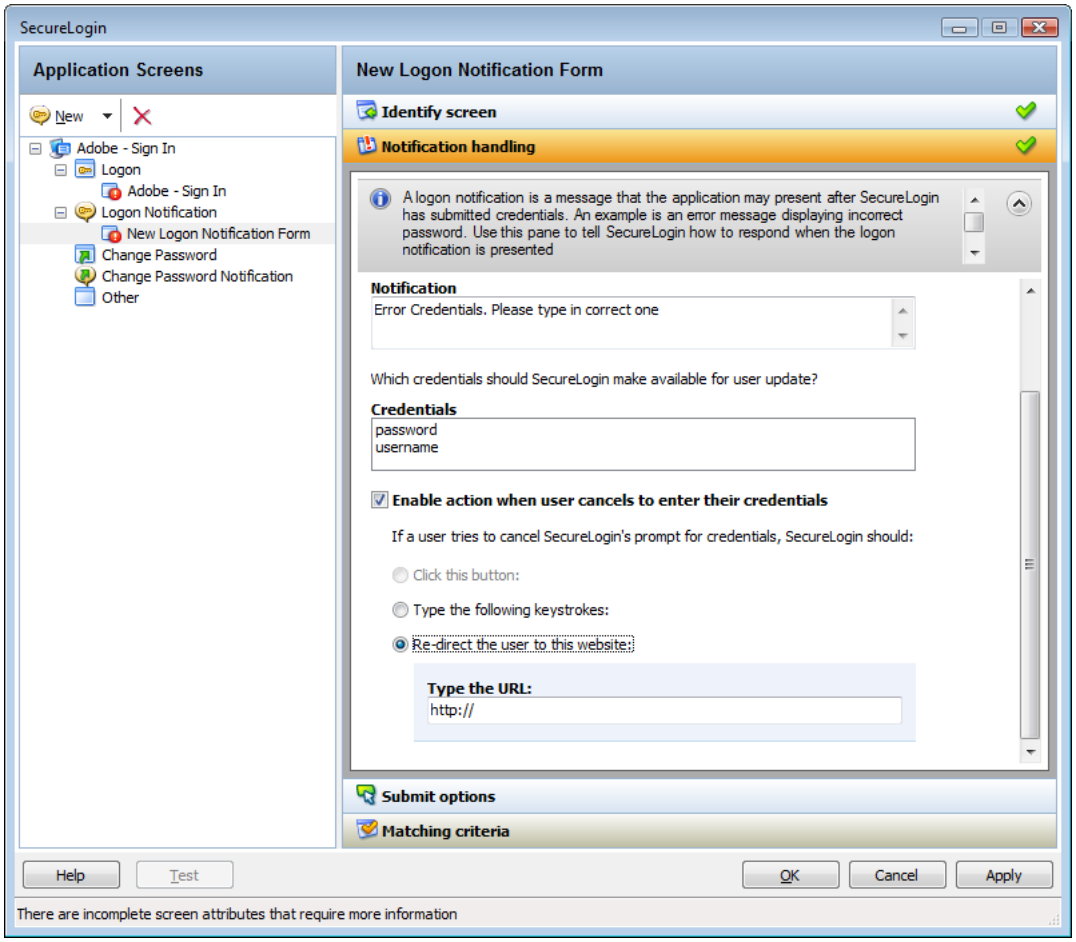
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct the user to this website:** Specify a URL to go to when a user cancels the prompt for credentials. You can redirect users to the login screen and force them to specify the login credentials again.

NOTE: If the label text for the control is empty or incorrect:

- Click **Show me** to check if the selected control is correct.
- If **Show me** does not highlight the expected control, update it by using the **Choose** icon or by using the **Type the following keystrokes** option.

The **Choose** icon might not update the label if the application is built without ordering labels in accordance with controls.

- **Enable action when user cancels to enter their credentials:** If you select this option, specify what action SecureLogin takes when a user cancels credential entry.



You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a cancels the promptfor credentials. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes that SecureLogin enters when the user cancels the prompt for credentials.

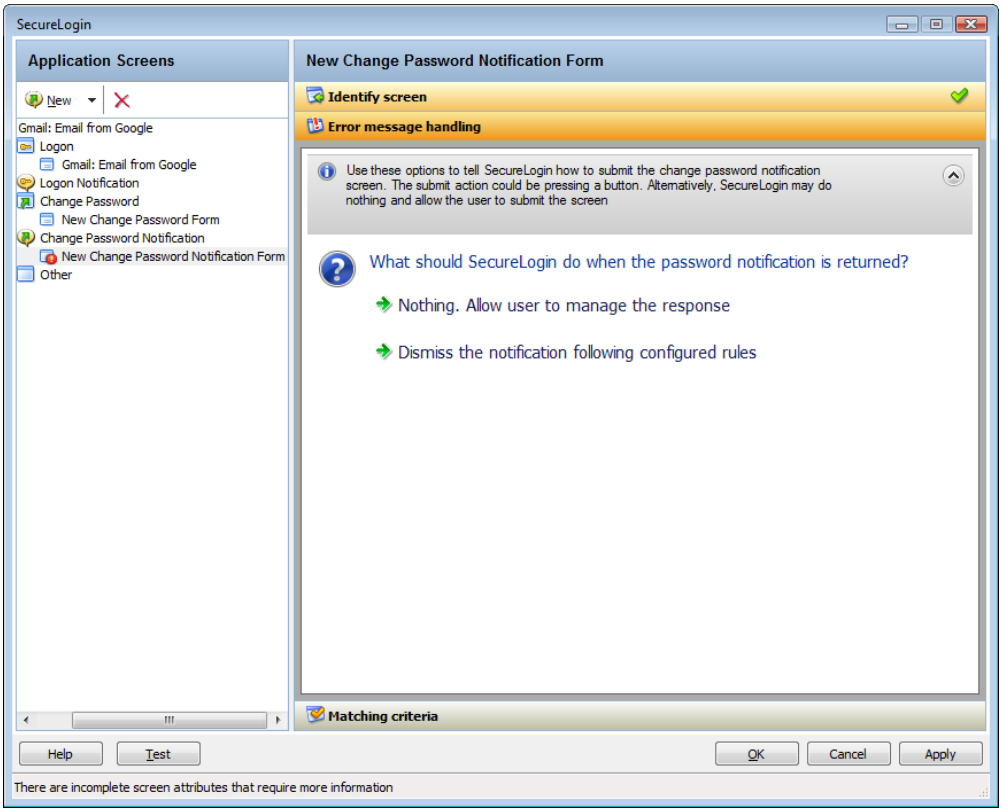
  To record keystrokes:

  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct the user to this website:** Specify a URL to go to when a user cancels the prompt for credentials. You can redirect users to the login screen and force them to specify the login credentials again.

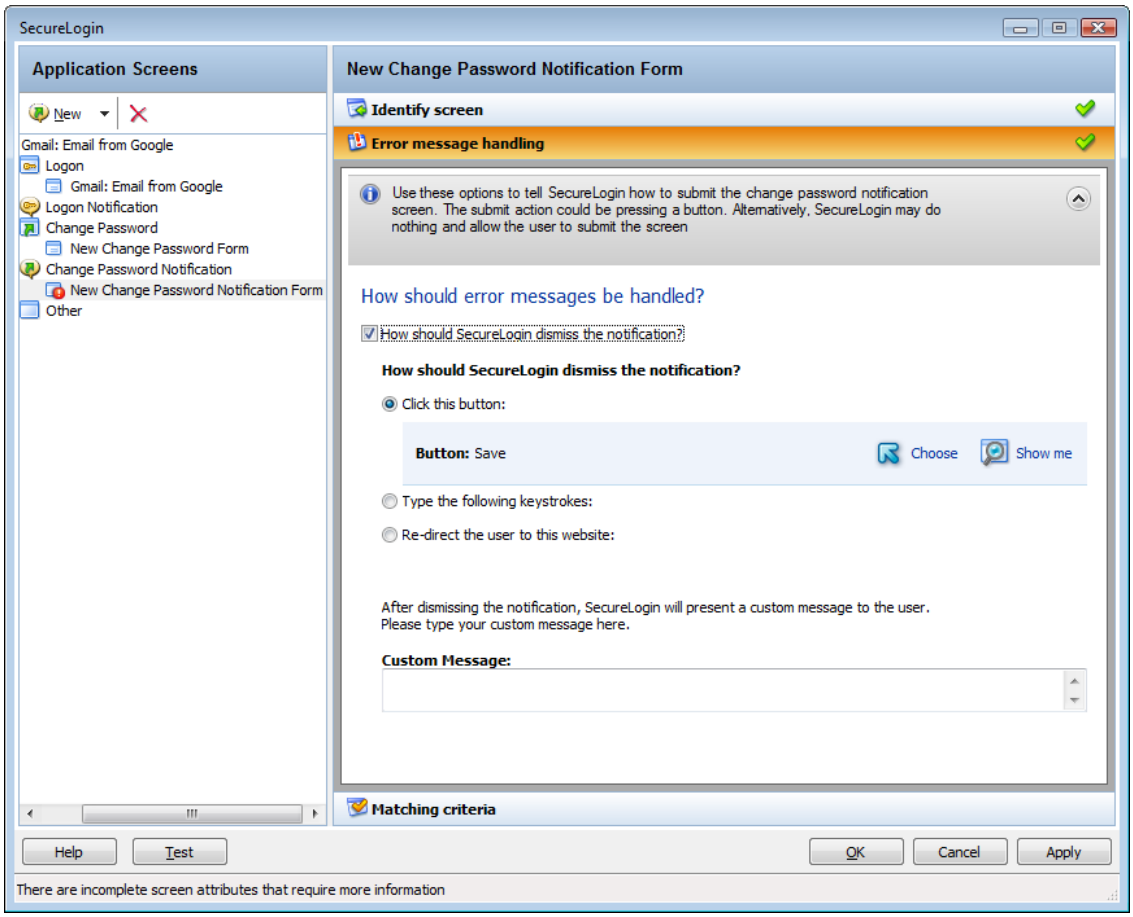
Handling Errors

If a change password notification screen does not confirm a password change, you must define rules for SecureLogin to handle the notification.

Figure 2-14 *The Change Password Notification Screen*



1. If you select **Nothing. Allow user to manage the response**, it displays the notification from the application. Users can manage the response.
2. If you select **Dismiss the notification following configured rules**, define the action that SecureLogin must take.



You can do any of the following:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** efine the commands or keystrokes that SecureLogin enters to submit the login screen.

  To record keystrokes:

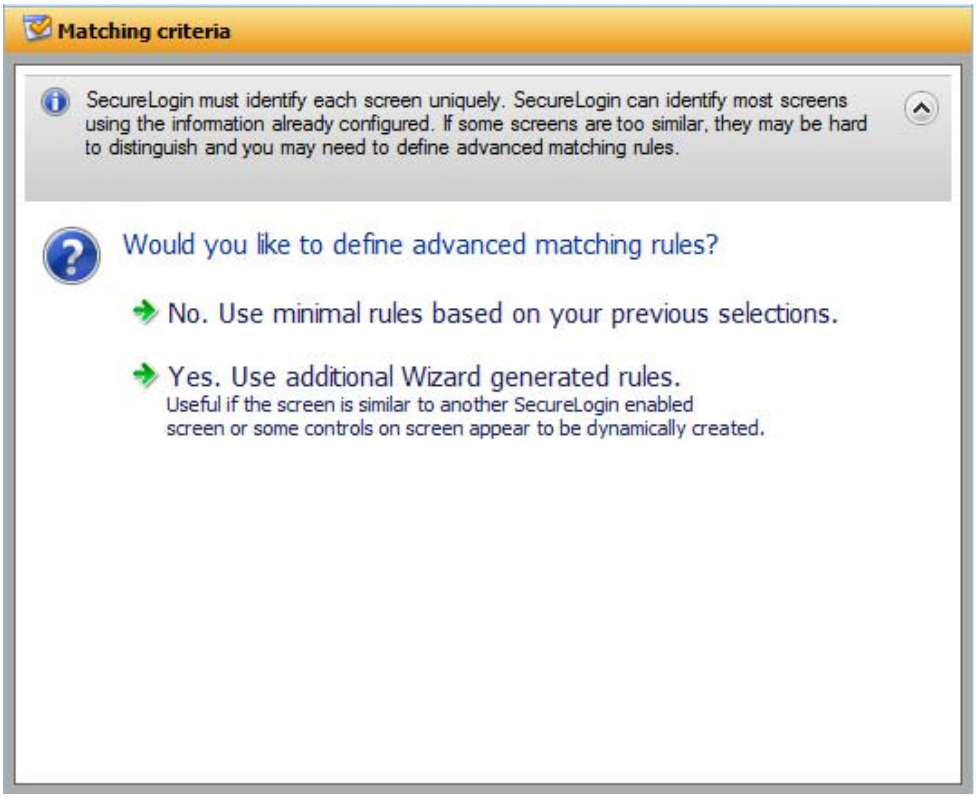
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct the user to this website:** Specify a URL to go to when a user cancels the promptfor credentials. You can redirect users to the login screen and force them to specify the login credentials again.

In the **Custom Message** text field, specify a custom message to be displayed to the users.

Defining Matching Criteria

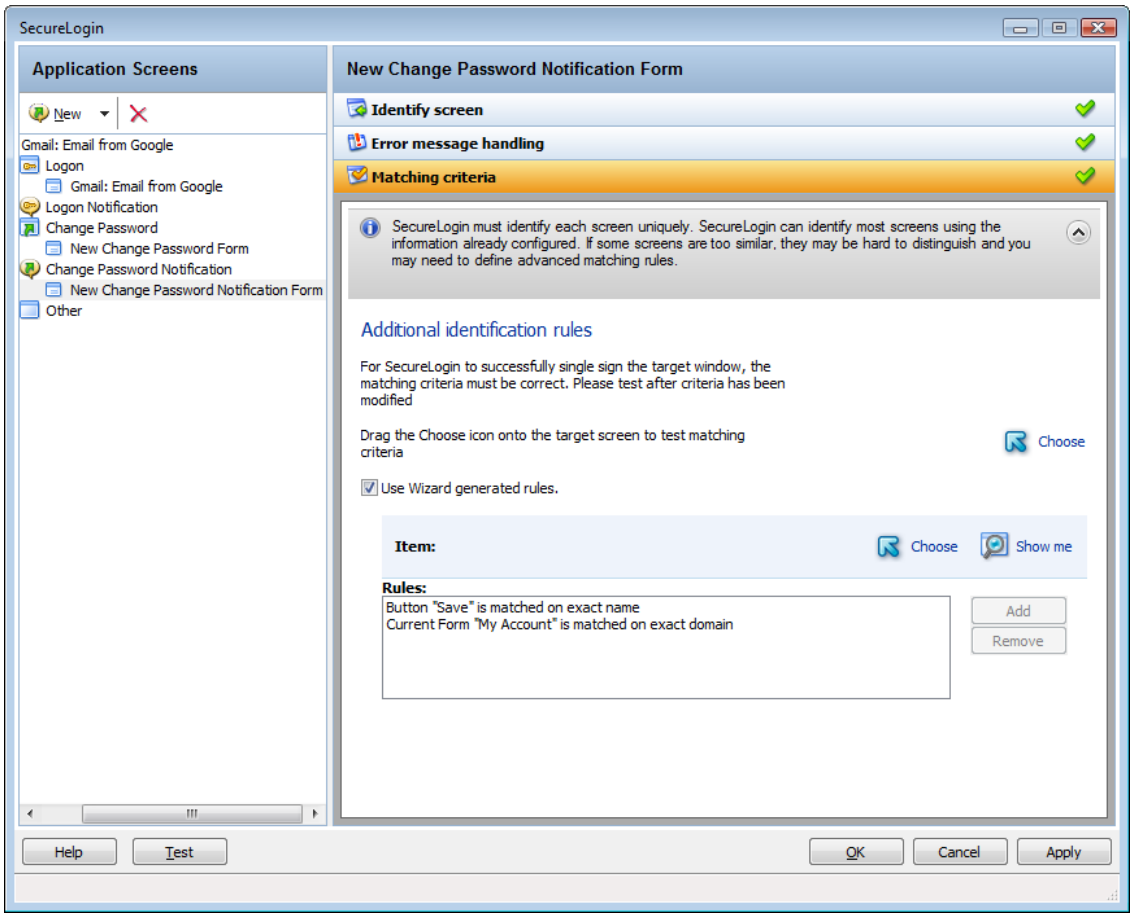
SecureLogin must uniquely identify each application screen in order to run an application definition. If SecureLogin cannot uniquely identify a particular application screen, you can manually define the matching criteria.

Figure 2-15 *Setting the Matching Criteria*



1 If you select **No. Use minimal rules based on your previous selections**, SecureLogin uses the rules defined in previous attribute panels to identify and handle an application.

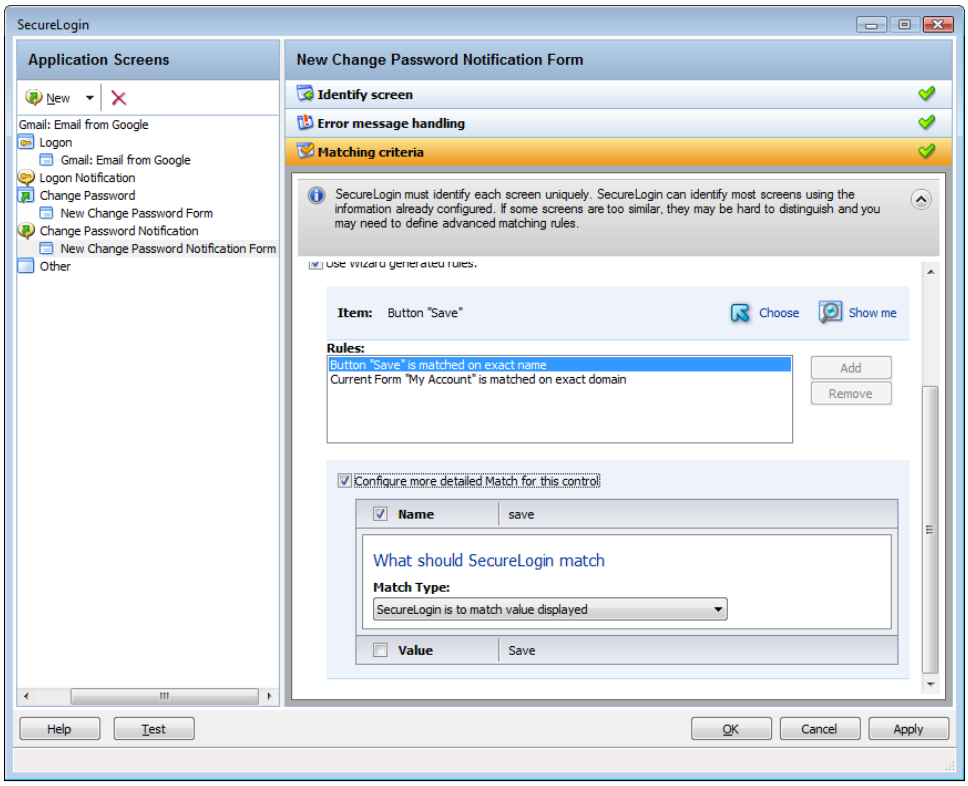
2 If you select Yes. Use additional Wizard generated rules, you can add, modify, or remove rules. Your matching criteria must include at least one rule. After you have selected this option, the following screen appears:



By default, **Use Wizard generated rules** is selected. The **Rules** text box lists the controls detected by SecureLogin. You can add a new rule by dragging the **Choose** icon to a specific control and clicking **Show me** to confirm that SecureLogin has identified the correct control.

To modify a rule for a control:

1 Select the rule you want to edit, then click **Configure more detailed match for this control**



2 Define what SecureLogin must match. You can set the following matching rule:

- **SecureLogin is to match value displayed:** If you select this option, SecureLogin only matches those screens that exactly match the displayed text and rules identified.

To test a regular expression:

1 Click **Test Match** to verify if your regular expression is correct. If a regular expression does not match any control on the application screen, SecureLogin prompts you to verify your regular expression and select the correct control.

To delete a rule:

1 Select the rule, then click **Remove**.

Other

Use **Other** menu to define rules for the application definition to handle any other application screens, such as splash screens, automating menu navigation, or redirecting users to a Web site. To handle such screens, You must complete the following tasks:

- “Identifying the Screen” on page 54
- “Identifying the Fields” on page 54
- “Defining the Submit Options” on page 55
- “Defining Matching Criteria” on page 58

Identifying the Screen

SecureLogin identifies a login screen for which you want to create an application definition.

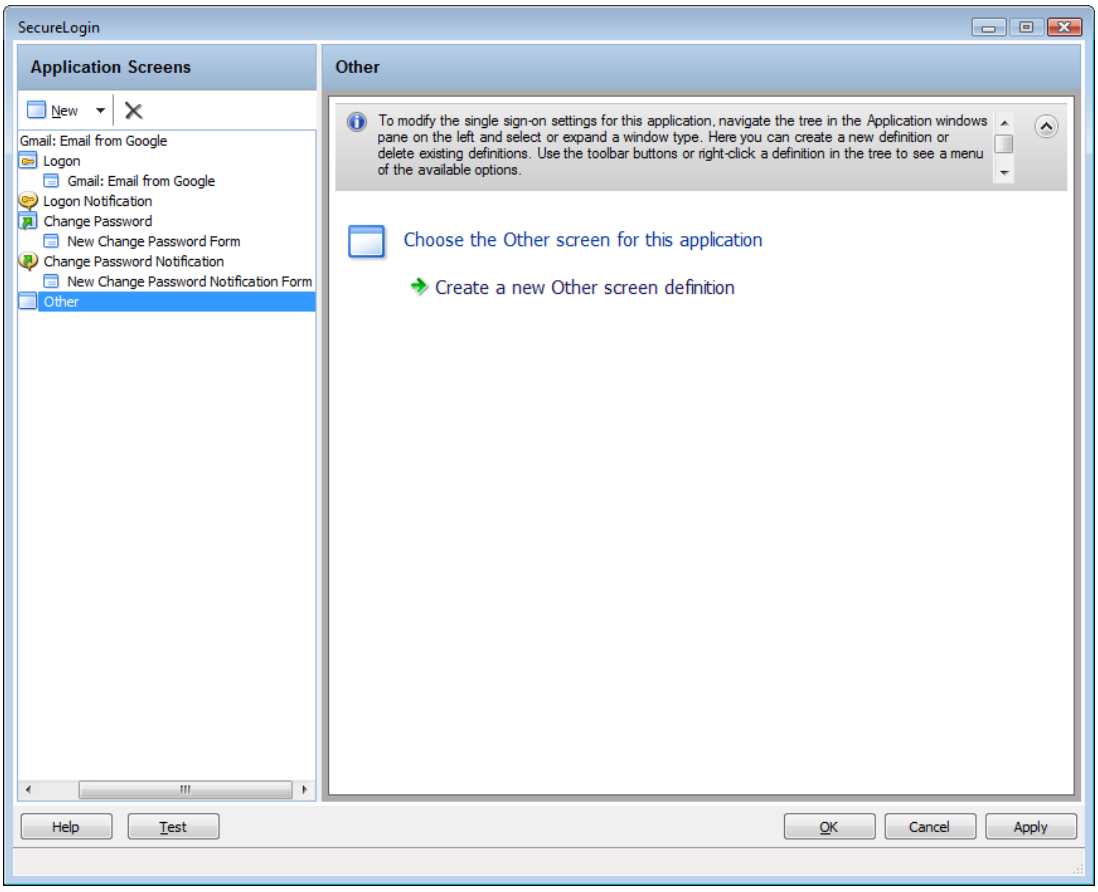
1. You can use the **Identify screen** attribute to select or review the login screen selected by the wizard.
2. Select the login screen by dragging the **Choose** icon to the login screen or by recording keystrokes. The title of the login screen is displayed.
3. Click the **Show me** icon to highlight the selection made by the wizard.

Identifying the Fields

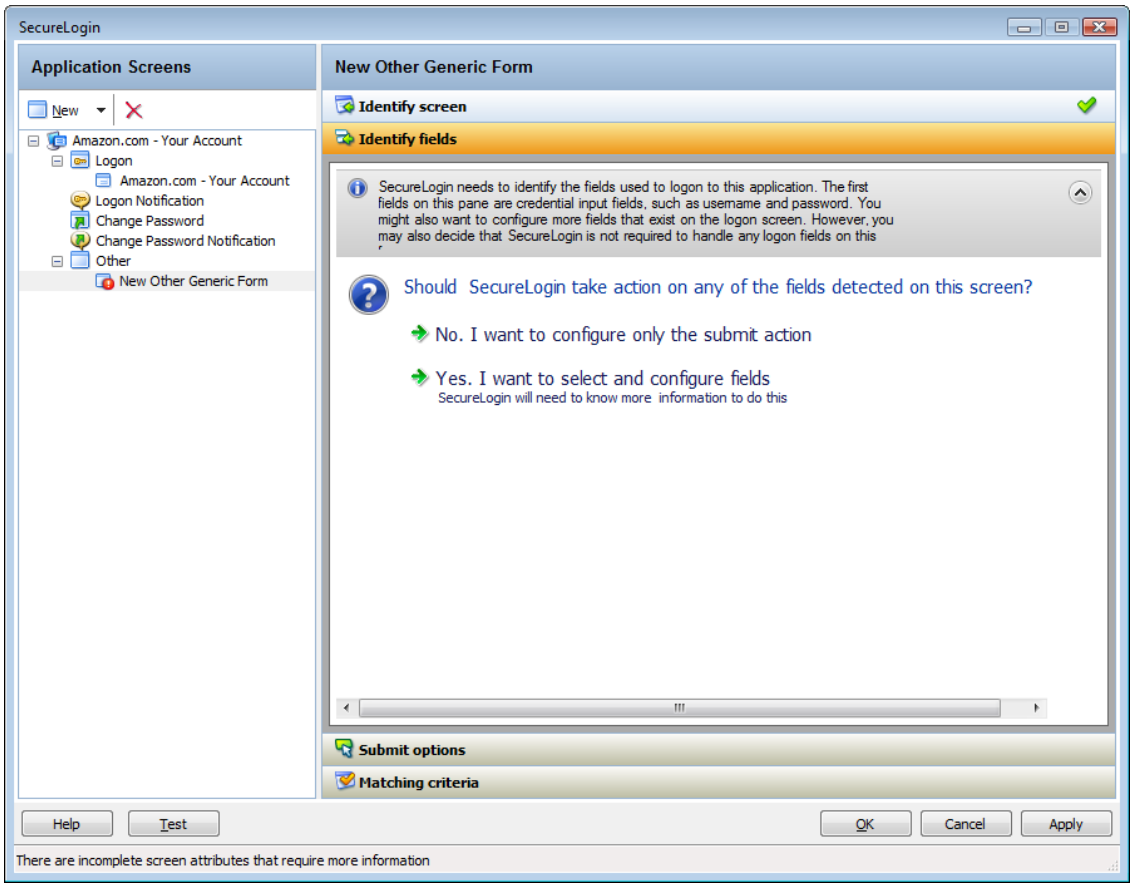
By default, SecureLogin does not select any fields on the screen. You must define the selection.

NOTE: If the screen you have selected does not contain any controls, **Identify fields** is automatically selected.

Figure 2-16 *Selecting a Screen*



1. After selecting a screen, define what SecureLogin must do when it detects any fields on the screen.

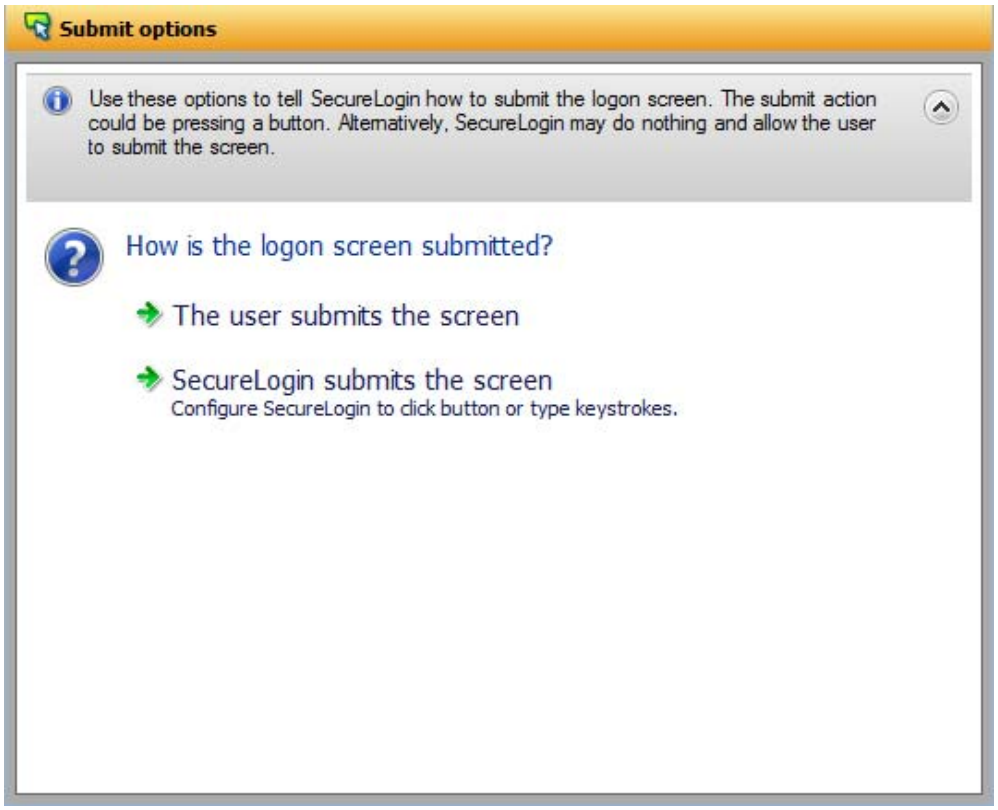


2 If you select **No. I want to configure only the submit action**, define only the submit options. Continue with "Defining the Submit Options" on page 55 to define the submit options.

3 If you select **Yes, I want to select and configure fields**, then you must identify the controls you want SecureLogin to handle and the actions it should take. The actions that can be taken depend on the control types that are identified.

Defining the Submit Options

1 Use the **Submit option** menu to define how SecureLogin must submit the login screen.



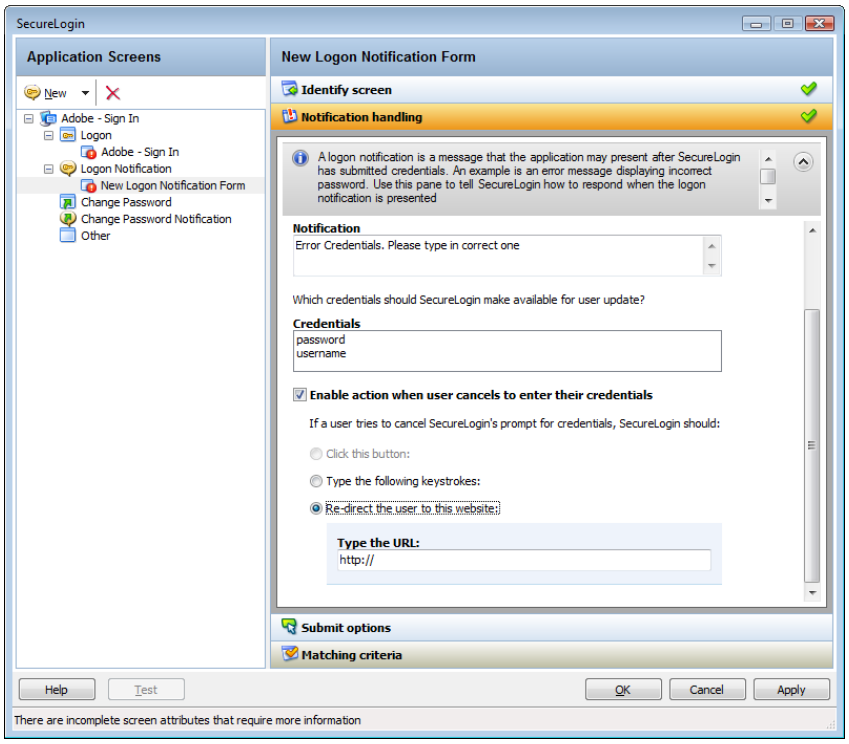
2 If you select **The user submits the screen**, SecureLogin does nothing and the user must manually submit the login screen.

3 If you select **SecureLogin submits the screen**, specify the action that SecureLogin must take to submit the login screen.

You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes that SecureLogin enters to submit the login screen. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct the user to this website:** Specify a URL to go to when a user cancels the prompt for credentials. You can redirect users to the login screen and force them to specify the login credentials again.
- **Enable action when user cancels to enter their credentials:** If you select **Enable action when user cancels to enter their credentials**, specify what action SecureLogin takes when a user cancels to enter their credentials.

Figure 2-17 *Defining Action When User Cancels Prompt for Credentials*



You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a cancels the prompt for credentials. Select and highlight the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes SecureLogin enter when user cancels the prompt for credentials. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct the user to this website:** Specify a URL to go to when a user cancels the prompt for credentials. You can redirect users to the login screen and force them to specify the login credentials again again.

If you select this option, you must also specify the action SecureLogin when users cancel when prompted to save their credentials. You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen. Select and highlight the button by dragging the **Choose** icon and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes that SecureLogin enters to submit the login screen. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.

- **Re-direct the user to this website:** Specify a URL to go to when a user cancels the prompt for credentials. You can redirect users to the login screen and force them to specify the login credentials again.

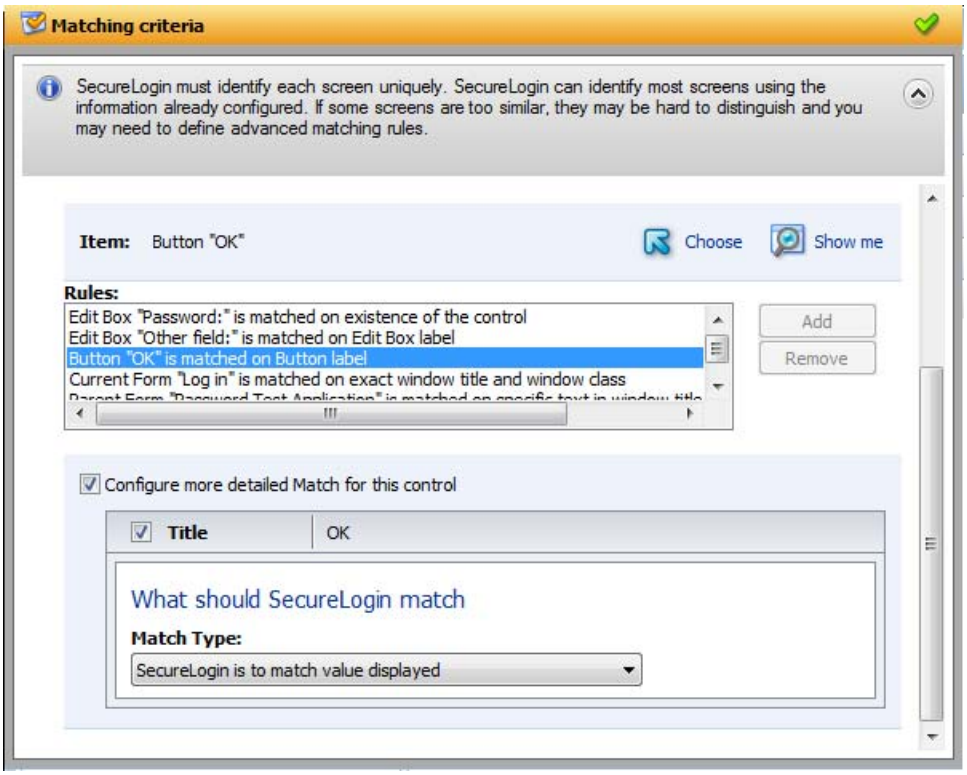
Defining Matching Criteria

SecureLogin must uniquely identify each application screen in order to run an application definition. If SecureLogin cannot uniquely identify a particular application screen, you can manually define the matching criteria.

1. If you select **No. Use minimal rules based on your previous selections**, SecureLogin uses the rules defined in previous attribute panels to identify and handle an application.
2. If you select **Yes. Use additional Wizard generated rules**, you can add, modify, or remove rules. Your matching criteria must include at least one rule. After you have selected this option, the following screen appears:
3. By default, **Use Wizard generated rules** is selected. The **Rules** text box lists the controls that are detected by SecureLogin. You can add new rule by dragging the **Choose** icon to a specific control and clicking **Show me** to confirm that SecureLogin has identified the correct control.

   To modify a rule for a control:

   3a Select the rule you want to edit, then click **Configure more detailed match for this control**.



   3b Define what SecureLogin must match. You can set one of the following matching rules:

   - **SecureLogin is to match value displayed:** f you select this option, SecureLogin only matches those screens that exactly match the displayed text and rules identified.
   - **SecureLogin is to match specific part of the identified ctrl:** If you select this option, you must use a regular expression to define and match the screen features. You cannot use special characters in a regular expression.

3c Click **Test Match** to verify if your regular expression is correct.

If a regular expression does not match any control on the application screen, SecureLogin prompts you to verify your regular expression and select the correct control.

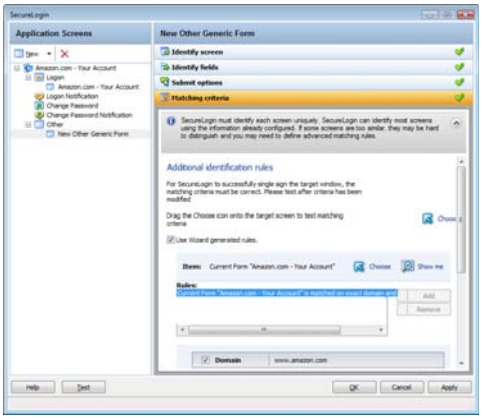
To delete a rule:

1 Select the rule, then click **Remove**.

Attributes Pane

The Attributes pane is displayed on the right side of the Application Definition Wizard interface. The attributes of the application definition for the selected screen are detailed in the Attributes pane. The attributes displayed are in relation to the selections made in the **Application Screens** pane.

Figure 2-18 *The Attributes Pane*



If the Application Definition Wizard opens automatically after detecting a login screen, it opens the **Credential Source** menu. Otherwise, it opens the **Identify screen** menu.

When you are building an application definition, the **Attributes** pane can be opened in a top-to-bottom order. You must complete each menu. After you successfully complete each menu, it is marked with a check mark .

Each menu in the **Attribute** pane has a description of the menu item. If you have not completed a menu, you are prompted to complete it before continuing to the next menu item.

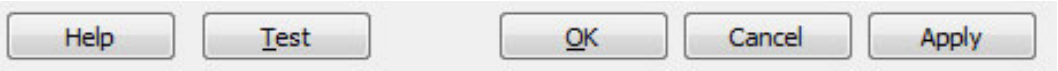
General Controls and Messages

The General controls and messages are located at the end of the Application Definition Wizard page.

Clicking **Test**, **OK**, or **Apply** synchronizes your data and saves it to the directory.

- “Help” on page 60
- “Test” on page 60
- “OK” on page 60
- “Apply” on page 60
- “Cancel” on page 60

Figure 2-19 *The General Controls and Messages*



Help

1 Click **Help** to launch the help integrated with SecureLogin. Alternatively, you can launch the help file by pressing F1.

Test

1 After you have created an application definition, click **Test** to test it . You should create and test an application definition by using a test account before distributing it.

For details on testing an application definition, refer to Chapter , “Testing Application Definitions,” on page 94.

OK

1 Click **OK** to save the changes made to the application definition and close the wizard.

Apply

1 Click **Apply** to save the changes you have made to the application definition and leave the wizard open for further editing.

Cancel

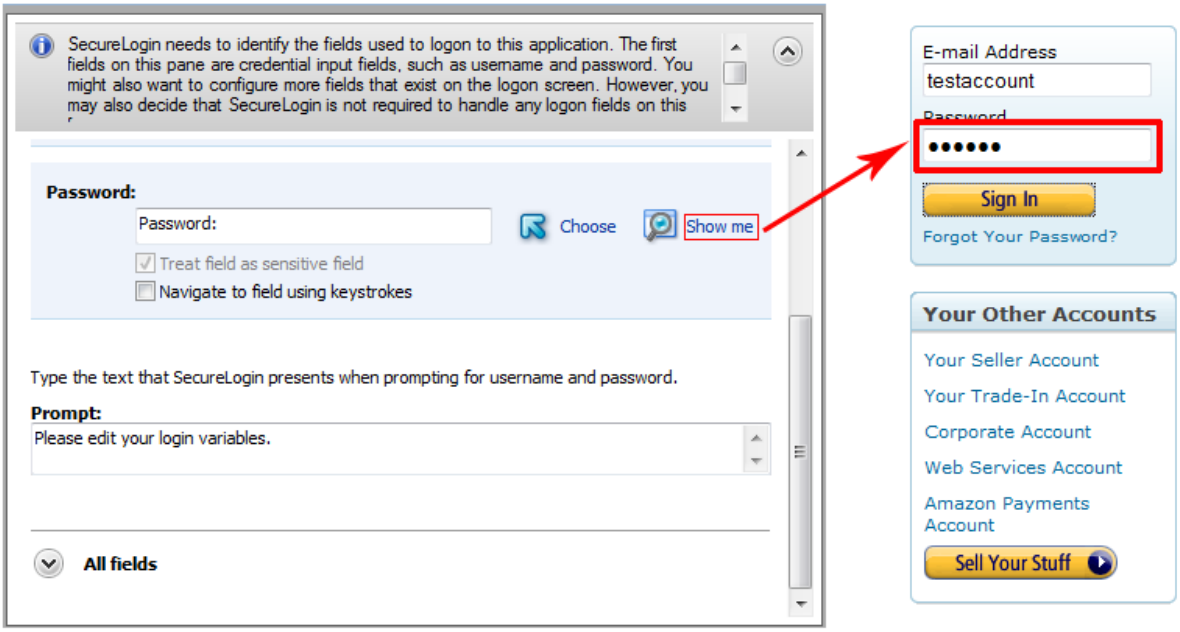
Click **Cancel** to cancel creating or editing the application definition. Clicking **Cancel** closes the Application Definition Wizard without saving any changes you have made. Unsaved changes are lost.

Selecting and Identifying Screens and Controls

You can identify the controls of an application by dragging the **Choose** icon to the fields within the application. The wizard moves behind the all the other windows and allows you to choose the correct field.

To confirm if the fields are identified correctly, click **Show me**. It highlights the identified fields.

Figure 2-20 *Identifying the Control*



SecureLogin detects most standard user interface elements. If an application uses a non-standard framework, the Application Definition Wizard does not select or highlight the controls.

For example, the wizard does not detect non-native UI framework such as Gecko, and Qt* but single sign-on can be achieved by manually scripting the application. Similarly, applications such as Mozilla* Thunderbird* 2.0.0.18 and Novell iFolder® cannot be enabled for single sign-on by using the wizards. The wizard fails to detect the control to enable these applications.

For such applications, you must identify the fields by recording keystrokes, as described in "Recording Keystrokes" on page 61.

Recording Keystrokes

SecureLogin can record keystrokes to facilitate navigation or to enter particular commands, if you cannot identify the controls. If you have difficulty in identifying the controls on the application window then select **Navigate to field** using keystrokes.

IMPORTANT: You cannot record the following keystrokes. They are reserved by Windows.

- Ctrl+Esc: This posts a journal quit message.
- Ctrl+Alt+Del: This posts a journal quit message.
- Ctrl+Break:his is part of the journal quit code.
- Ctrl+Shift+Esc: This cancels the collection of keystrokes.

You cannot type directly in the **Navigate to field by using keystrokes**, because the field displays only recorded keystrokes.

To record keystrokes:

1. Click **Start**.
2. Specify the keystrokes.
3. After you have recorded the keystrokes, click **Close**. The dialog box closes and returns you to the Application Definition Wizard.

If you make a mistake in recording the keystrokes, repeat the procedure.

Using Regular Expressions

Some dialog boxes in SecureLogin allow you to specify text to identify an application screen. The **SecureLogin needs to match** option allows you to use regular expressions as another way to uniquely identify a particular application screen.

Regular expressions are text patterns that are used for string matching. They contain a mix of plain text and special characters to indicate what kind of matching to do.

If your regular expression does not match any controls on the particular application screen, SecureLogin prompts you to check your regular expression and ensure the correct control is selected. You might need to skip special characters in your regular expression.

You can specify a regular expression such as:

Connecting to server (.*)

The (.*) specifies the value that must be captured to define the credentials. You can have one credential set for each regular expression value.

3 Using the Application Definition Wizard

The Application Definition wizard provides a unified and intuitive process that helps you manage different application types.

You use the Application Definition Wizard to define how SecureLogin behaves when you select an application for single sign-on.

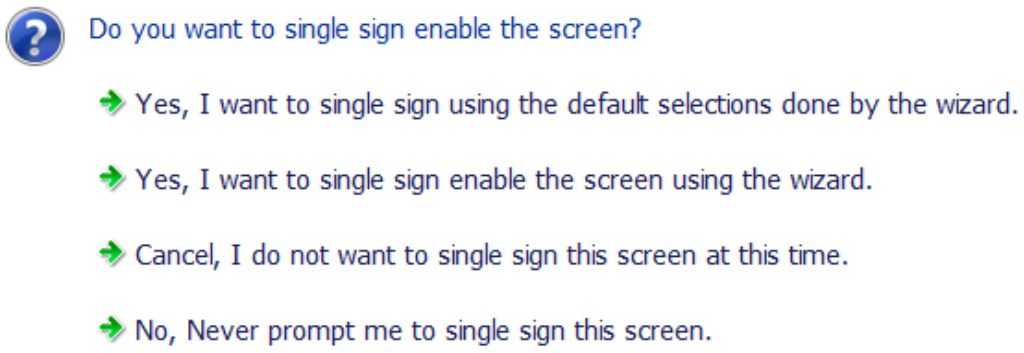
The following sections provide information on using the Application Definition Wizard to create application definitions for Web, Windows, and Java applications.

- “Launching the Application Definition Wizard” on page 63
- “Creating an Application Definition for a Web Application” on page 65
- “Creating an Application Definition for a Windows Application” on page 74
- “Creating an Application Definition for a Java Application or an Oracle Form” on page 82
- “Using a Predefined Application Definition” on page 89
- “Testing Application Definitions” on page 94
- “Deploying Application Definitions” on page 96
- “Configuring Notifications” on page 96

Launching the Application Definition Wizard

If SecureLogin is active on your workstation and if you have permission to create an application definition, a notification appears in the system tray when you launch an application. This notification notifies that the application is available for single sign-on. When you click on the notification you get the following prompt to enable single sign-on for the application.

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



SecureLogin caches the applications that are available for single sign-on and this is indicated with orange color of the SecureLogin icon. If you ignore the notification when the application is launched for the first time then, you can click on the SecureLogin icon and select the required application from the list of available applications for single sign-on.

Typically, the wizard launches when it detects a new login screen. However, you can also create or modify application definitions by using the wizard to automate handling the notification screens. You can do this in one of the following ways:

- “Automatically Launching the Wizard” on page 64
- “Launching the Wizard through the Add Application Menu” on page 64

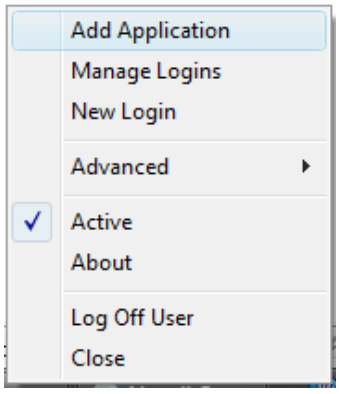
Automatically Launching the Wizard

If the Wizard option is enabled, SecureLogin automatically prompts you to use the wizard to create an application definition for the application. This is determined by the Wizard mode preference as described in Chapter 5, “Setting the Wizard Mode Preference,” on page 119.

The auto-detection dialog box does not appear if the Application Definition Wizard or the administrative management utilities are open.

Launching the Wizard through the Add Application Menu

1 Right-click the SecureLogin icon on the notification area (system tray), then select **Add Application**.



2 The Add an Application Definition dialog box appears, prompting you to drag the **Choose** icon to the application’s login window.

3 Select **Cancel, I do not want to create a new definition** if you do not want to modify the existing application definition.

When you launch an application and its application definition already exists then, the Add Application wizard displays the following additional option:

```
Cancel, open script editor so I can make changes.
```

Selecting this option, closes the wizard and opens the script editor of the application.

Creating an Application Definition for a Web Application

A Web application is an application that runs on a Web browser. You can create an application definition for a Web application by accepting the default selections in the wizard, or you can manually select the attributes required for the application definition.

- "Prerequisites" on page 65
- "Using the Default Selections for an Application Definition" on page 65
- "Manually Defining the Attributes for an Application Definition" on page 67

Prerequisites

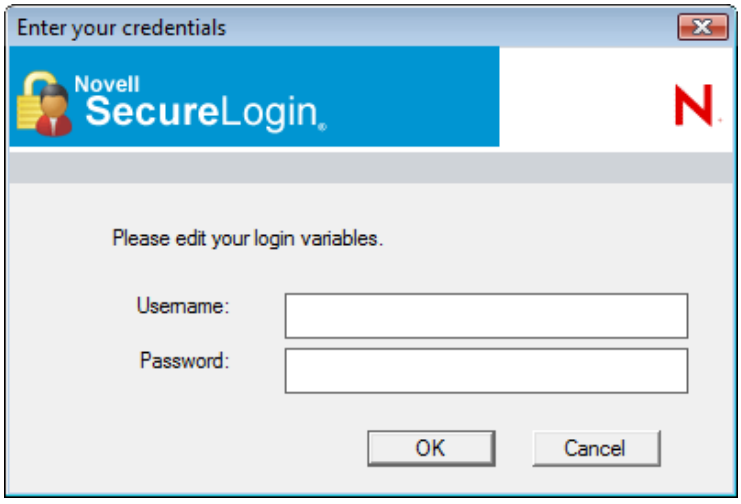
- Close all open SecureLogin prompts.
- Verify if you have permissions to create an application definition. See Chapter 5, "Setting the Wizard Mode Preference," on page 119.
- Ensure that SecureLogin is running on your workstation.

Using the Default Selections for an Application Definition

1. Ensure that you have completed the prerequisites in "Prerequisites" on page 65.
2. Launch the Web application for which you want to enable single sign-on.

   SecureLogin detects the application and prompts you to enable single sign-on.
3. Select **Yes, I want to single sign using the default selections done by the wizard**.

   The Enter your Credentials dialog box is displayed.



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

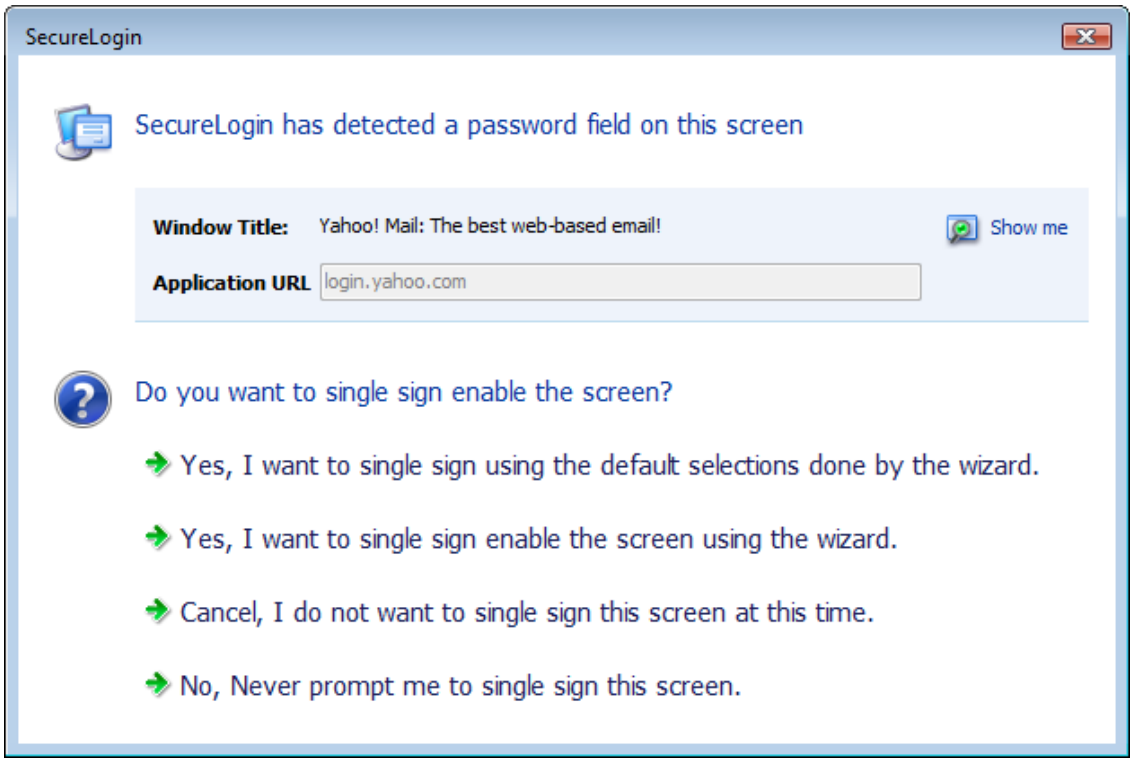
   SecureLogin saves your credentials in the directory. The next time you launch the application, SecureLogin provides the credentials for you.

Example: Using the Default Selections to Enable Yahoo! Mail for Single Sign-On

1 Ensure that you have completed the prerequisites in “Prerequisites” on page 65.

2 Launch Yahoo!* Mail.

SecureLogin detects the application and prompts you to enable it for single sign-on.



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

The Enter your credentials dialog box is displayed.

4 Specify your Yahoo! ID and password.

5 Click **OK**.

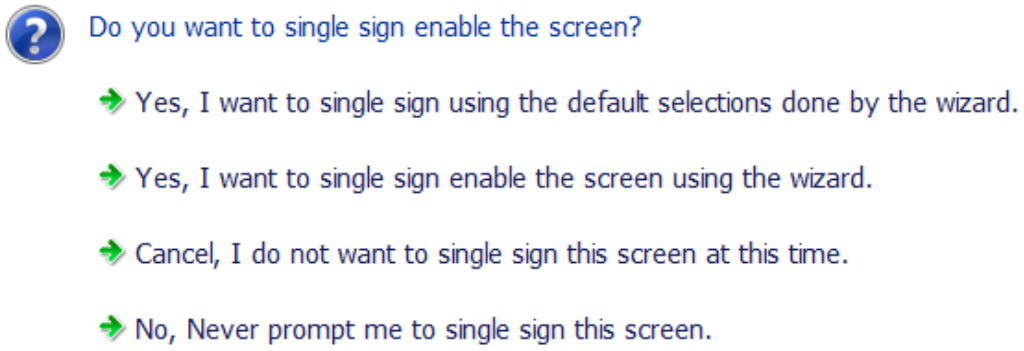
If you have specified the correct credentials, you are logged in to Yahoo! Mail.

For subsequent logins, SecureLogin provides the credentials and logs in.

Manually Defining the Attributes for an Application Definition

1. Ensure that you have completed the prerequisites in “Prerequisites” on page 65.
2. Launch the Web application for which you want to create an application definition.

   SecureLogin detects the application and prompts you to enable the screen for single sign-on.



3. Select **Yes, I want to single sign enable the screen using the wizard**. The Application Definition Wizard page is displayed.
4. Configure the following attributes to create an application definition.

- “Identifying the Screens” on page 67
- “Specifying the Credentials Source” on page 67
- “Identifying the Fields” on page 69
- “Specifying Re-authentication Rules” on page 71
- “Defining the Submit Options” on page 72
- “Defining the Matching Criteria” on page 73

Identifying the Screens

Use the **Identify screen** tab to identify the login screen. If the Application Definition Wizard identifies the login screen correctly, a check mark displays next to **Identify screen**. Click **Show me** to verify if the screen is correctly identified.

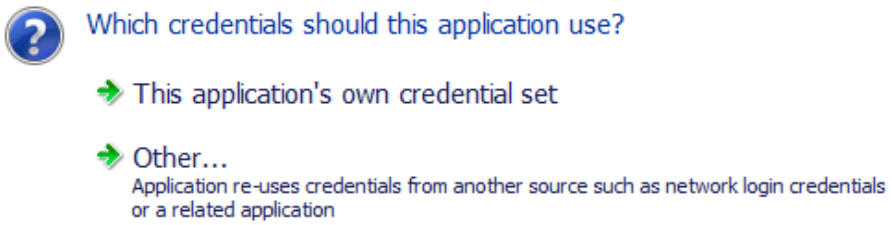
If the screen is not correctly identified, drag the **Choose** icon to the login screen to select it.

Specifying the Credentials Source

Use the **Credential source** tab to define the source of the credentials for the applications.

Some applications use their own credential set to log in. However, some applications might reuse credentials from another source, such as the user's network password or a one-time password.

Figure 3-2 *Specifying the Credential Source*

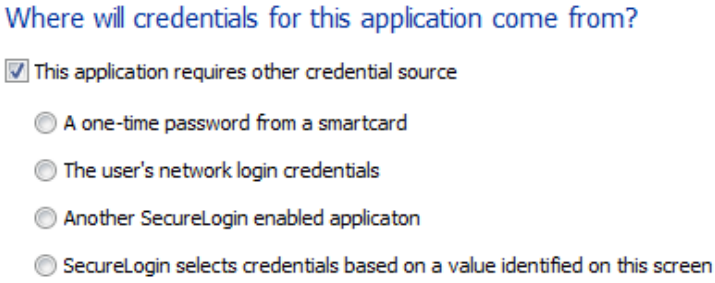


1 Select **This application's own credential set** to use the application's credential set to log in. If you select this option, SecureLogin creates a discrete set of credentials to enable the application. The credential set has the name of the application.

2 Select **Other** to define another source of credentials. If you select this option, select the source of credentials for the application.

   The options for the credential source are:

- “Using a One-Time Password” on page 69
- “Using the User’s Network Login Credentials” on page 69
- “Using Credentials from Another Single Sign-On-Enabled Application” on page 69
- “Selecting Credentials Based on a Value Identified on the Screen” on page 69



Using a One-Time Password

1 Select **A one-time password from a smart card** to use a one-time password from a smart card.

Using the User's Network Login Credentials

1 Select **The user's network logon credentials** to use the user's directory credentials to log in.

Using Credentials from Another Single Sign-On-Enabled Application

1 Select **Another SecureLogin enabled application** to use the credentials of another application enabled for single sign-on. Select the application from a list of available applications enabled for SecureLogin.

Selecting Credentials Based on a Value Identified on the Screen

1 Select **SecureLogin selects credentials based on a value identified on this screen** to provide the credentials based on the presence of a particular value on the login screen. This option uses a text entry. Regular expressions are supported in the text entry.

For example;

```
Connecting to server (.*)
```

where (.*) specifies the value that must be captured to define the credentials.

Identifying the Fields

SecureLogin must identify the fields on the login screen before it can log in to the application. Typically, these are the username and password fields. You can also configure fields such as radio buttons or edit boxes on the login screen. Use the **Identify fields** menu to view the selected field.

Figure 3-3 *Selecting or Reviewing the Login Fields*

- "Not Allowing SecureLogin to Handle the Fields" on page 69
- "Reviewing the Fields" on page 70
- "Reviewing Other Fields" on page 71

Not Allowing SecureLogin to Handle the Fields

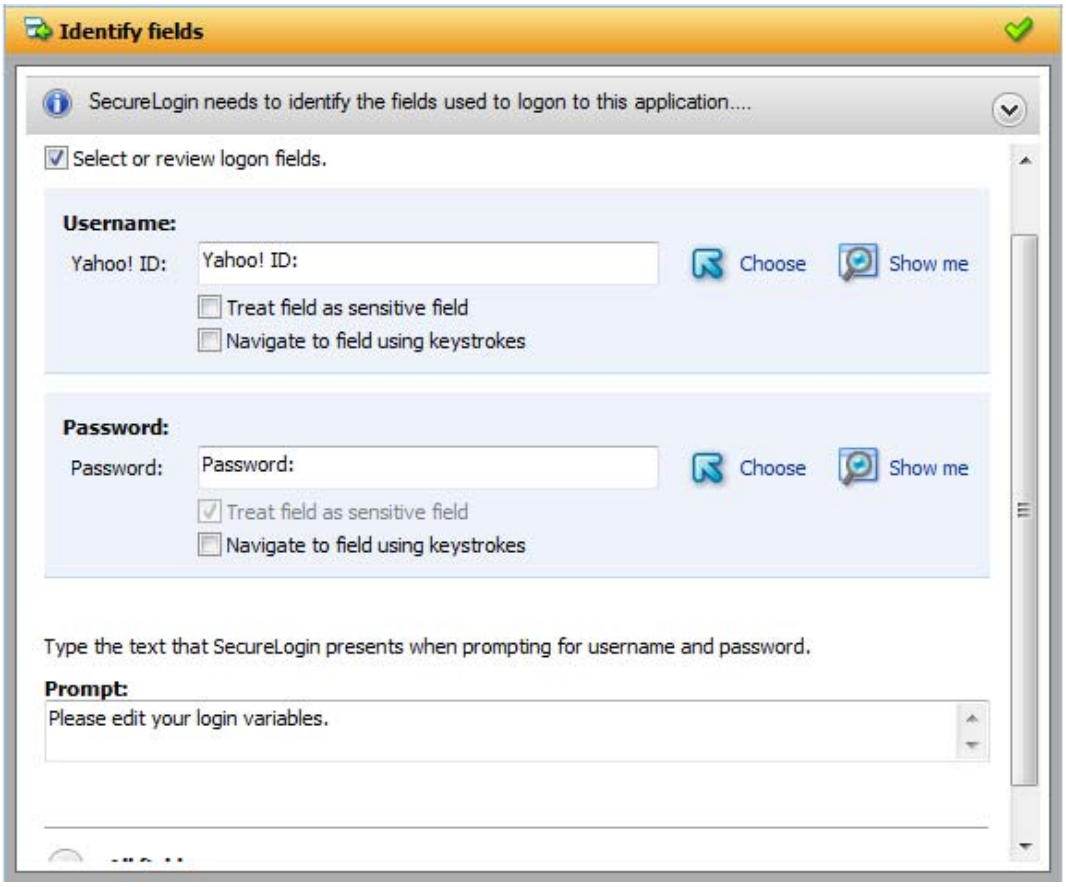
1 Select **No. SecureLogin is not required to handle the fields on this screen** if you do not want SecureLogin to handle the login fields on the screen.

You can use this option to create a credential set, which can be used with other application screens. Similarly, you can use the credential set to link to other application definitions.

Reviewing the Fields

1 Select **Yes. Let me select or review the logon fields** to review the fields selected by the wizard . By default, SecureLogin uses the field names as the prompts in the dialog boxes. You can edit the field names to make them clear and user-friendly.

2 If the login fields are not identified correctly, identify them manually by dragging the **Choose** icon to the fields and clicking the **Show me** icon. The selected fields are highlighted.



3 If **Show me** does not highlight the correct control, update it by dragging and dropping the **Choose** icon to the button you want.

or

Use the **Navigate to field using the keystrokes** option:

3a Click **Start**.

3b Specify the keystrokes.

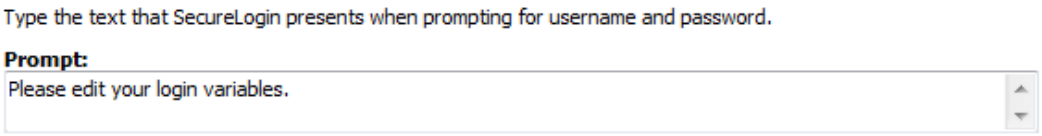
3c Select **Close** to return to the **Identify fields** menu.

3d Select **Stop** to stop the recording.

The next time you log in to the application, the keystrokes are used to log in.

4 Select **Treat text field as a sensitive field** to treat the username field like a password field and disguise the characters with asterisks. This is optional for the username but mandatory for the password.

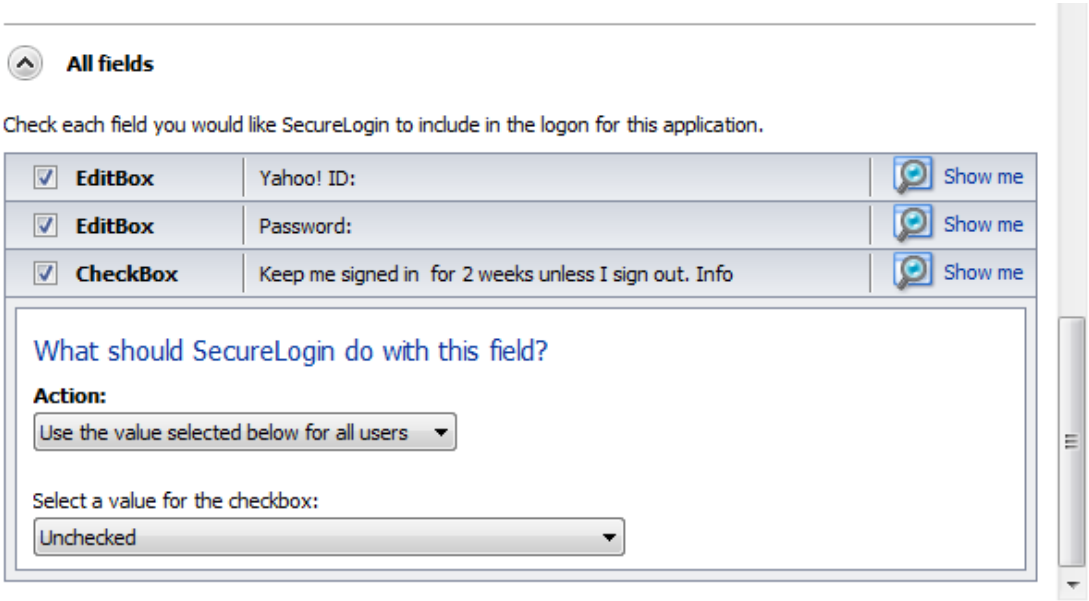
5 (Optional) Specify the text that SecureLogin presents when prompting the user for username and password.



Reviewing Other Fields

1 Click **All fields** to show other fields detected by the wizard on the login screen. Each control is listed by type and name (if known).

Select the field you want SecureLogin to use in managing the login for the application, then specify the actions for SecureLogin.



Depending on the application, any or all of the following fields are displayed.

- Edit box
- Check Box
- Combo Box
- Radio Button

For information on configuring SecureLogin to use these additional fields, refer "All Fields" on page 17.

Specifying Re-authentication Rules

1 Use the **Re-authentication** menu to specify if users must reauthenticate with their network credentials or an authentication device.

2 If you select **No. The user is not required to re-authenticate**, SecureLogin does not prompt users to reauthenticate before providing credentials to the application.

3 If you select **Yes. Enforce re-authentication before accessing this application**, users must specify credentials in order to reauthenticate.

4 From the **Select from the methods detected** drop-down list, select the method SecureLogin must use. You can select from:

- **Use same Credentials as Network Login:** Use the network login credentials.
- **Default:** The method the user used to log in to the application.
- **Password:** The network password.
- **Smart Card:** After the PIN is verified, SecureLogin checks to see if the smart card belongs to the user or not.

5 You must also specify the action SecureLogin takes when the users cancels the reauthentication.

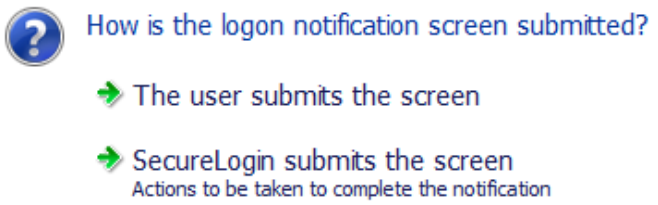
You can define one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user cancels the reauthentication dialog box. Select the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes SecureLogin enters when a user clicks **Cancel** in the reauthentication dialog box. To record keystrokes:
  1. Click **Start**.
  2. Specify the **keystrokes**.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct the user to this website:** Specify a URL to go to when a user cancels the prompt for credentials. You can redirect users to the login screen and force them to specify the login credentials again.

Defining the Submit Options

1 Use the **Submit options** menu to define how SecureLogin submits the login screen.

2 If you select **The user submits the screen**, SecureLogin does nothing and the user must manually submit the login screen.



3 If you select **SecureLogin submits the screen**, specify the action SecureLogin takes to submit the login screen.

You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen. Select the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes SecureLogin enters to submit the login notification screen. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.

- **Re-direct the user to this website:** Specify a URL to go to when a user submits the login notification screen.

4 You can also specify the action SecureLogin uses when users cancel a prompt to save their credentials. For this, select **Enable action when user cancels to change their password**.

You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen.Select the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes SecureLogin enters to submit the login screen. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct users to this website:** Specify a URL to go to when users cancel the change password prompt.

Defining the Matching Criteria

SecureLogin must uniquely identify each application screen in order to run an application definition. If SecureLogin cannot uniquely identify a particular application screen, you can manually define the matching criteria.

1 Use the **Matching criteria** menu to define the matching criteria.

2 If you select **No. Use minimal rules based on your previous selections**, SecureLogin uses the rules defined in previous attribute panels to identify and handle the application window.

3 If you select **Yes. Use additional Wizard generated rules**, you can add, modify, or remove rules. Your matching criteria must include at least one rule. After you select this option, the following screen appears:

4 By default, **Use Wizard generated rules** is selected. The **Rules** text box lists the controls that are detected by SecureLogin. You can add a new rule by dragging the **Choose** icon to a specific control on the application window and then clicking Show me to confirm that SecureLogin has identified the correct control.

To modify a rule for a control:

4a Select the rule you want to edit, then click **Configure more detailed match for this control**

4b Define what SecureLogin must match. You can set the following matching rule:

- **SecureLogin is to match value displayed:** If you select this option, SecureLogin only matches those screens that exactly match the displayed text and rules identified.

To verify if your regular expression is correct:

1 Click **Test Match**.

If a regular expression does not match any control on the application screen, SecureLogin prompts you to verify your regular expression and select the correct control.

To delete a rule:

1 To delete a rule, select the rule, then click **Remove**.

You have successfully completed creating an application definition for a Web application. The next time you launch the application, SecureLogin provides the credentials for you.

Creating an Application Definition for a Windows Application

A Windows application is any application that is launched with an executable (`.exe`) file.

You can create an application definition for a Windows application by accepting the default selections in the wizard, or you can manually select the attributes you want.

- "Prerequisites" on page 74
- "Using the Default Selections to Create an Application Definition" on page 74
- "Manually Defining the Attributes for an Application Definition" on page 75

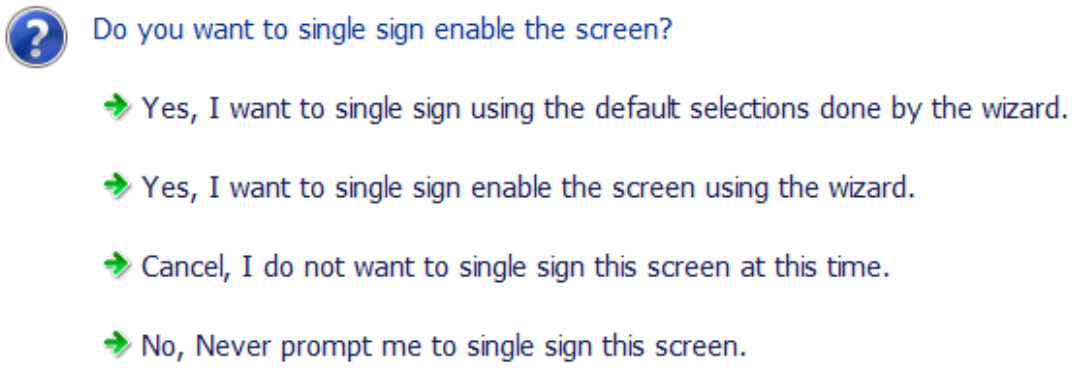
Prerequisites

- Close all open SecureLogin prompts.
- Verify if you have permissions to create application definition. See Chapter 5, "Setting the Wizard Mode Preference," on page 119.
- Ensure that **Add application prompts for Windows applications** option is selected.
- Ensure that SecureLogin is running on your workstation.

Using the Default Selections to Create an Application Definition

1. Ensure that you have completed the prerequisites in "Prerequisites" on page 74.
2. Start a Windows application for which you want to create an application definition.

   SecureLogin detects a login screen and displays the following prompt:



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

   SecureLogin identifies the application and displays the name of the application in the prompt.
4. You are prompted to specify the credentials for the application. Specify the username, password, and any other information required.
5. Click **OK**.

   SecureLogin saves your credentials and uses them to log in to the application.

   The next time you launch the application, SecureLogin provides the username and password for you.

Example: Using the Default Selections to Create an Application Definition for Google Talk

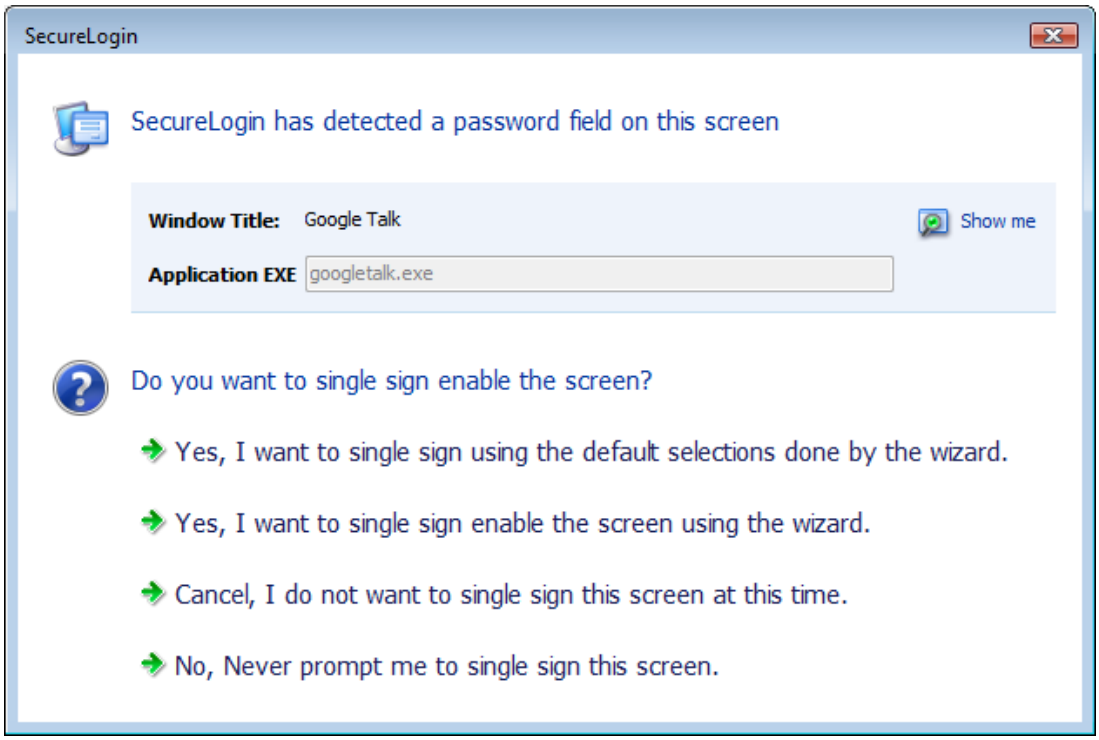
The following example demonstrates creating an application definition for Google* Talk*.

This procedure assumes that you already have a Google account.

1 Ensure that you have completed the prerequisites in “Prerequisites” on page 74.

2 Launch Google Talk.

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



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

The Enter your Credentials dialog box is displayed.

4 Specify your username and password, then click **OK**.

SecureLogin saves the credentials and uses them to log in to you Google Talk.

5 Test the application definition by logging out and logging in again.

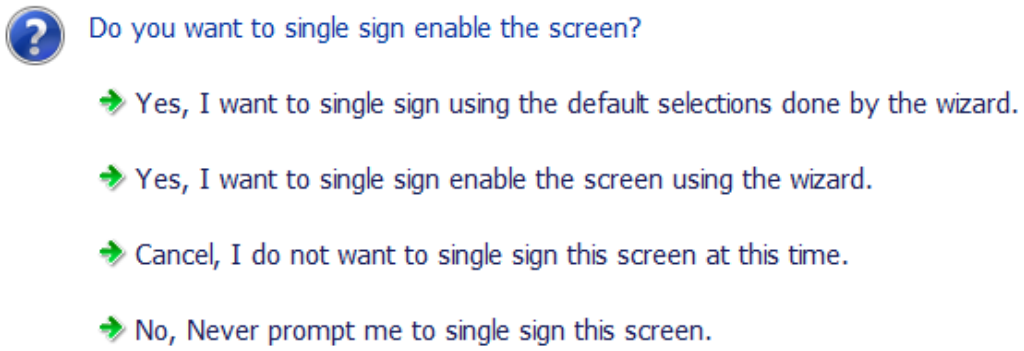
If the application is defined correctly with the correct credentials, you are logged in successfully. If your login is not successful, delete the application definition and repeat the above steps. You might also need to review the application definition for event responses and errors.

Manually Defining the Attributes for an Application Definition

1 Ensure that you have completed the prerequisites in “Prerequisites” on page 74.

2 Launch the Windows application for which you want to create an application definition.

SecureLogin detects the application and prompts you to enable the screen for single sign-on.



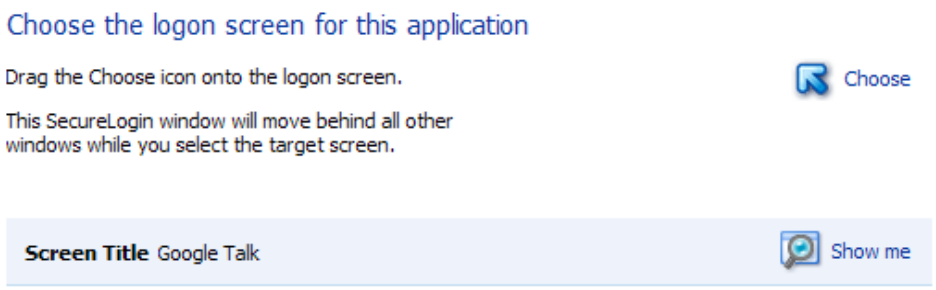
3 Select **Yes, I want to single sign enable the screen using the wizard**. The Application Definition Wizard page is displayed.

4 Configure the following attributes to create an application definition.

- "Identifying the Screens" on page 76
- "Specifying the Credential Source" on page 76
- "Identifying the Fields" on page 78
- "Specifying Re-authentication Rules" on page 80
- "Defining the Submit Options" on page 80
- "Defining the Matching Criteria" on page 81

Identifying the Screens

1 Use the **Identify screen** tab to identify the login screen. If the Application Definition Wizard identifies the login screen correctly, a check mark displays next to **Identify screen**. Click **Show me** to verify if the screen is correctly identified.



2 If the screen is not correctly identified, drag the **Choose** icon to the login screen to select it.

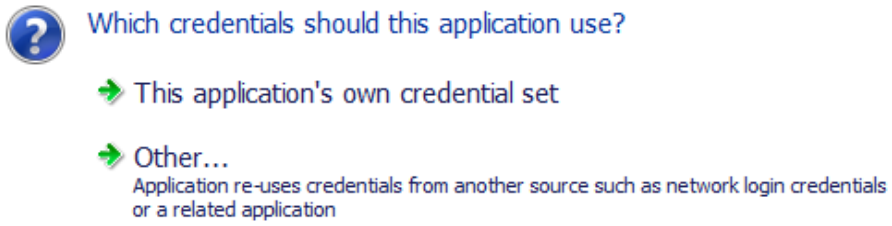
Specifying the Credential Source

- "Using a One-Time Password" on page 78
- "Using User's Network Login Credentials" on page 78

- “Using Credentials from Another Single Sign-One Enabled Application” on page 78
- “Selecting Credentials Based on a Value Identified on the Screen” on page 78

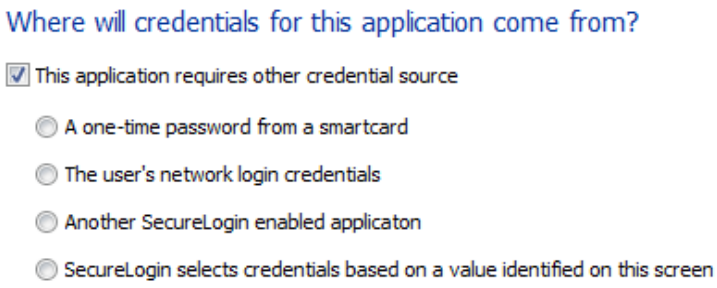
1 Use the **Credential source** tab to define the source of the credentials for the applications.

Some applications use their own credential set to log in. However, some applications might reuse credentials from another source, such as the user's network password or a one-time password.



2 Select **This application's own credential set** to use the application's credential set to log in. If you select this option, SecureLogin creates a discrete set of credentials to enable the application. The credential set has the name of the application.

3 Select **Other** to define another source of credentials. If you select this option, select the source of credentials for the application.



The options for the credential source are:

- “Using a One-Time Password” on page 78
- “Using User’s Network Login Credentials” on page 78
- “Using Credentials from Another Single Sign-One Enabled Application” on page 78
- “Selecting Credentials Based on a Value Identified on the Screen” on page 78

Using a One-Time Password

1 Select **A one-time password from a smart card** to use a one-time password from a smart card.

Using User's Network Login Credentials

1 Select **The user's network logon credentials** to use the user's directory credentials to log in.

Using Credentials from Another Single Sign-One Enabled Application

1 Select **Another SecureLogin enabled application** to use the credentials of another application enabled for single sign-on.

Select the application from a list of available applications enabled for SecureLogin.

Selecting Credentials Based on a Value Identified on the Screen

1 Select **SecureLogin selects credentials based on a value identified on this screen** to provide the credentials based on the presence of a particular value on the login screen.

This option uses a text entry. Regular expressions are supported in the text entry.

For example:

```
Connecting to server (.*)
```

where (.*) specifies the value that must be captured to define the credentials.

Identifying the Fields

SecureLogin must identify the fields on the login screen before it can log in to the application. Typically, these are the username and password fields. You can also configure fields such as radio buttons or edit boxes on the login screen. Use the **Identify fields** menu to view the selected fields.

Figure 3-4 *Selecting or Reviewing the Login Fields*

- "Not Allowing SecureLogin to Handle the Fields" on page 78
- "Reviewing the Fields" on page 79
- "Reviewing Other Fields" on page 79

Not Allowing SecureLogin to Handle the Fields

1 Select **No. SecureLogin is not required to handle the fields on this screen** if you do not want SecureLogin to handle the login fields on the screen.

Use this option to create a credential set, which can be used with other application screens.

Similarly, you can use the credential set to link to other application definitions.

Reviewing the Fields

1 Select **Yes. Let me select or review the logon fields** to review the fields selected by the wizard .

By default, SecureLogin uses the field names as the prompts in the dialog boxes. You can edit the field names to make them clear and user-friendly.

2 If the login fields are not identified correctly, identify them manually by dragging the **Choose** icon to the button you want to the fields and clicking the **Show me** icon.

The selected fields are highlighted.

3 If **Show me** does not highlight the correct control, update it by dragging and dropping the **Choose** icon to the button you want.

or

Use the **Navigate to field using the keystrokes** option.

3a Click **Start**.

3b Specify the keystrokes.

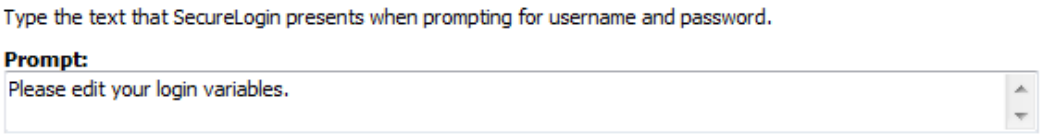
3c Select **Close** to return to the **Identify fields** menu.

3d Select **Stop** to stop the recording.

The next time you log in to the application, the keystrokes are used to log in.

4 Select **Treat text field as a sensitive field** to treat the username field like a password field and disguise the characters with asterisks. This is optional for the username but mandatory for the password.

5 (Optional) Specify the text that SecureLogin presents when prompting the user for username and password.



Reviewing Other Fields

1 Click **All fields** to show other fields detected by the wizard on the login screen. Each control is listed by type and name (if known).

Select the field you want SecureLogin to use in managing the login for the application, then specify the actions for SecureLogin.

Depending on the application, any or all of the following fields are displayed.

- Edit box
- Check Box
- Combo Box
- Radio Button

For information about configuring SecureLogin to use these additional fields, see “All Fields” on page 17.

Specifying Re-authentication Rules

1. Use the **Re-authentication** menu to specify if users must reauthenticate with their network credentials or an authentication device.
2. If you select **No. The user is not required to re-authenticate**, SecureLogin does not prompt users to reauthenticate users before providing the credentials to the application.
3. If you select **Yes. Enforce re-authentication before accessing this application**, users must specify the credentials in order to reauthenticate.
4. From the **Select from the methods detected** drop-down list, select the method SecureLogin must use.

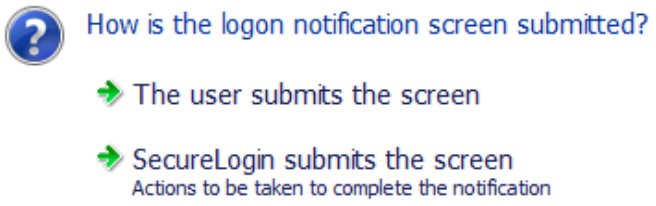
   You can select from:

   - **Use same credentials as network login:** Use the network login credentials.
   - **Password:** The network password.
   - **Smart card:** After the PIN is verified, SecureLogin checks to see if the smart card belongs to the user or not.
5. You must also specify the action SecureLogin takes when the users cancels the reauthentication. You can define one of the following actions:

   - **Click this button:** Select a button on the application that SecureLogin clicks when a user cancels the reauthentication dialog box. Select the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
   - **Type the Following Keystorkes:** Define the commands or keystrokes SecureLogin enters when a user clicks **Cancel** in the reauthentication dialog box. To record keystrokes:
     1. Click **Start**.
     2. Specify the **keystrokes**.
     3. After you have recorded the keystrokes, click **Close**.
   - **Re-direct the user to this website:** Specify a URL to go to when a user cancels the promptfor credentials. You can redirect users to the login screen and force them to specify the login credentials again.

Defining the Submit Options

1. Use the **Submit options** menu to define how SecureLogin submits the login screen.
2. If you select **The user submits the screen**, SecureLogin does nothing and the user must manually submit the login screen.



3. If you select **SecureLogin submits the screen**, specify the action SecureLogin takes to submit the login screen.

You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen. Highlight Select the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes SecureLogin enters to submit the login notification screen. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct the user to this website:** Specify a URL to go to when a user submits the login notification screen.

4 You can also specify the action SecureLogin uses when users cancel a prompt to save their credentials. For this, select **Enable action when user cancels to change their password**.

You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen.Select the button by dragging the **Choose** icon to the button you want and clicking **Show me**.
- **Type the following keystrokes:** Define the commands or keystrokes SecureLogin enters to submit the login screen. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct users to this website:** Specify a URL to go to when users cancel the change password prompt.

Defining the Matching Criteria

SecureLogin must uniquely identify each application screen in order to run an application definition. If SecureLogin cannot uniquely identify a particular application screen, you can manually define the matching criteria.

Use the **Matching criteria** menu to define the matching criteria.

1 If you select **No. Use minimal rules based on your previous selections**, SecureLogin uses the rules defined in previous attribute panels to identify and handle the password change.

2 If you select Yes. Use additional Wizard generated rules, you can add, modify, or remove rules. Your matching criteria must include at least one rule.

After you select this option, the following screen appears:

3 By default, **Use Wizard generated rules** is selected.

The **Rules** text box lists the controls that are detected by SecureLogin.

Add new rule by dragging the **Choose** icon to a specific control.

Click **Show me** to confirm that SecureLogin has identified the correct control.

To modify a rule for a control:

1. Select the rule you want to edit, then click **Configure more detailed match for this control**
2. Define what SecureLogin must match. You can set the following matching rule:
   - **SecureLogin is to match value displayed:** If you select this option, SecureLogin only matches those screens that exactly match the displayed text and rules identified.

To verify the regular expression:

1. Click **Test Match** to verify if your regular expression is correct.

   If a regular expression does not match any control on the application screen, SecureLogin prompts you to verify your regular expression and select the correct control.

To delete a rules:

1. Select the rule, then click **Remove**

You have successfully completed creating an application definition for a Windows application. The next time you launch the application, SecureLogin provides the credentials for you.

Creating an Application Definition for a Java Application or an Oracle Form

SecureLogin supports single sign-on feature for Oracle forms which uses Java 1.7 or later.

A Java application is a Java program that runs independently. The Java Virtual Machine in the client or server interprets the instructions.

For Oracle form applications SecureLogin uses the pre-installed JRE 1.7 or later in the machine. If any of these Java components is added after installing (or upgrading to) SecureLogin, you need to enable SecureLogin to use the newly added Java component. To enable support to the new Java component, run the repair option of the SecureLogin installer.

You can create an application definition for a Java application or an Oracle application by accepting the default selections in the wizard, or you can manually select the attributes you want.

NOTE: Loading of Oracle components requires some time before an application definition for Oracle form is started. Therefore, the Wizard consumes some time when starting the application definition for Oracle form.

- "Prerequisites" on page 82
- "Using the Default Selections to Create an Application Definition" on page 83
- "Manually Defining the Attributes for an Application Definition" on page 84

Prerequisites

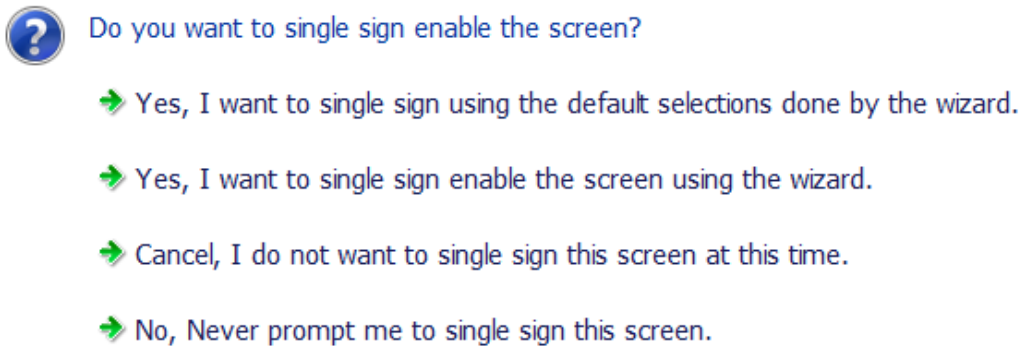
- In the Java preferences, set the A**dd application prompts for Java applications** preference to **Yes**.
- In the Java preferences, set the **Allow single sign-on to Java applications** preference to **Yes**.
- Ensure that you have JRE 1.7 or later to support single sign-on to Oracle Forms.
- Close all open SecureLogin prompts.

- Verify if you have permissions to create application definition. See Chapter 5, “Setting the Wizard Mode Preference,” on page 119.
- Ensure that SecureLogin is running on your workstation.

Using the Default Selections to Create an Application Definition

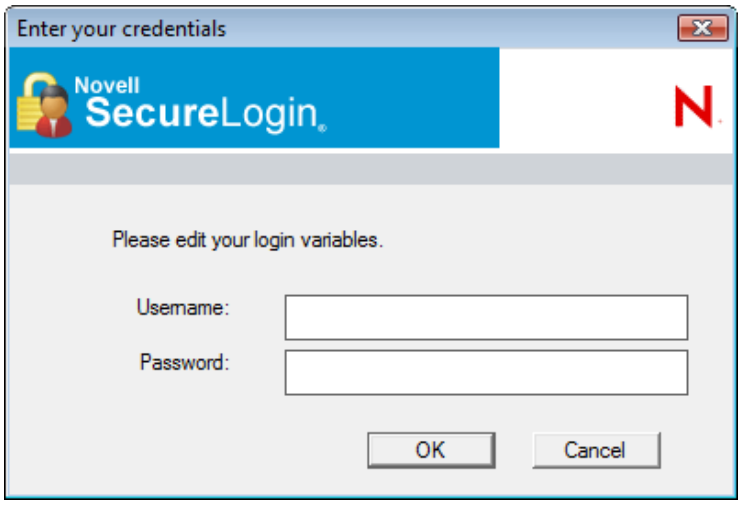
1. Ensure that you have completed the prerequisites in “Prerequisites” on page 82.
2. Launch the Java application for which you want to create an application definition.

   SecureLogin detects the application and prompts you to enable single sign-on.



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

   The Enter your Credentials dialog box is displayed.



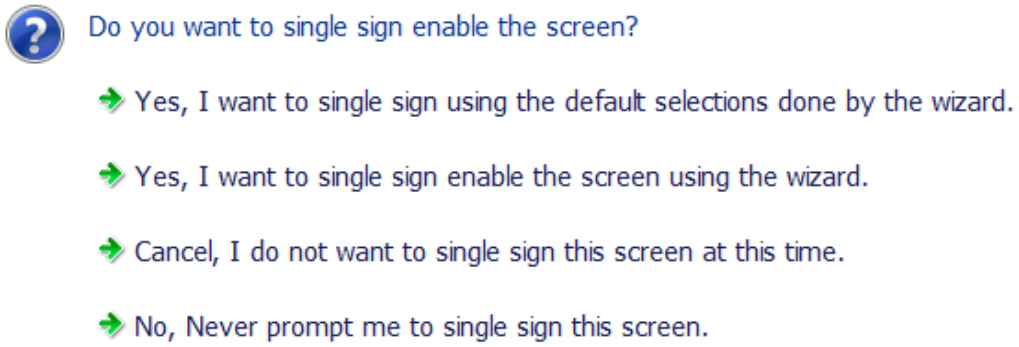
4. Specify your credentials, then click **OK**.

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

Manually Defining the Attributes for an Application Definition

1. Ensure that you have completed the prerequisites in “Prerequisites” on page 82.
2. Launch the Java application for which you want to create an application definition.

   SecureLogin detects the application and prompts you to enable the screen for single sign-on.



3. Select **Yes, I want to single sign enable the screen using the wizard**. The Application Definition Wizard page is displayed.
4. Configure the following attributes to create application definition.

- “Identifying the Screens” on page 84
- “Specifying the Credential Source” on page 84
- “Identifying the Fields” on page 86
- “Specifying Reauthentication Rules” on page 87
- “Defining the Submit Options” on page 88
- “Defining the Matching Criteria” on page 89

Identifying the Screens

1. Use the **Identify screen** tab to identify the login screen. If the Application Definition Wizard identifies the login screen correctly, a check mark displays next to **Identify screen**.

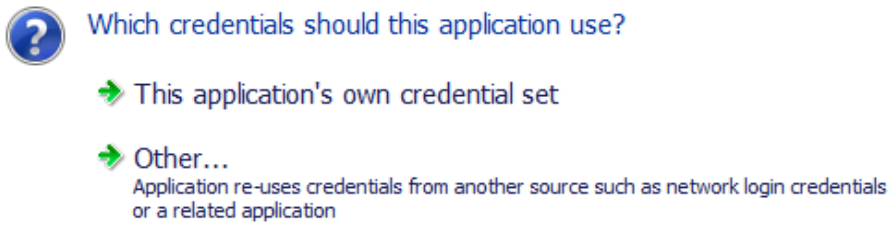
   NOTE: The **Show me** icon fails to highlight the fields identified by the wizard for all embedded Java applets from JRE 6u7 and later. It fails to highlight the corresponding target for all the attributes of the Application Definition Wizard, such as **Identify fields**, **Re-authentication**, **Submit options**, and **Matching criteria**.

2. Drag the **Choose** icon to the detect and select login screen.

Specifying the Credential Source

1. Use the **Credential source** tab to define the source of the credentials for the applications.

   Some applications use their own credential set to log in. However, some applications might reuse credentials from another source, such as the user's network password or a one-time password.

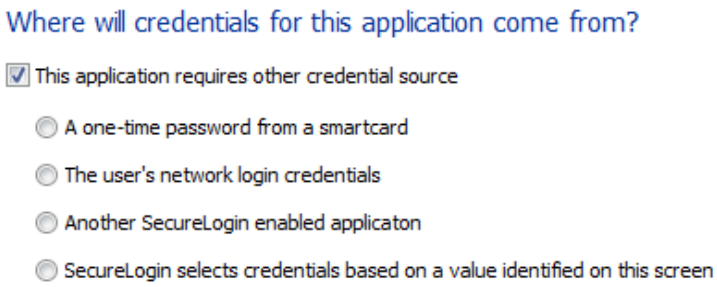


2 Select **This application's own credential set** to use the application's credential set to log in.

If you select this option, SecureLogin creates a discrete set of credentials to enable the application. The credential set has the name of the application.

3 Select **Other** to define another source of credentials.

If you select this option, select the source of credentials for the application.



The options for the credential source are:

- “Using a One-Time Password” on page 85
- “Using a User’s Network Login Credentials” on page 85
- “Using Credentials from Another Single Sign-One Enabled Application” on page 85
- “Selecting Credentials Based on a Value Identified on the Screen” on page 85

Using a One-Time Password

1 Select **A one-time password from a smart card** to use a one-time password from a smart card.

Using a User’s Network Login Credentials

1 Select **The user's network logon credentials** to use the user's directory credentials to log in.

Using Credentials from Another Single Sign-One Enabled Application

1 Select **Another SecureLogin enabled application** to use the credentials of another application enabled for single sign-on.

Select the application from a list of available applications enabled for SecureLogin.

Selecting Credentials Based on a Value Identified on the Screen

1 Select **SecureLogin selects credentials based on a value identified on this screen** to provide the credentials based on the presence of a particular value on the login screen.

This option uses a text entry. Regular expressions are supported in the text entry.

For example:

```
Connecting to server (.*)
```

where (.*) specifies the value that must be captured to define the credentials.

Identifying the Fields

SecureLogin must identify the fields on the login screen before it can log in to the application. Typically, these are the username and password fields. You can also configure fields such as radio buttons or edit boxes on the login screen.

Use the **Identify fields** menu to view the selected fields.

Figure 3-5 *Selecting or Reviewing the Login Fields*

- "Not Allowing SecureLogin to Handle the Fields" on page 86
- "Reviewing the Fields" on page 86
- "Reviewing Other Fields" on page 87

Not Allowing SecureLogin to Handle the Fields

1 Select **No. SecureLogin is not required to handle the fields on this screen** if you do not want SecureLogin to handle the login fields on the screen.

You can use this option to create a credential set, which can be used with other application screens.

Similarly, you can use the credential set to link to other application definitions and to identify the application screens.

Reviewing the Fields

1 Select **Yes. Let me select or review the logon fields** to review the fields selected by the wizard.

By default, SecureLogin uses the field names as the prompts in the dialog boxes. You can edit the field names to make it clear and user-friendly.

2 Select **Treat text field as a sensitive field** to treat the username field like a password field and disguise the characters entered with asterixes.

This is optional for the username but mandatory for the password.

NOTE: If the label text for a control is empty or incorrect, do the following:

- Click **Show me** to verify if the correct control is selected.
- If **Show me** does not highlight the correct control, update it by dragging and dropping the **Choose** icon or use the **Navigate to field using the keystrokes** option.

---

3 Select **Navigate to field using keystrokes** if you are having difficulty identifying the correct fields using other methods. SecureLogin prompts you to use **Navigate to field using keystrokes** if it cannot identify the fields on the login screen.

To record keystrokes:

3a Click **Start**.

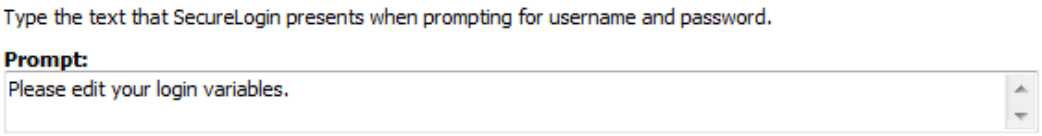
3b Specify the keystrokes.

3c Select **Close** to return to the **Identify fields** menu.

3d Select **Stop** to stop the recording.

Next time you login to the application, keystrokes are used to log in.

4 You can also specify the text that SecureLogin presents when prompting the user for the username and password.



Reviewing Other Fields

1 Click **All fields** to show other fields detected by the wizard on the login screen.

Each control is listed by type and name (if known).

Select the field you want SecureLogin to use in managing the login for the application, then specify the actions for SecureLogin.

Depending on the application, any or all of the following fields are displayed.

- Edit box
- Check Box
- Combo Box
- Radio Button

For information on configuring SecureLogin to use these additional fields, refer "All Fields" on page 17.

Specifying Reauthentication Rules

1 Use the **Re-authentication** menu to specify how users must reauthenticate. Specify if they must reauthenticate with their network credentials or an authentication device.

2 If you select **No. The user is not required to re-authenticate**, SecureLogin does not prompt users to reauthenticate before providing the credentials to the application.

3 If you select **Yes. Enforce re-authentication before accessing this application**, users must specify the credentials that SecureLogin uses to reauthenticate the user's identity.

4 From the **Select from the methods detected** drop-down list, select the method SecureLogin must use. You can select from:

- **Use same credentials as network login:** Use the network login credentials.
- **Password:** The network password.
- **Smart card:** After the PIN is verified, SecureLogin checks to see if the smart card belongs to the user or not.

5 You must also specify the action SecureLogin takes when the users cancels the reauthentication.

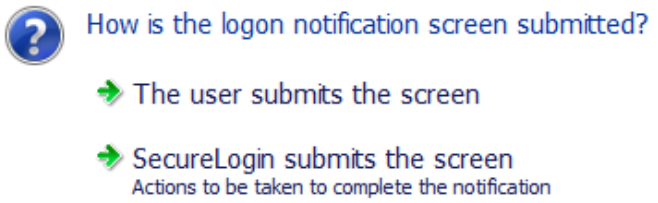
You can define one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user cancels the reauthentication dialog box.
- **Type the following keystrokes:** Define the commands or keystrokes SecureLogin enters when a user clicks **Cancel** in the reauthentication dialog box. To record keystrokes:
  1. Click **Start**.
  2. Specify the **keystrokes**.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct the user to this website:** Specify a URL to go to when a user cancels the prompt for credentials. You can redirect users to the login screen and force them to specify the login credentials again again.

Defining the Submit Options

1 Use the **Submit options** menu how SecureLogin submits the login screen.

2 If you select **The user submits the screen**, SecureLogin does nothing and the user must manually submit the login screen.



If you select **SecureLogin submits the screen**, specify the action SecureLogin takes to submit the login screen.

You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen.
- **Type the following keystrokes:** Define the commands or keystrokes SecureLogin enters to submit the login notification screen. To record keystrokes:
  1. Click **Start**.
  2. Specify the keystrokes.
  3. After you have recorded the keystrokes, click **Close**.
- **Re-direct the user to this website:** Specify a URL to go to when a user submits the login notification screen.

3 You can also specify the action SecureLogin uses when users cancel a prompt to save their credentials.. For this, select **Enable action when user cancels to change their password**. You can specify one of the following actions:

- **Click this button:** Select a button on the application that SecureLogin clicks when a user submits the screen.
- **Type the following keystrokes:** Define the commands or keystrokes SecureLogin enters to submit the login screen. To record keystrokes:
  1. Click **Start**.

2. Specify the keystrokes.
3. After you have recorded the keystrokes, click **Close**.

- **Re-direct users to this website:** Specify a URL to go to when users cancel the change password prompt.

Defining the Matching Criteria

SecureLogin must uniquely identify each application screen in order to run an application definition. If SecureLogin cannot uniquely identify a particular application screen, you can manually define the matching criteria. Use the **Matching criteria** menu to define the matching criteria.

1 If you select **No. Use minimal rules based on your previous selections**, SecureLogin uses the rules defined in previous attribute panels to identify and handle the password change.

2 If you select **Yes. Use additional Wizard generated rules**, you can add, modify, or remove rules. Your matching criteria must include at least one rule. :

3 By default, **Use Wizard generated rules** is selected. The **Rules** text box lists the controls that are detected by SecureLogin.

To modify a rule for a control:

1 Select the rule you want to edit, then click **Configure more detailed match for this control**

2 Define what SecureLogin must match. You can set the following matching rule:

- **SecureLogin is to match value displayed:** If you select this option, SecureLogin only matches those screens that exactly match the displayed text and rules identified.

To verify regular expression:

1 Click **Test Match** to verify if your regular expression is correct.

If a regular expression does not match any control on the application screen, SecureLogin prompts you to verify your regular expression and select the correct control.

To delete a rule:

1 To delete a rule, select the rule, then click **Remove**.

You have successfully completed creating an application definition for a Web application. The next time you launch the application, SecureLogin provides the credentials for you.

Using a Predefined Application Definition

SecureLogin provides a set of predefined application definitions. Use the predefined application definitions to enable applications for single sign-on.

NOTE: SecureLogin does not provide predefined application definitions for Java applications.

- “Using a Predefined Application Definition to Enable a Web Application for Single Sign-On” on page 90
- “Using a Predefined Application Definition to Enable Windows Application for Single Sign-On” on page 92

Using a Predefined Application Definition to Enable a Web Application for Single Sign-On

1. Launch a Web application.

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

   The SecureLogin dialog box is displayed.

2. Select **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**.

   SecureLogin saves your credentials and uses them to log in to the application.

   The next time you launch the application, SecureLogin provides the username and password for you. .

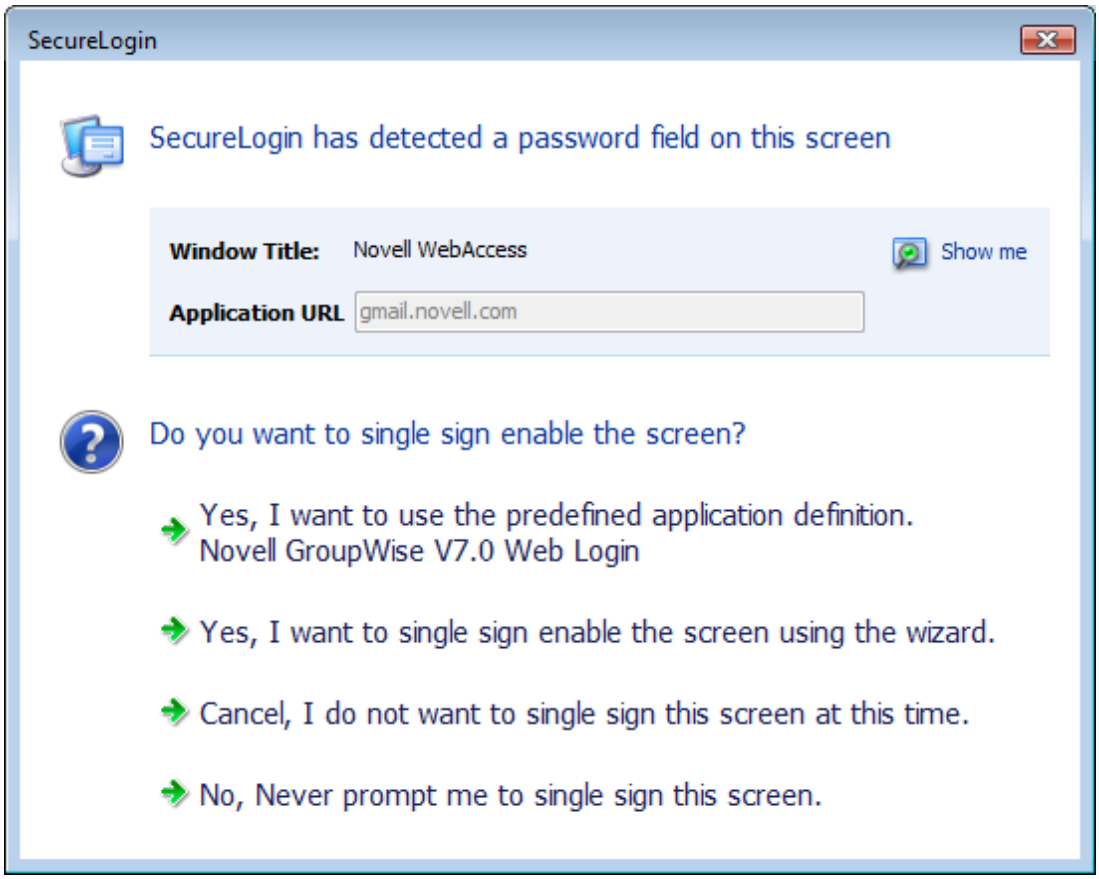
Example: Using a Predefined Application Definition to Enable Single Sign-On for Novell WebAccess

The following example demonstrates enabling single sign-on for a Novell WebAccess. SecureLogin provides a predefined application for Novell WebAccess.

This procedure assumes that you already have a GroupWise® account.

1. Launch Novell WebAccess.

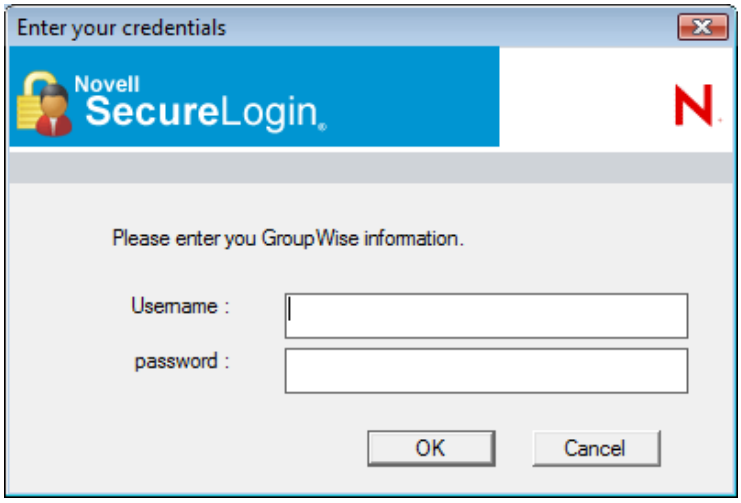
   A predefined application definition exists for Novell WebAccess. SecureLogin detects the application and the SecureLogin dialog box is displayed.



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

The Enter your GroupWise information dialog box is displayed.

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



SecureLogin saves the credentials and uses them to log in to your GroupWise WebAccess account.

4 Test the application definition by logging out and logging in again.

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 event responses and errors

Using a Predefined Application Definition to Enable Windows Application for Single Sign-On

1 Launch a Windows application.

If a predefined application definition exists for that application, SecureLogin

automatically detects the application definition.

The SecureLogin dialog box is displayed.

2 Select **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**.

SecureLogin saves your credentials and uses them to log in to the application.

The next time you launch the application, SecureLogin provides the username and password for you. .

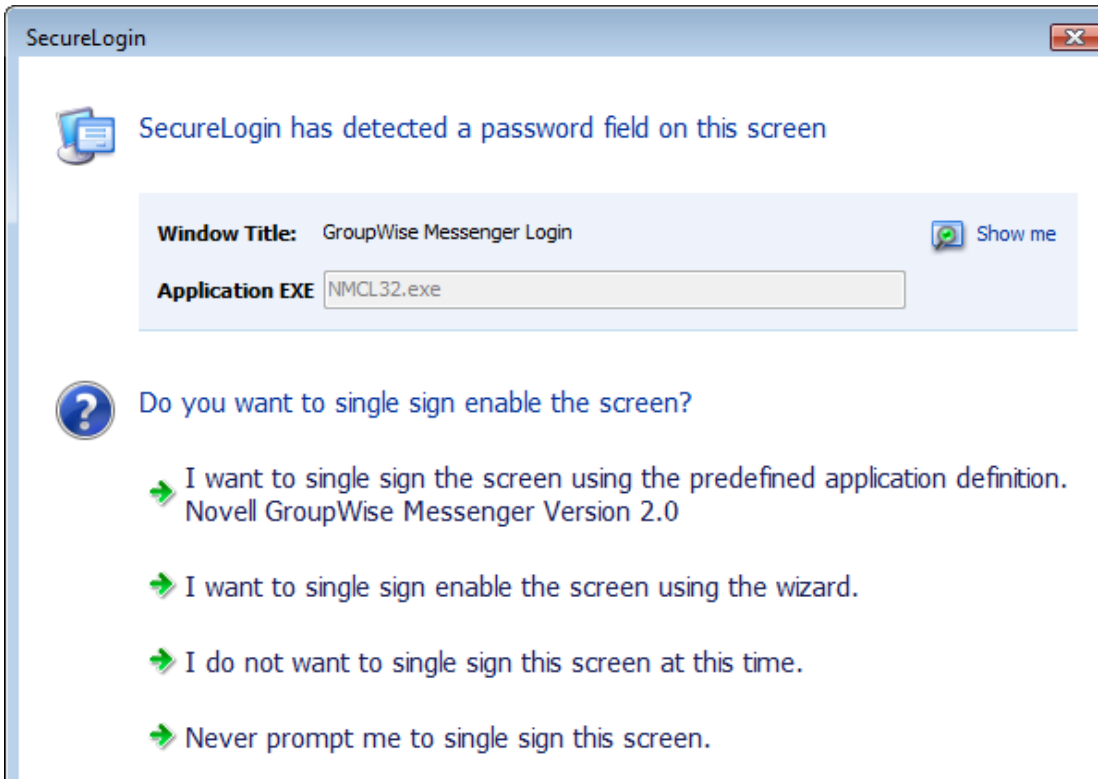
Example: Using a Predefined Application to Enable Single Sign-On for Novell GroupWise Messenger

The following example demonstrates enabling single sign-on for Novell GroupWise Messenger.

This procedure assumes that you already have a GroupWise Messenger account.

1 Launch GroupWise Messenger.

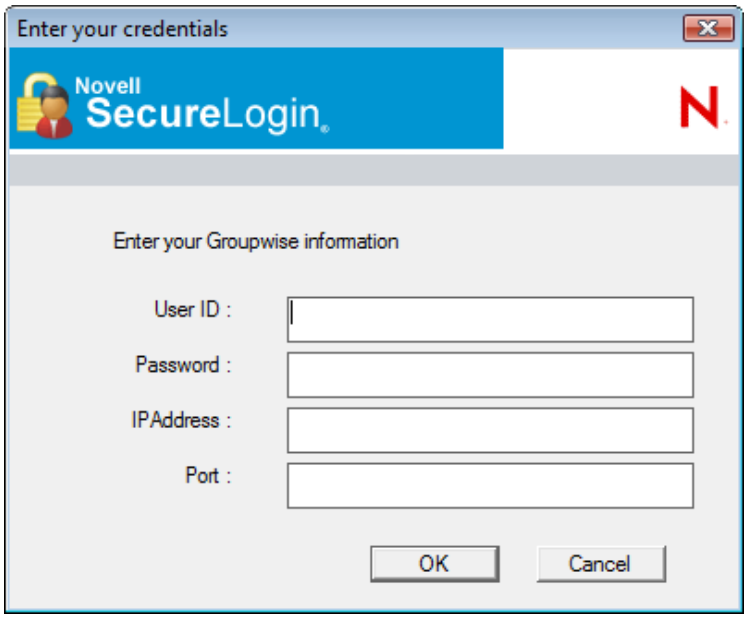
A predefined application definition exists for GroupWise Messenger. SecureLogin detects the application and the SecureLogin dialog box is displayed.



2 Select **I want to single sign the screen using the predefined application definition. Novell GroupWise Messenger Version 2.0**.

The Enter your GroupWise information dialog box is displayed.

3 Specify your User ID, Password, IP Address, and Port details, then click **OK**.



SecureLogin saves the credentials and uses them to log in to your GroupWise Messenger account.

4 Test the application definition by logging out and logging in again.

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 event responses and errors.

Testing Application Definitions

You can test only the application definitions that were created by using the wizard. Application definitions created manually or with earlier versions of SecureLogin cannot be tested in the current version.

IMPORTANT: Before you begin to test the application definition, close the application and relaunch it.

You can test an application definition after you have completed filling in the relevant attributes.

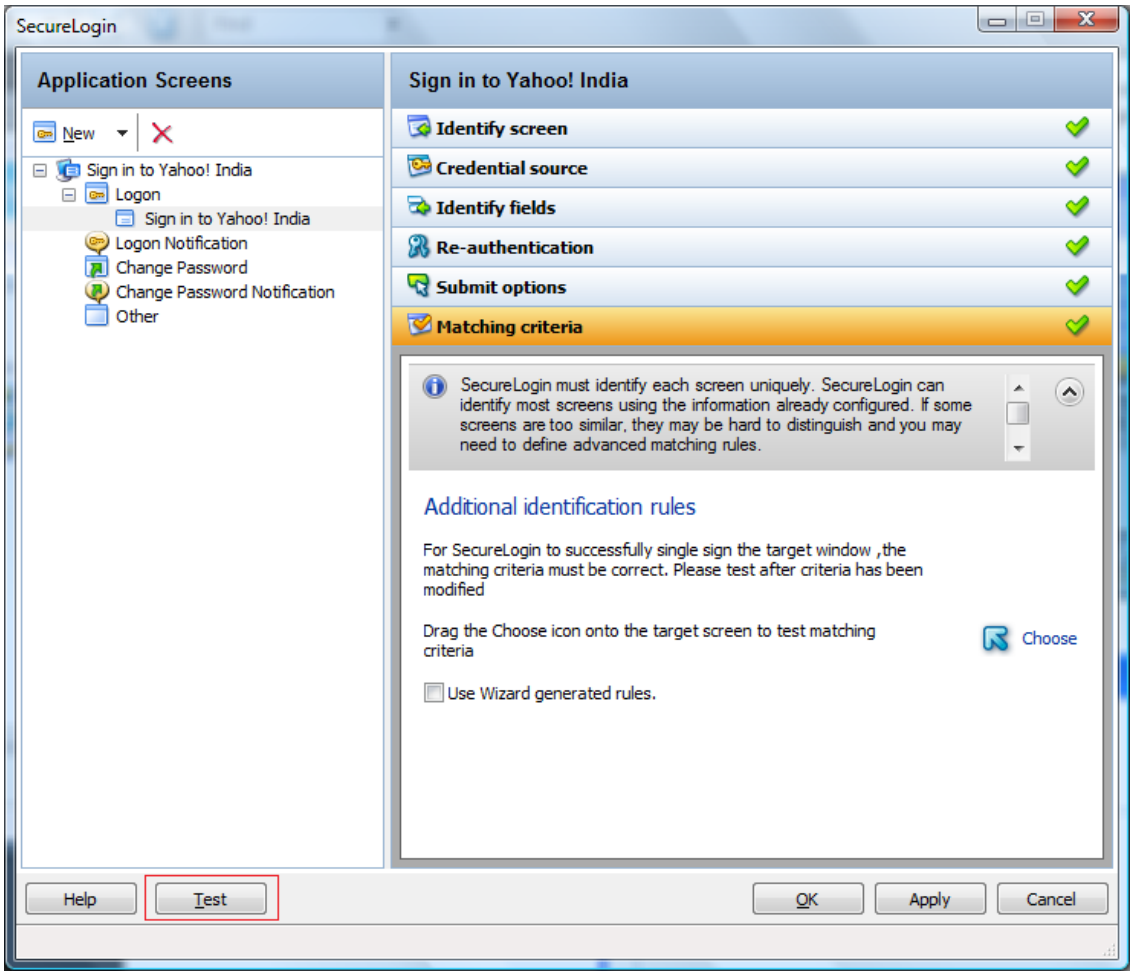
---

1 Make sure you have specified all of the attributes you want for the application definition.

Attributes that are included in the application definition are indicated by a green check mark  .

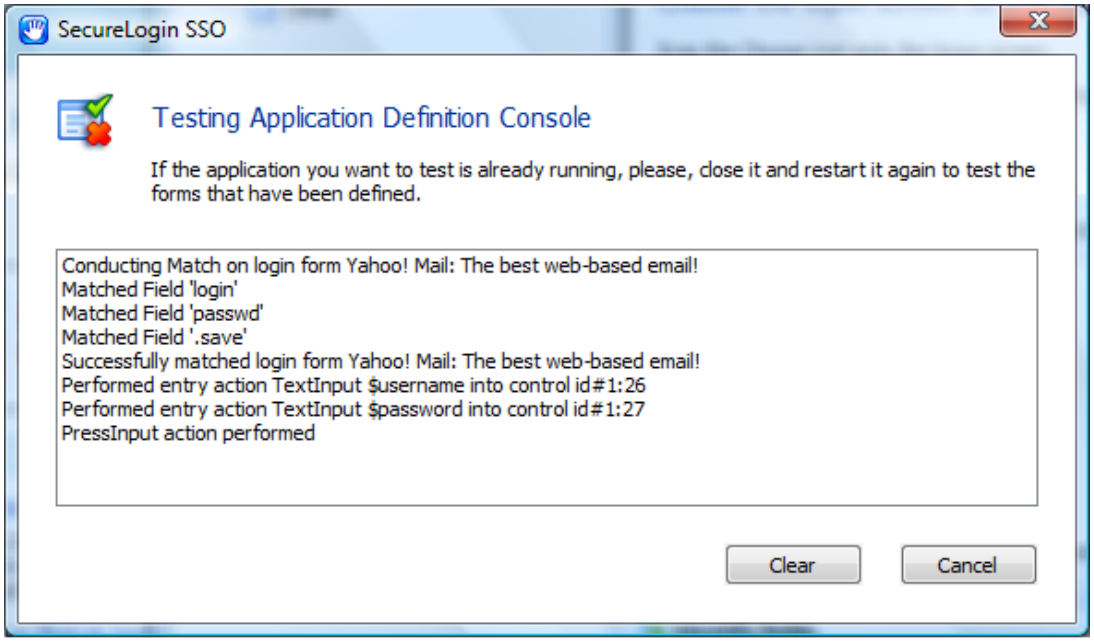
2 After you have completed specifying the attributes, click **Test**.

Only saved application definitions can be tested.



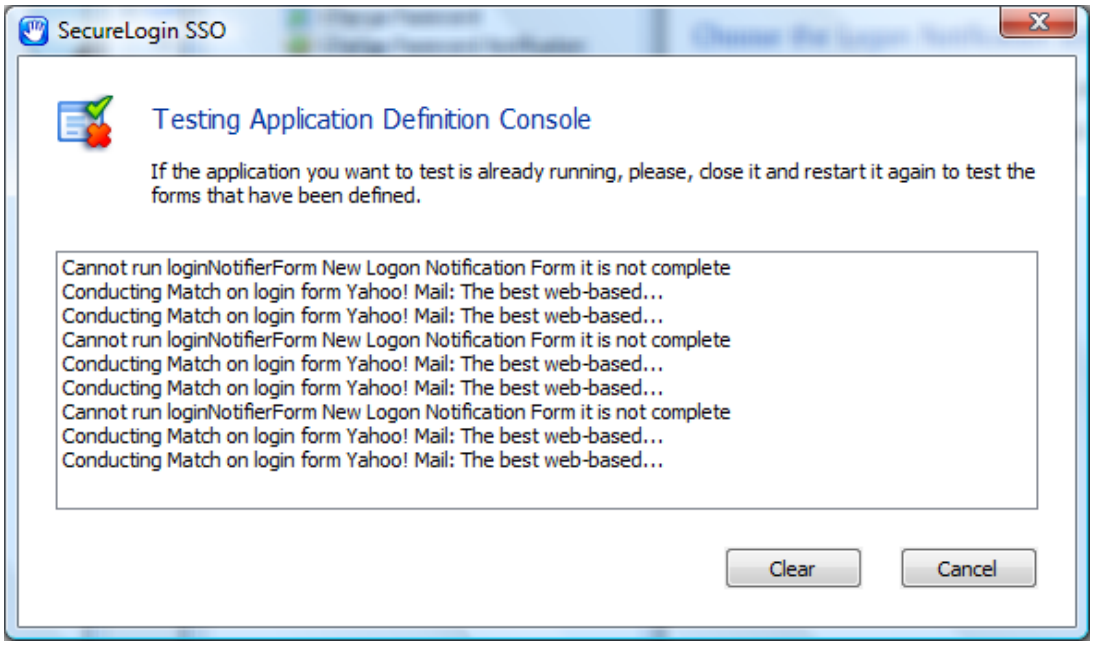
The Testing Application Definition Console displays a log of the following items:

- The steps SecureLogin takes to match the application you have started with the application definition.
- The fields matched by the wizard .
- If the credentials are successful, a message indicating that the login was successful.
- The actions performed on each of the fields.



3 Review the log to troubleshoot possible errors that occurred while creating the application definition.

The following graphic indicates that the application cannot be launched because the **New Logon Notification Form** is incomplete.



4 Select **Clear** to clear the log.

5 Select **Cancel** to close the Testing Application Definition Console and return to the Application Definition Wizard.

Deploying Application Definitions

An application definition created using the Application Definition Wizard is stored in the creator's object in the directory. You should create and test an application definition by using a test account before distributing it.

For detailed information on deploying and distributing the configuration, refer "Distributing Configurations" in the *NetIQ SecureLogin Administration Guide*.

Configuring Notifications

You can use the Application Definition Wizard to configure notifications such as login notifications and change password notifications.

- "Creating an Application Definition for Login Notification" on page 96
- "Creating an Application Definition for Change Password" on page 101
- "Creating an Application Definition for Change Password Notification" on page 108

Creating an Application Definition for Login Notification

You can use the **Logon Notification** menu to create application definitions that inform the users about an event that occurred during login, such as a mismatch of the username and password or an incorrect password. You can configure the notification to display all or part of the credentials to the user. A login notification is also a message that the application presents after SecureLogin submits the credentials.

NOTE: A login notification cannot be created if a login form is not defined.

For details on the tasks involved in creating a login notification, see "Login Notification" on page 26.

- "Example: Creating a GroupWise Messenger Login Notification" on page 96
- "Testing the Login Notification Application Definition" on page 100

Example: Creating a GroupWise Messenger Login Notification

In the following example, you create a login notification for the Google Talk.

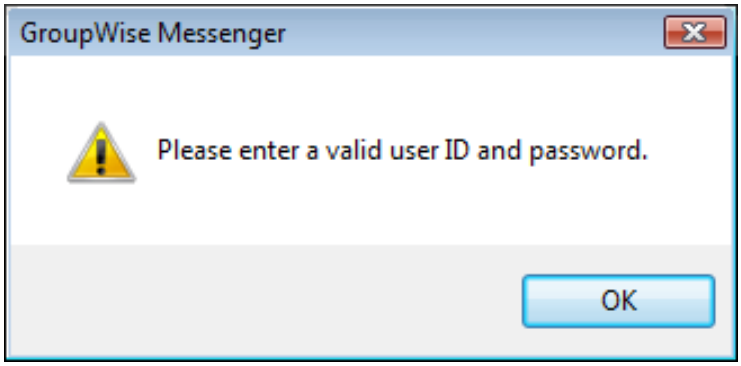
Prerequisites

- Create a login for GroupWise Messenger. That is, an application definition must be created for GroupWise Messenger.
- This example assumes that you have previously specified an incorrect username or password or, both.

1 Launch GroupWise Messenger.

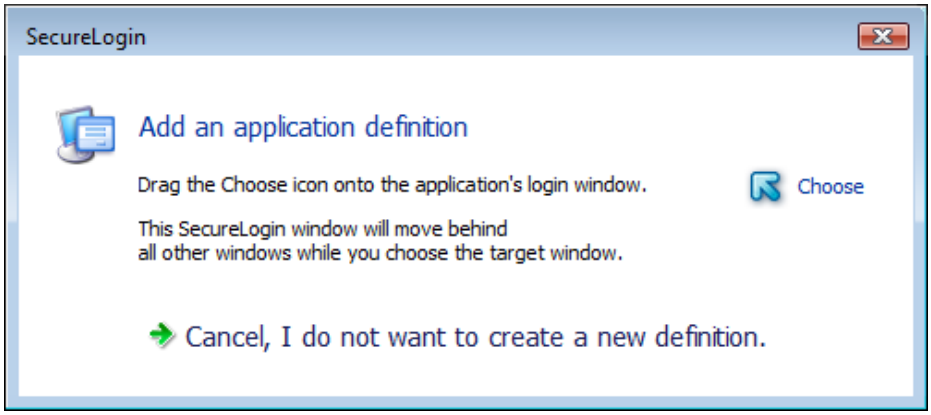
2 (Conditional) Because you have specified incorrect credentials when creating the application definition, SecureLogin detects the incorrect credentials and prompts you to specify correct credentials.

The GroupWise Messenger dialog box is displayed.



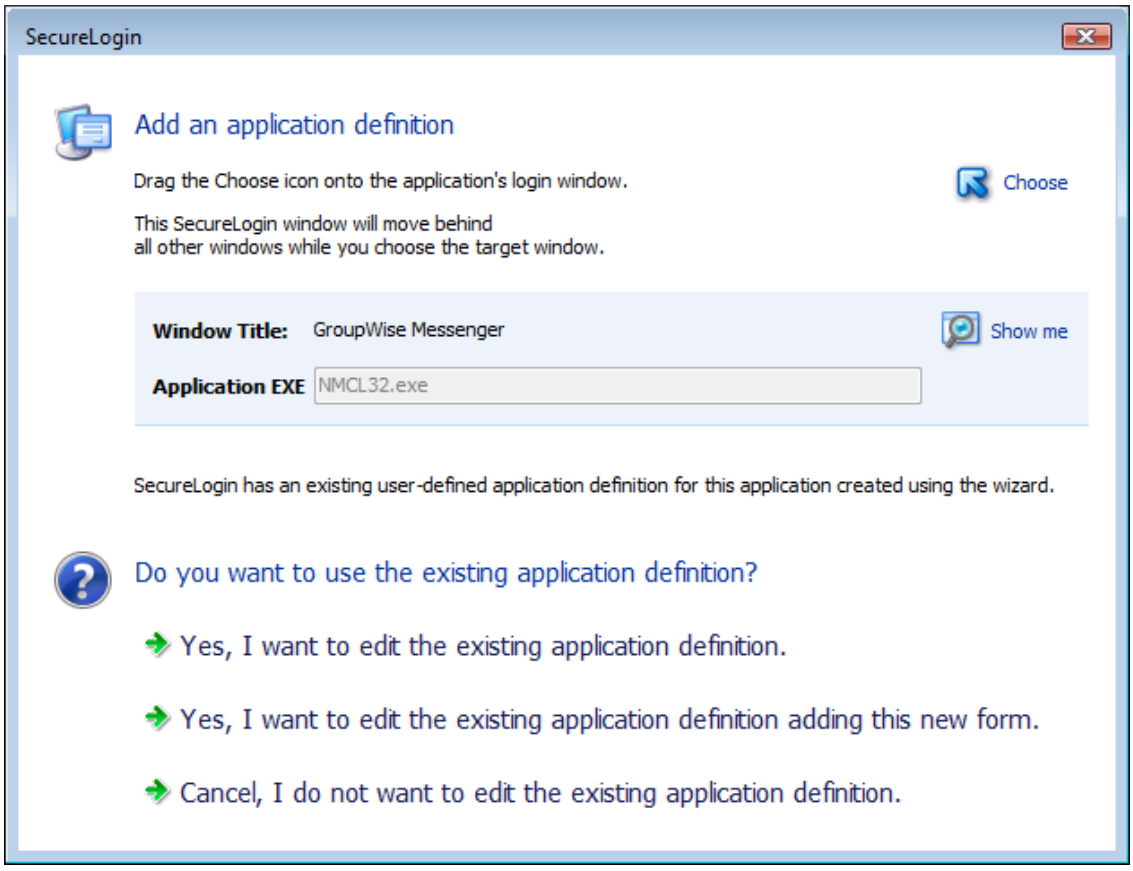
3 Right-click the SecureLogin icon on the notification area (system tray), then select **Add Application**.

The Add an Application Definition dialog box is displayed.



4 In this example, you have specified incorrect user ID and password. To identify the fields, drag the **Choose** icon to the GroupWise Messenger dialog box displaying the error message.

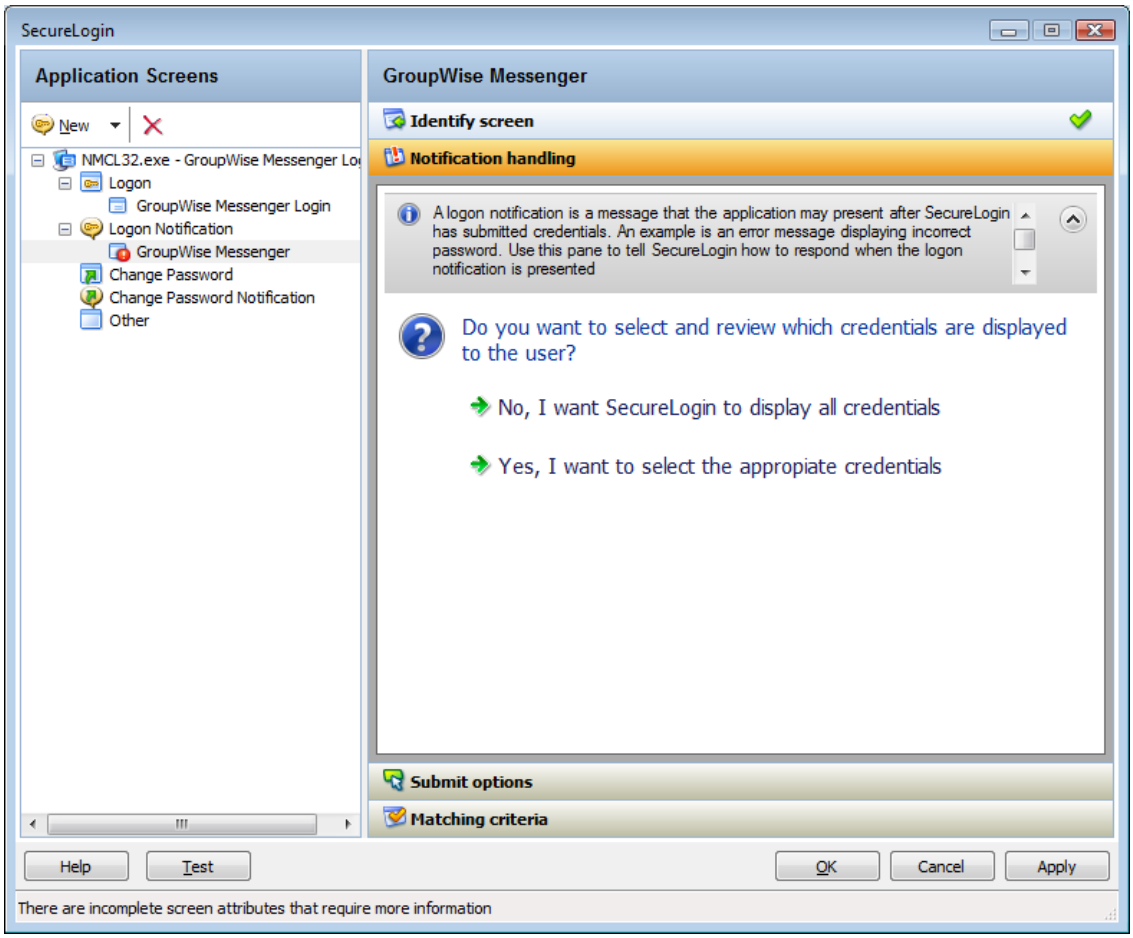
You are prompted to edit the existing application definition, edit the application definition by adding a new form, or not edit the application definition.



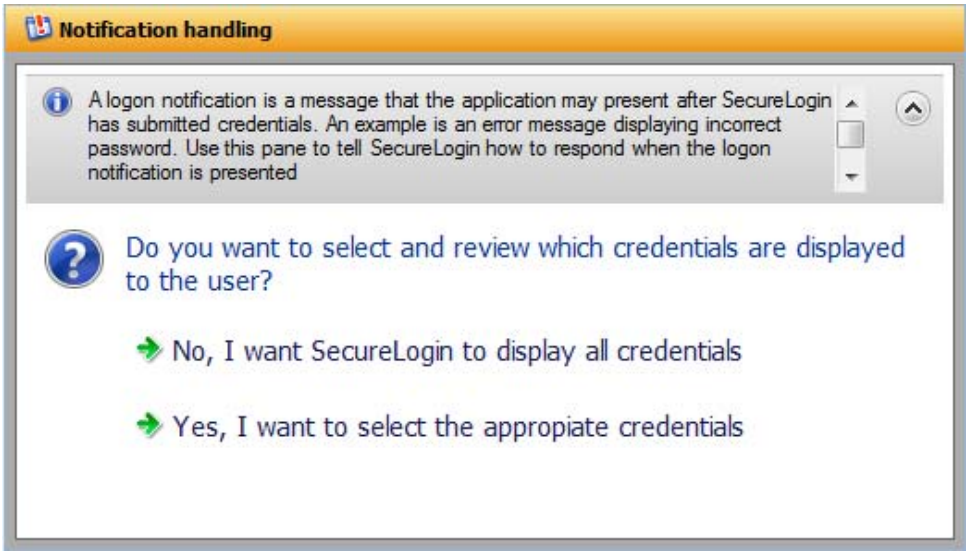
5 Select **Yes, I want to edit the existing application definition adding this new form**.

The Application Definition Wizard opens. The Identify Screen menu has a green check mark because the fields are identified correctly.

NOTE: A form named GroupWise Messenger is created under **Logon Notification**.

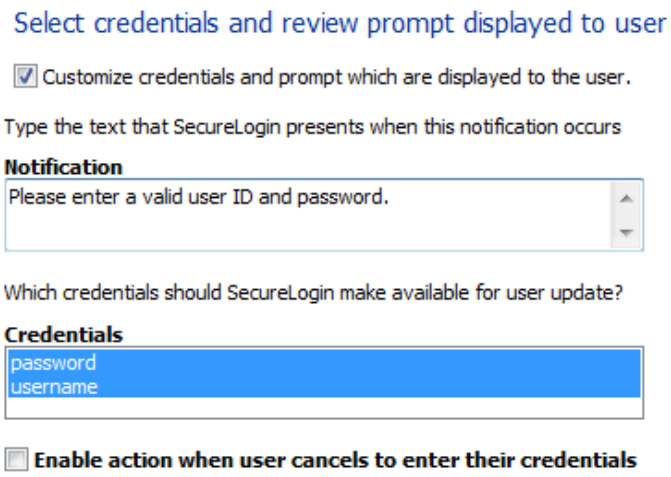


6 Navigate to the **Notification Handling** menu.



7 Select **Yes, I want to select the appropriate credentials**.

8 In the **Notification** text box, specify the message that is presented to the user.



9 From the **Credentials** list, select the credential for which you want to create a notification. In this example, select **Password**.

10 Navigate to the **Submit options** menu.

11 Specify how the login notification screen is submitted. Select **SecureLogin submits the screen**.

By default, the **SecureLogin submits the logon notification screen** is selected

12 Select the **Click this button** option. In this example, the **OK** button is identified by the wizard to submit the login screen.

13 Navigate to **Matching criteria** menu.

14 Select **No. Use minimal rules based on your previous selections**.

15 Click **Apply** to save your settings.

16 Click **OK** to exit the Application Definition Wizard and return to the SecureLogin Client Utility page.

17 Click **Apply** and **OK** to exit.

You have successfully created an application definition to handle a login notification. Next, test the application definition.

Testing the Login Notification Application Definition

1 Launch GroupWise Messenger.

In “Creating an Application Definition for Login Notification” on page 96 you created an application definition to notify the wrong password.

Because you specified a wrong password when enabling Google Talk for single sign-on, you are prompted to specify the credentials. The message is displayed on the Enter your Credentials dialog box is the message that you specified.

2 Specify the correct password to log in successfully.

Creating an Application Definition for Change Password

Application definitions can also include instructions for changing the password for an application. SecureLogin can automatically generate new passwords for an application that match your organization's password policy or it can allow users to select new password. You can also customize the change password prompts displayed to the users.

- "Example: Creating a Gmail Change Password" on page 101
- "Testing the Change Password" on page 107

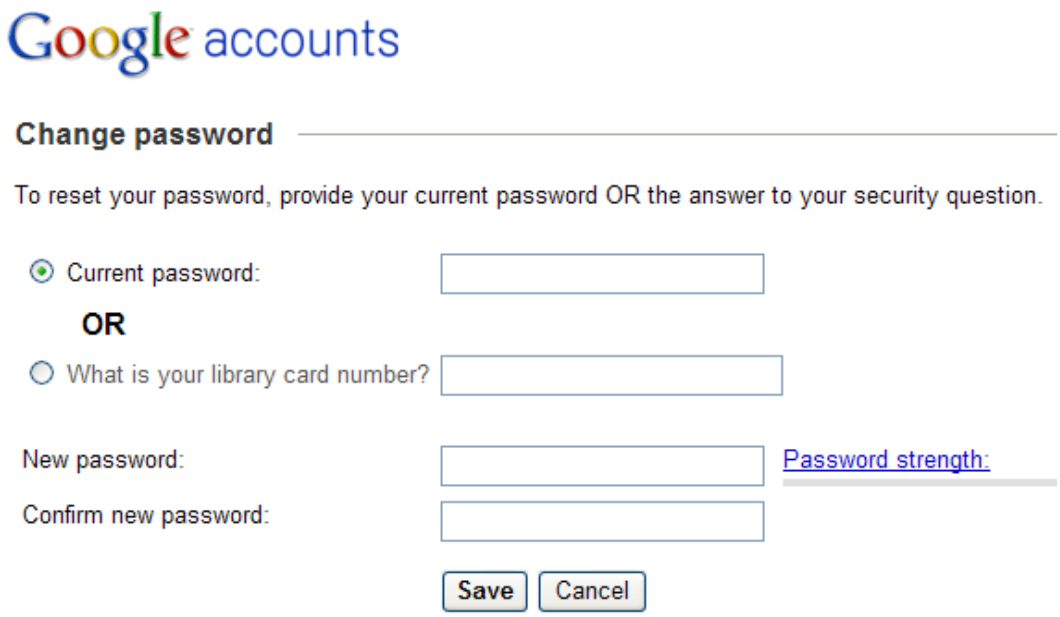
Example: Creating a Gmail Change Password

Prerequisite

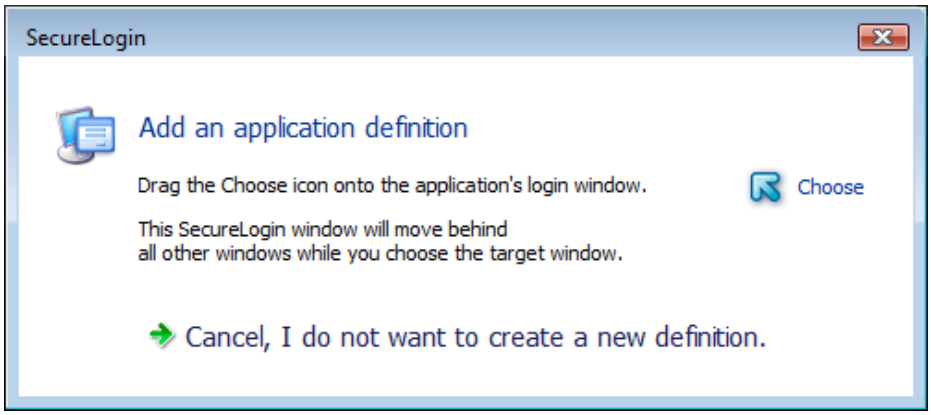
- Create a login for Gmail*. That is, an application definition must be created for Gmail.

1 Launch Gmail.

2 Navigate to the **Change Password** screen.



3 Right-click the SecureLogin icon on the notification area (system tray), then select **Add Application**.

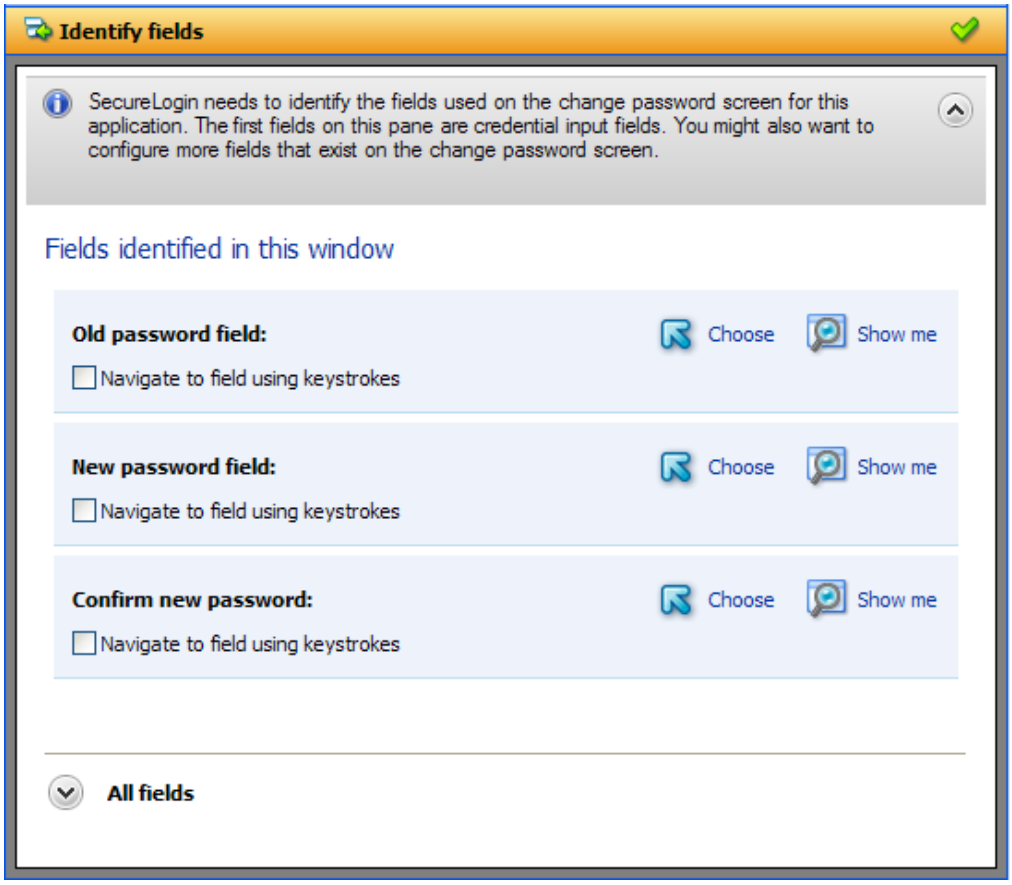


4 Drag the **Choose** icon to the change password screen.

5 Select **Yes, I want to edit the existing application definition adding this new form**.

The Application Definition Wizard opens. The **Identify Screen** menu has a green check mark because the fields are identified correctly.

By default, the **Identify Fields** menu is displayed.



6 From the Fields identified in this windows, click **Show me** to verify if the **Old password**, **New password**, and **Confirm new password** fields are identified correctly.

7 Navigate to **Password generation** menu. Specify how you want to generate a new password: whether the user specifies the password or allow SecureLogin to generate a new password.

8 Select **The user chooses a new password**.

Specify how the new password is managed. By default, **The user chooses a new password** option is selected.

9 Specify a prompt that is displayed to the user.

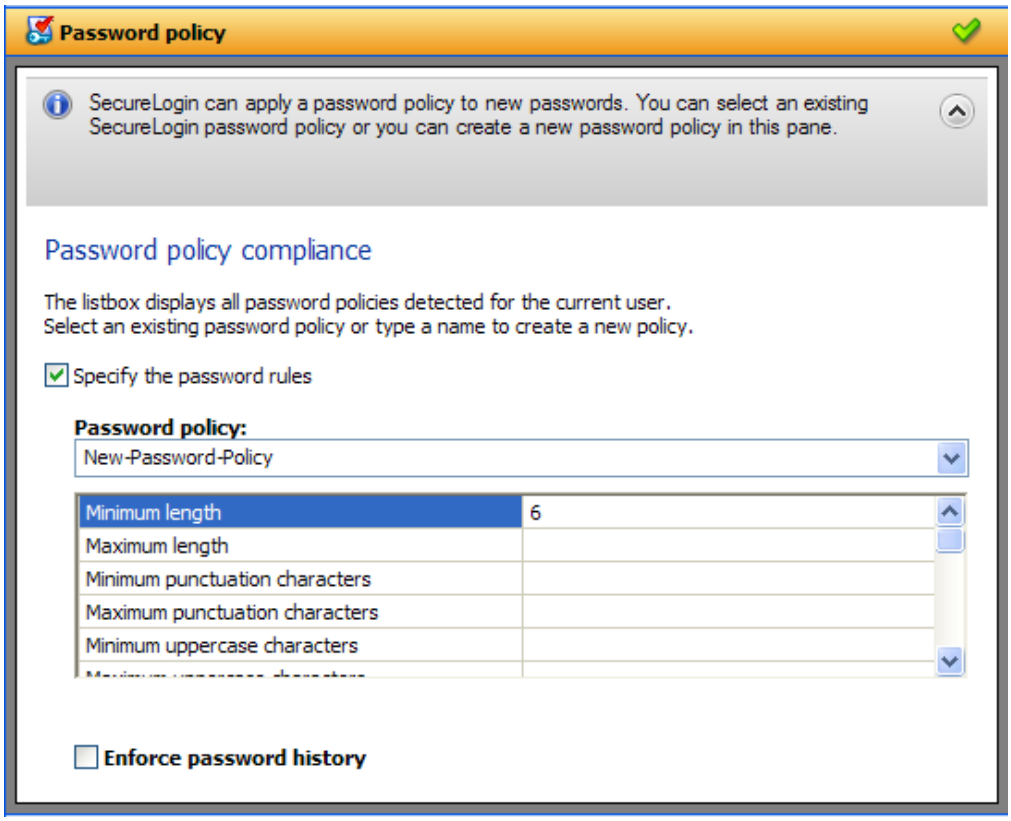
10 Navigate to the **Password policy** menu.

Specify whether you want to apply a password policy for the application.

11 Select **Yes. Let me specify the password rules**.

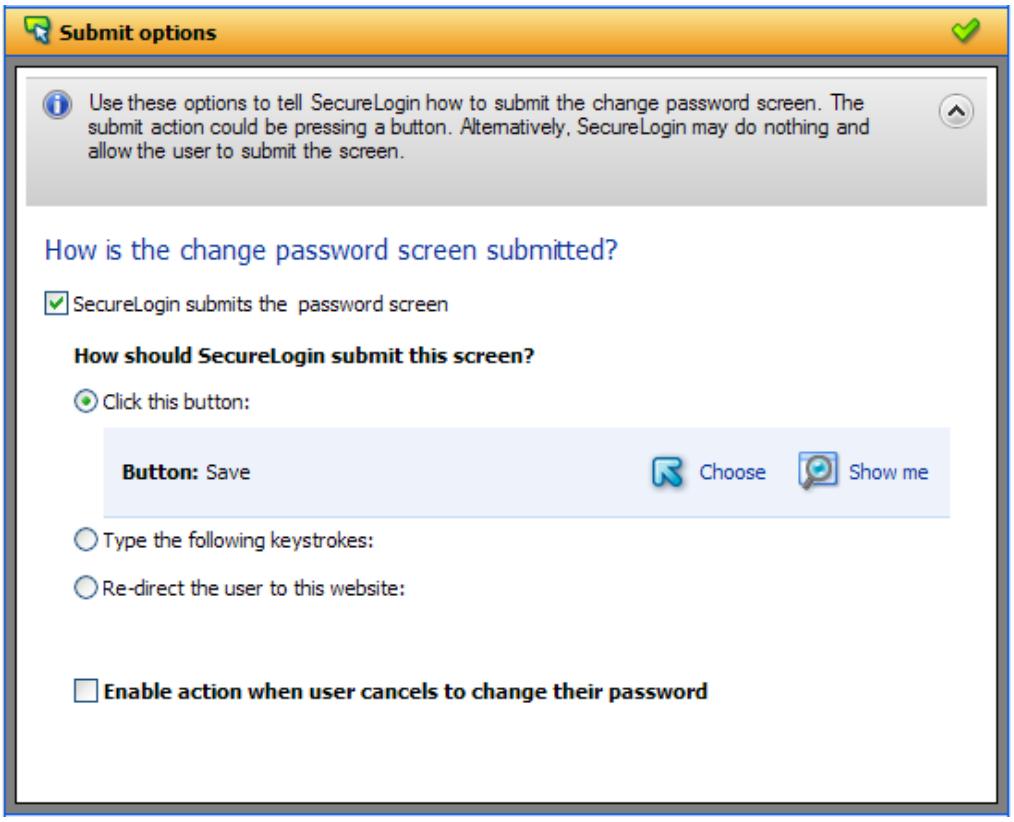
12 In the **Password policy** field, sepcify a name for the password policy.

13 From the password policy rules, specify the rules that apply to the new policy.

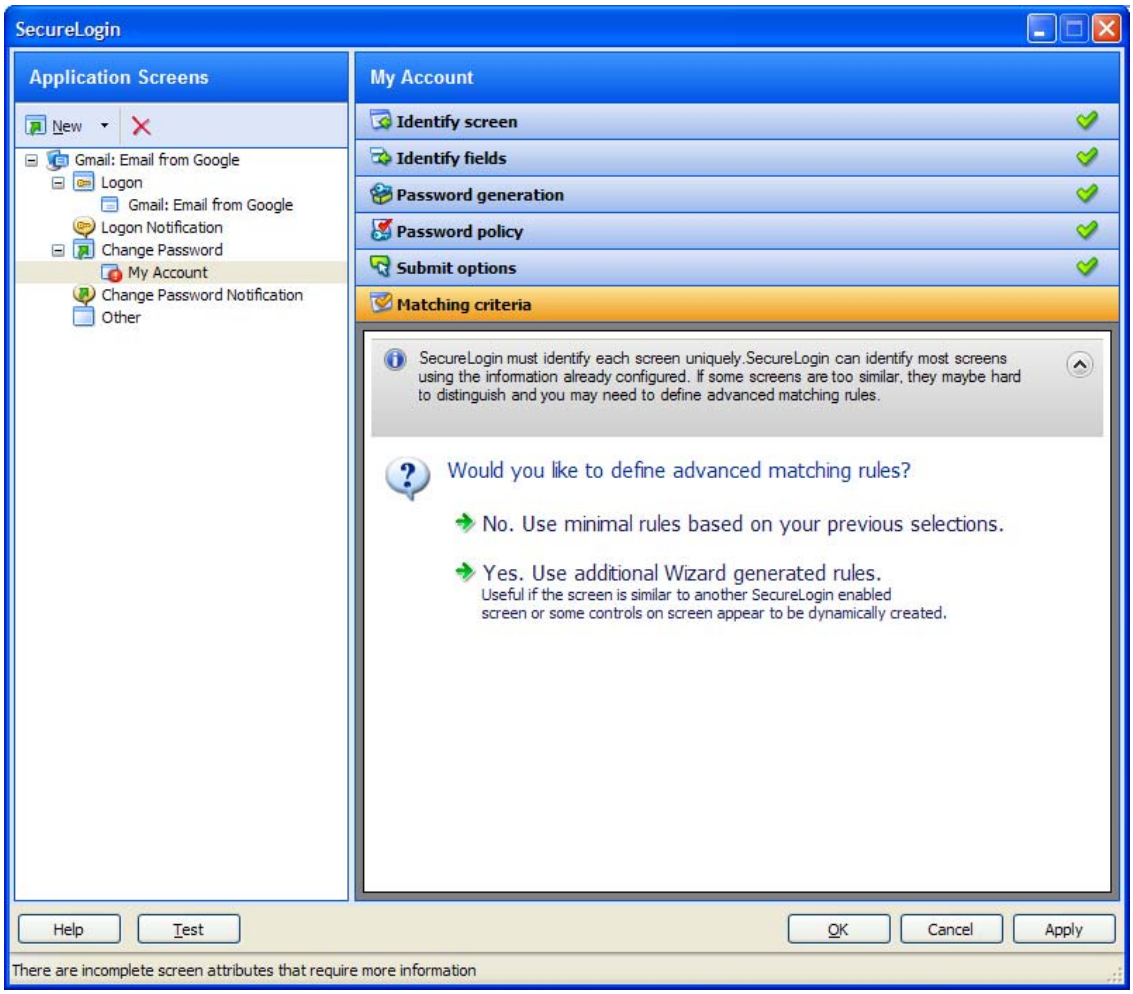


14 Navigate to the **Submit options** menu. Specify how the change password screen is submitted.

15 Select **SecureLogin submits the password screen**.



16 Navigate to the **Matching criteria** menu. Specify how SecureLogin uniquely identifies each screen.



17 Select **No. Use minial rules based on your previous selections**.

18 Click **Apply** to save your settings.

19 Click **OK** to exit the wizard.

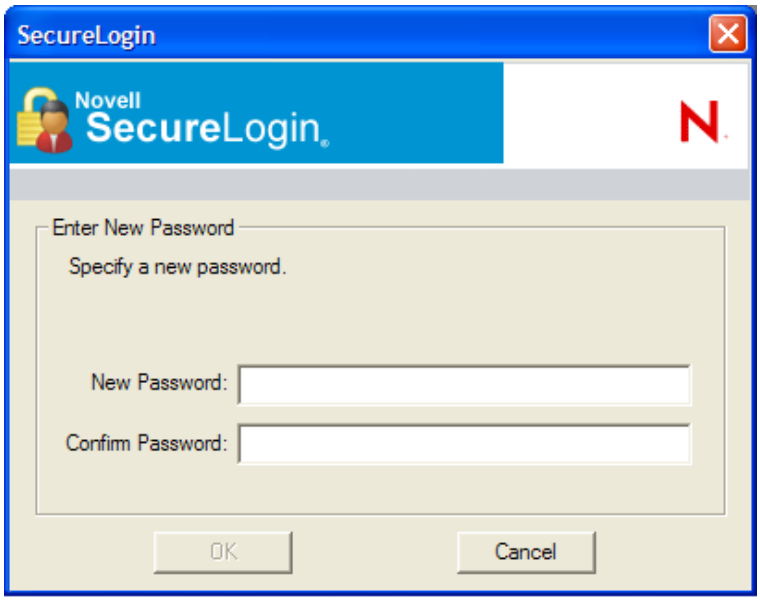
You have successfully completed creating an application definition for Gmail change password screen.

Testing the Change Password

The next time you launch Gmail and try to change the password, the application definition you created in “Creating an Application Definition for Change Password” on page 101.

1 Launch Gmail.

2 Navigate to the **Change Password** screen. The following dialog box appears.



3 Specify the new password and confirm the new password.

IMPORTANT: Ensure that the password policy you have set in Step 13 is adhered.

4 Click OK.

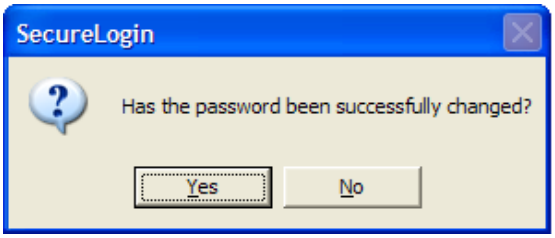
Creating an Application Definition for Change Password Notification

A Change Password Notification is a message that the application displays after SecureLogin submits the new password. This might be a confirmation or an error message.

NOTE: You cannot create an application definition for change password notification if a change password form is not defined.

This notification is important for SecureLogin to know whether the password is changed successful because it needs to update the credentials for the application after they are updated.

If an application definition is created for change password but not defined for change password notifications, SecureLogin displays the following prompt:



This prompt appears before updating the credential set with the new password if it is changed successfully.

In the following example, we will create an application definition for change password notification for Gmail application. In this example, we will consider a successful change password.

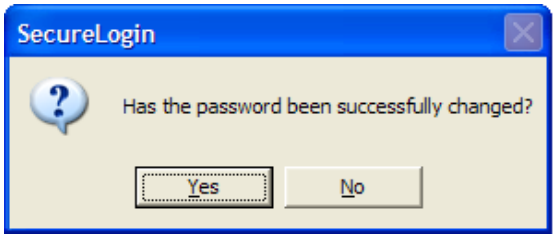
Prerequisite

- An application definition is created for Gmail change password form.

Assumption

- The change password for Gmail is successful.

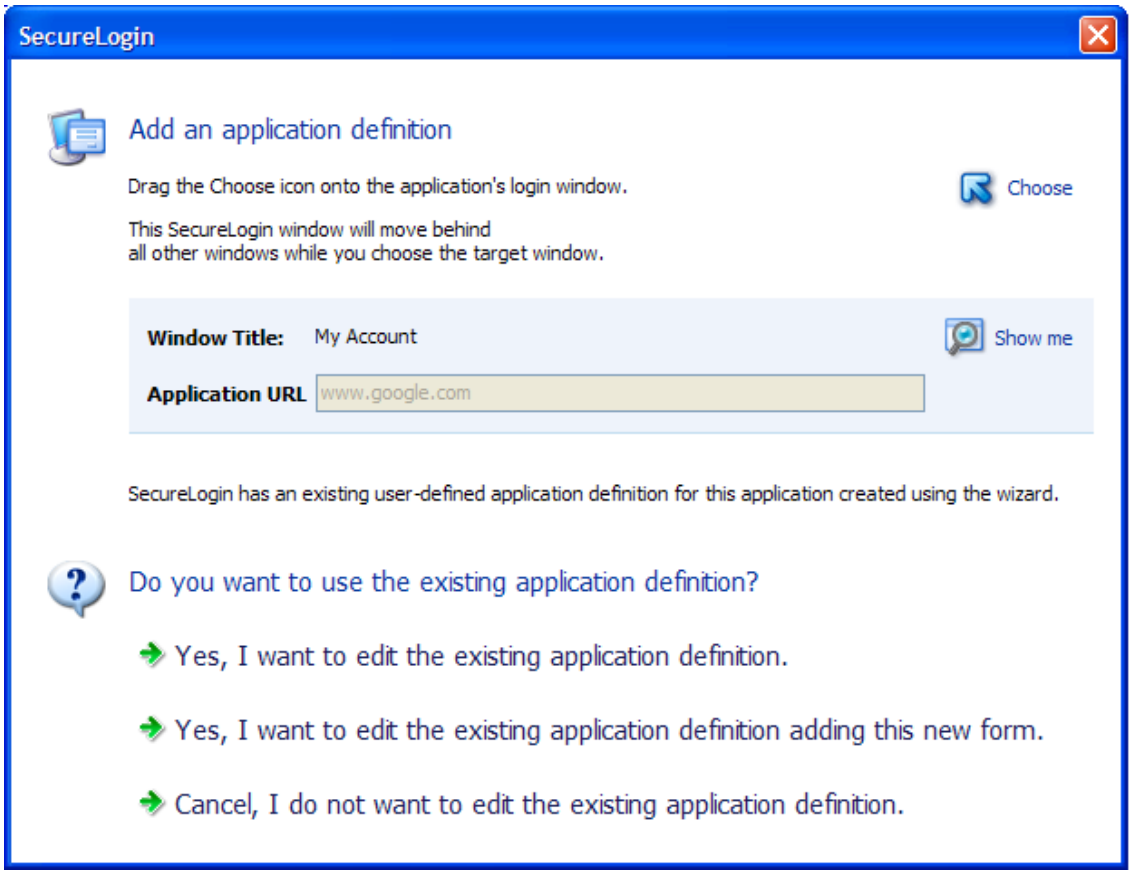
1 Because you have not yet definied the change password notification, you are prompted whether the password is changed successfully. The following prompt appears:



2 Right-click the SecureLogin icon on the notification area (system tray), then select **Add Application**.

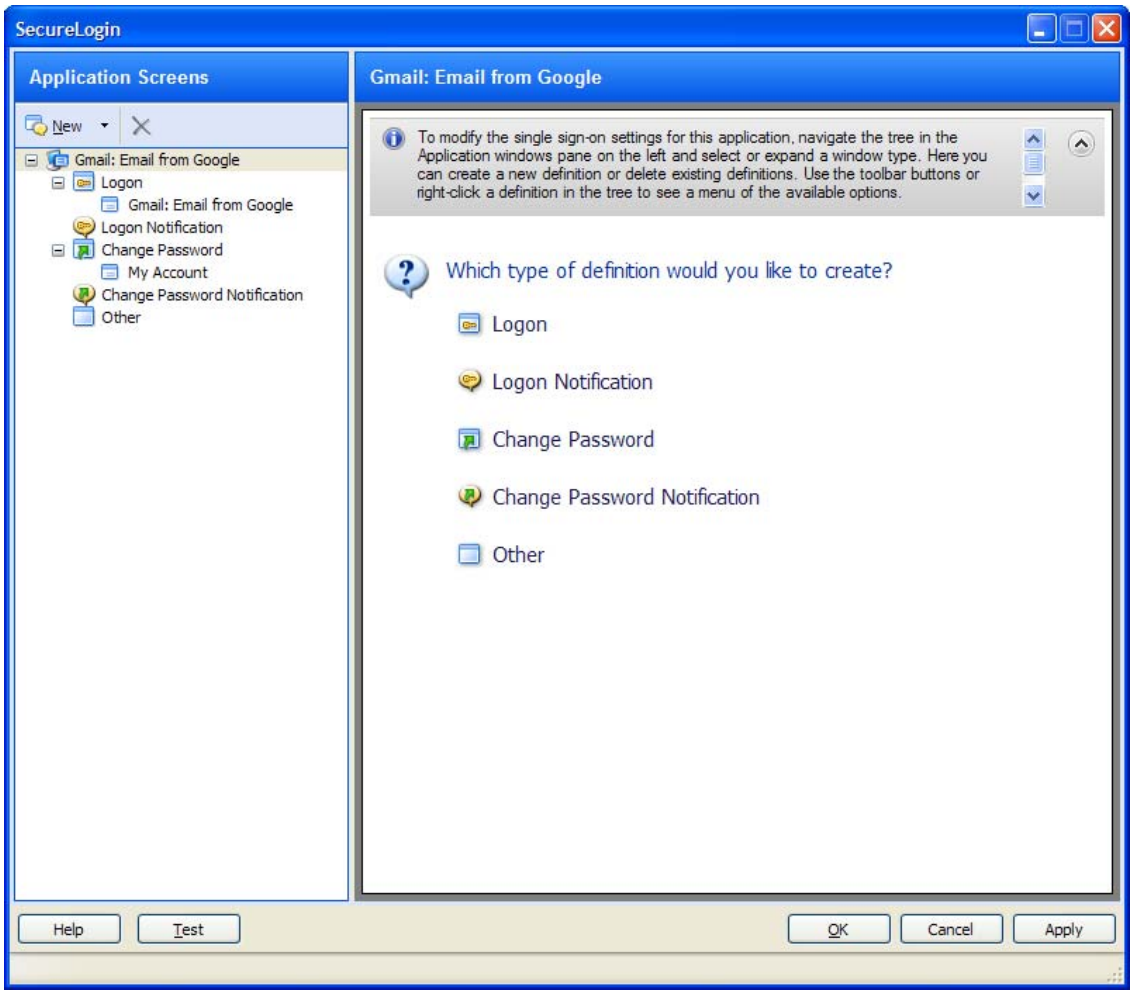
3 Drag the **Choose** icon to the change password successful message screen. In this example the message is, `Your new password has been saved - OK`.

The Add an Application Definition prompt is displayed.



4 Select **Yes, I want to edit the existing application definition**. You are prompted to select the type of definition.

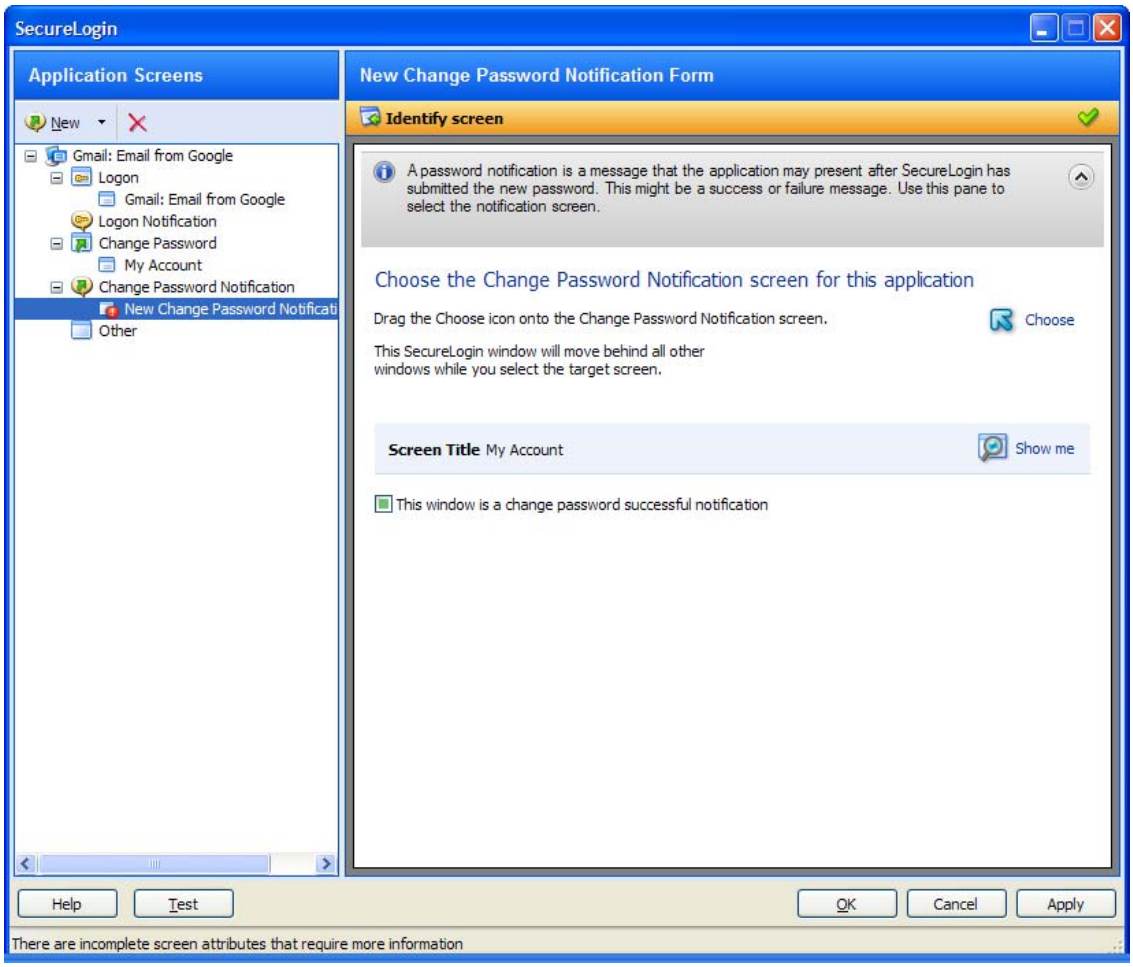
5 Select **Change Password Notification**.



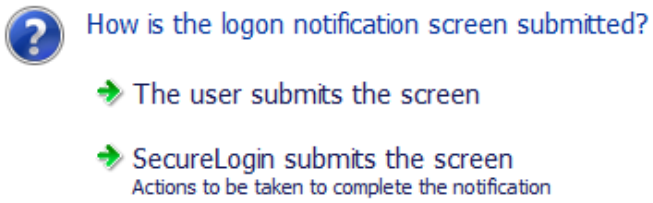
6 Drag the **Choose** icon to the change password notification screen.

7 (Conditional) To specify options that will be available for a user whose password change is successful, select the **This window is a change password successful notification** option. On a successful password change, the changed password is stored and the password notification can be dismissed.

8 (Conditional) To specify options that will be available for a user whose password change fails, deselect the **This window is a change password successful notification** option. On a failed password change, the entered password is removed, the password notification is dismissed, and the password change process is restarted.



9 (Optional) Select **SecureLogin submits the screen**.



Continue with Step 11.

10 (Optional) Select **Nothing. Allow user to manage the response**.

11 Navigate to **Matching criteria** menu. Specify the rules to match.

12 Seelct **No. use minial rules based on your previous selections**.

13 Click Apply to save your application definition.

14 Click OK to exit the wizard.

4 Modifying Application Definitions

You can use the Application Definition Wizard to modify your application definitions.

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

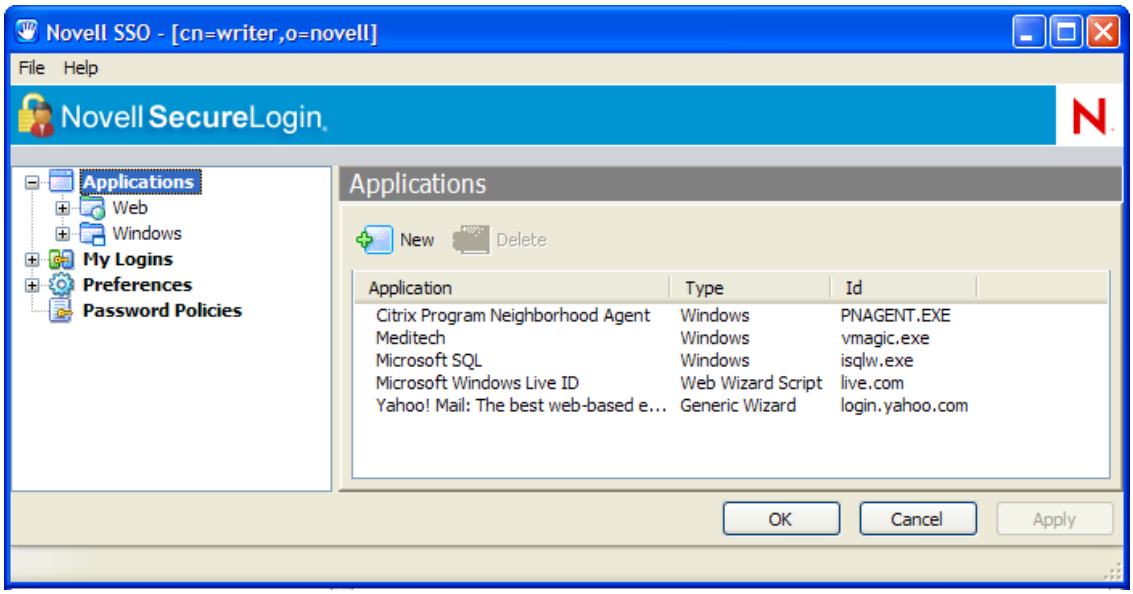
You can modify an application definition in one of the following ways:

- "Using the Application Definition Wizard to Modify an Application Definition" on page 113
- "Using the Manage Logins Menu to Modify the Application Definition" on page 115

Using the Application Definition Wizard to Modify an Application Definition

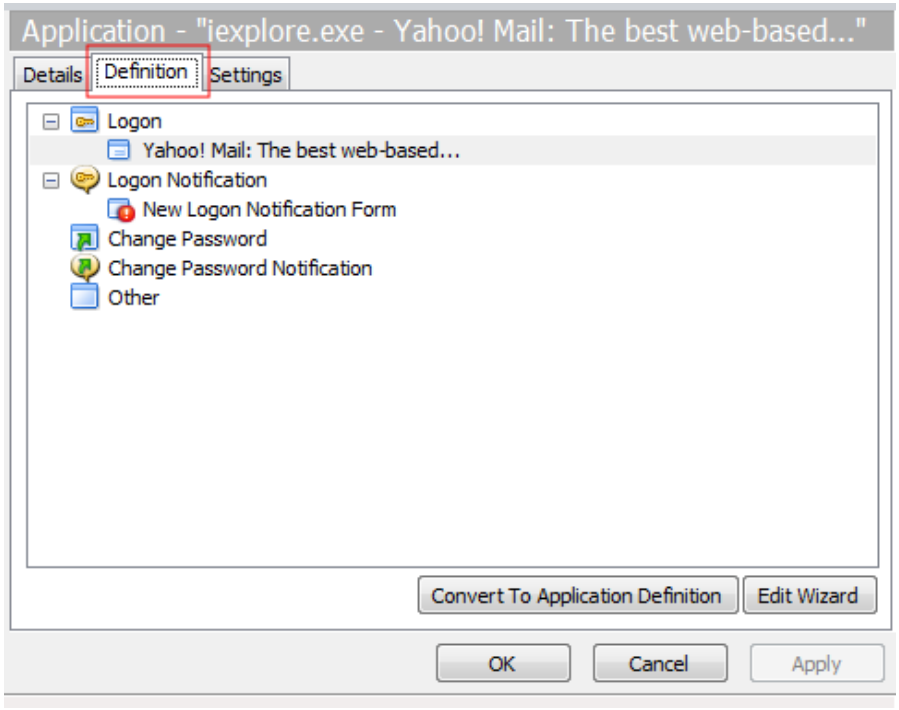
1 Double-click the SecureLogin icon in the notification area.

The Application Definition Wizard opens, displaying a list of applications enabled for single sign-on.

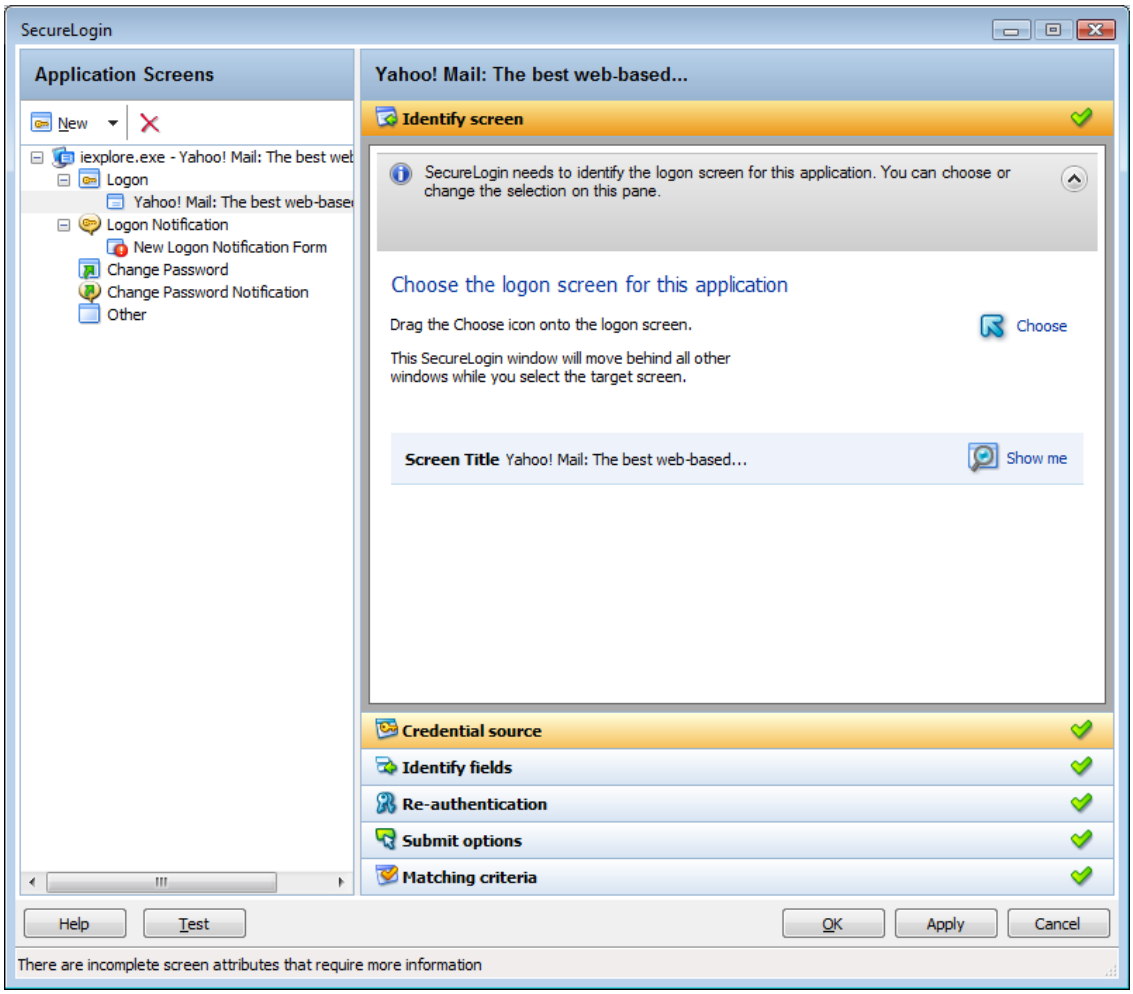


2 From the **Applications** pane, select the application definition you want to modify.

3 Click the **Definition** tab.



4 Select **Edit Wizard**. The attributes pane opens, enabling you to edit the application definition.



5 Change the application definition.

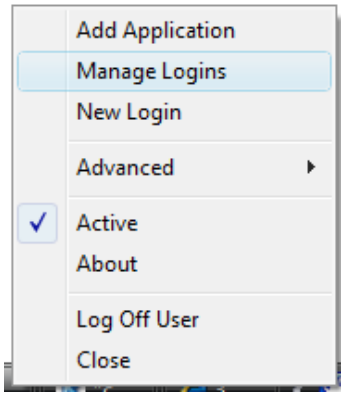
For more information on attributes that can be modified for an aplication definition, see “The Application Screens Pane” on page 10.

6 Click **Apply** to save your changes.

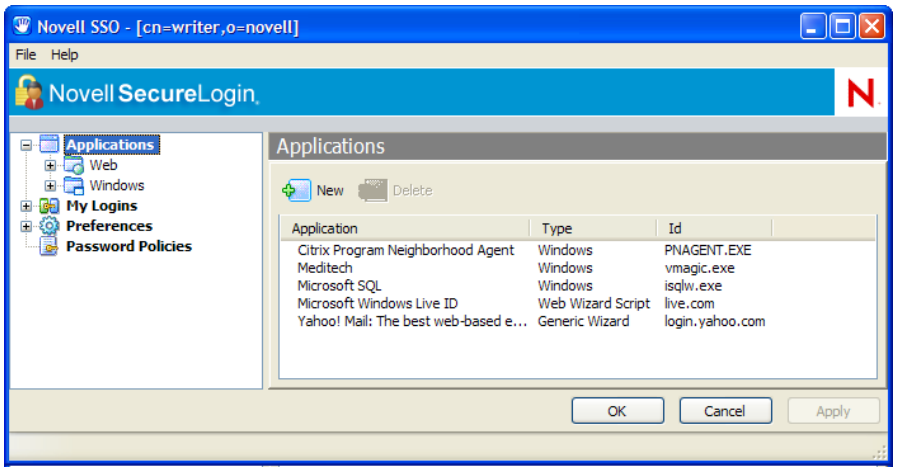
7 Click **OK** to exit.

Using the Manage Logins Menu to Modify the Application Definition

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

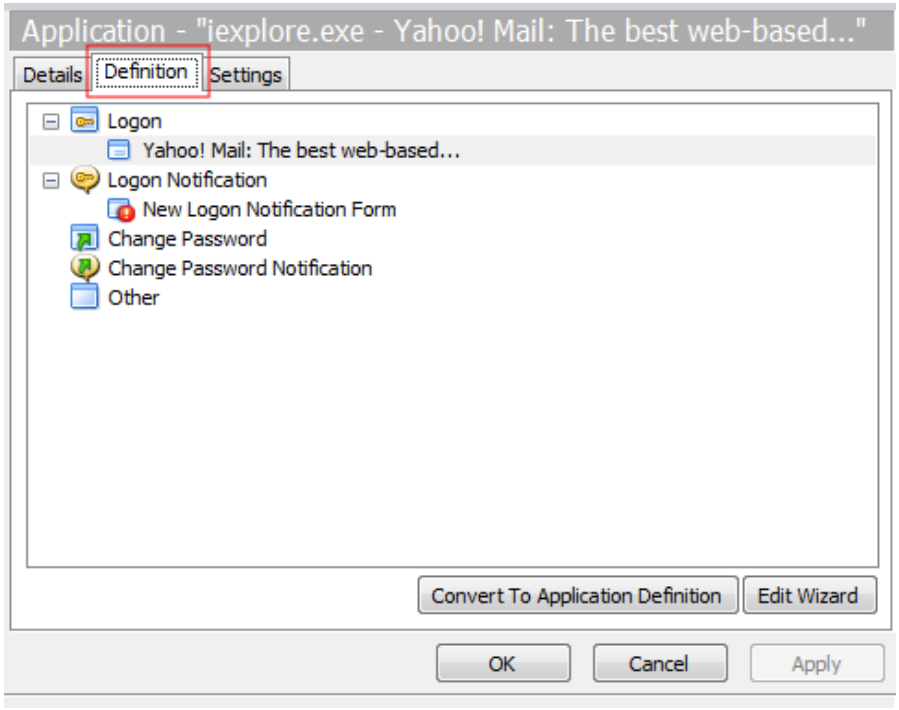


2 The administrative management utility displays a list of applications that are already enabled for single sign-on.

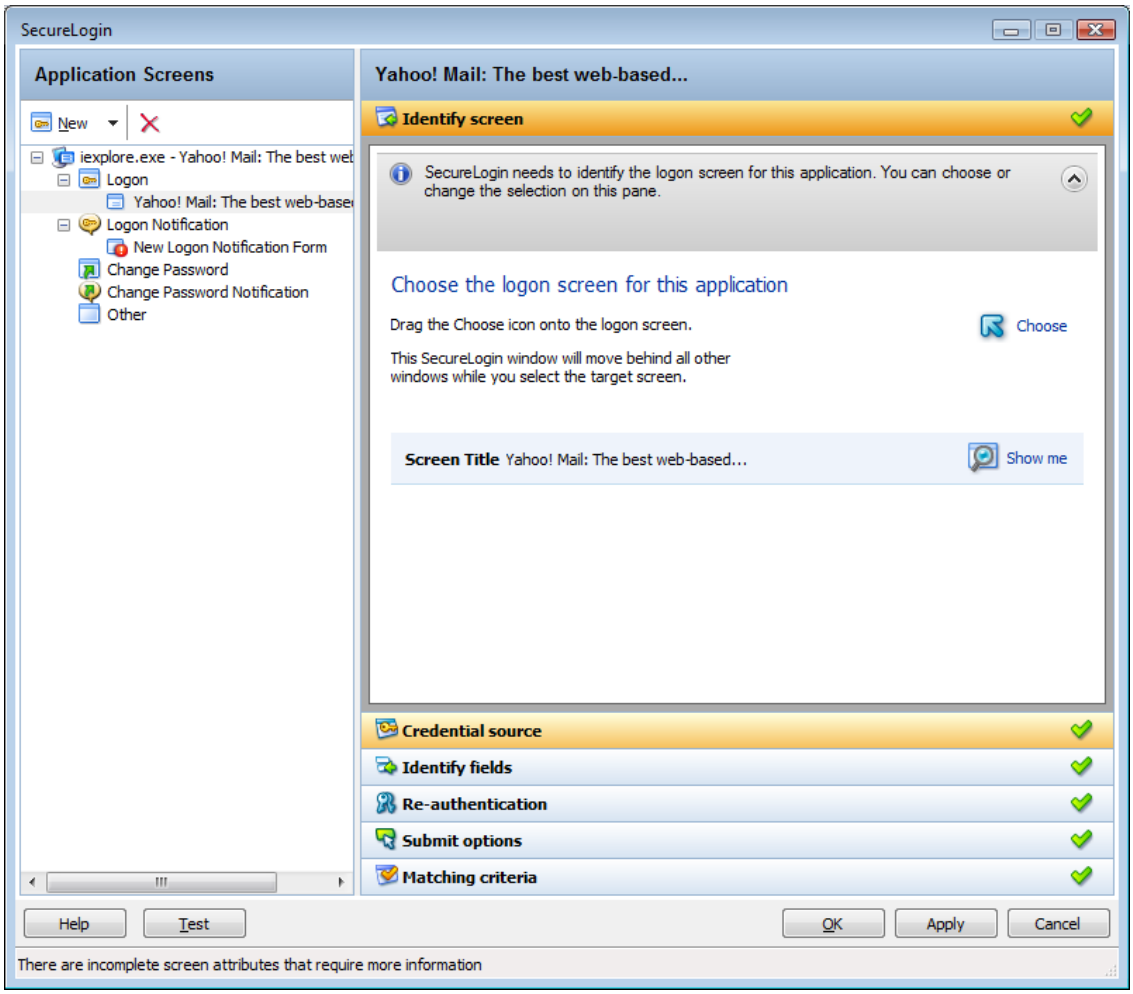


3 From the **Applications** pane, select the application definition you want to modify.

4 Click the **Definition** tab.



5 Select **Edit Wizard**. The attributes pane opens, enabling you to edit the application definition.



6 Make the changes.

For more information on attributes that can be modified for an aplication definition, see “The Application Screens Pane” on page 10.

7 Click **Apply** to save your changes.

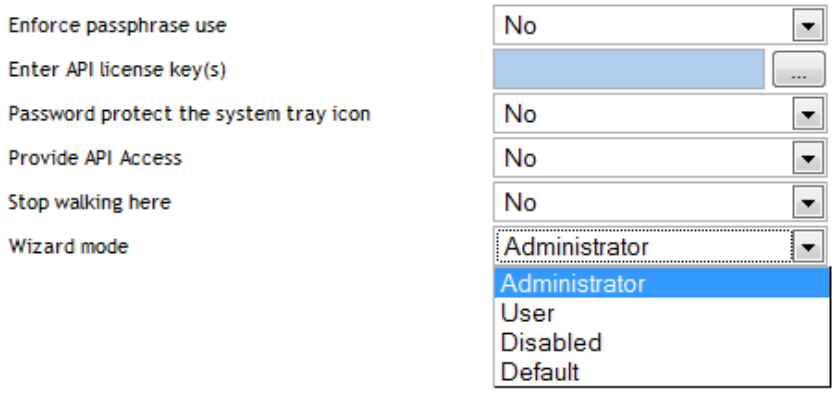
8 Click **OK** to exit.

5 Setting the Wizard Mode Preference

Access to the Application Definition Wizard is controlled by the SecureLogin Wizard Mode preference, which is available in the administrative management utilities. You can enable or disable access to the Application Definition Wizard for users.

1 Launch the administrative management utilities (iManager, SLManager, or MMC snap-ins).

2 Navigate to **Preferences** > **General** > **Wizard mode**.



The **Wizard Mode** has three settings:

- **Administrator:** The **Administrator** option controls users access to the Application Definition Wizard.

  If the **Wizard mode** is set to Administrator, users can create and edit application definitions by using the Wizard.

  This is the default setting.

- **User:** The **User** preference controls a user's ability to create login credential sets for new applications by using the auto-detection setting.

  If the preference is set to **User**:

  - The **I want to single sign enable using the wizard** option is not available when an application is detected for single sign-on.
  - The **Edit Wizard** button is disabled in the SecureLogin Client Utility.
  - The **Add Application** option is not available from the SecureLogin icon in the notification area.

- **Disabled:** This preference controls launching the Application Definition Wizard when an application is detected for single sign-on.

  If the **Wizard mode** preference is set to **Disabled**:

  - All automatic prompts to enable an application for single sign-on are disabled. The user is not prompted to enable any application for single sign-on.
  - The **Edit Wizard** button is disabled in the SecureLogin Client Utility.
  - The **Add Application** option is not available from the SecureLogin icon in the notification area.

NOTE: The **Allow user to modify application definitions** preference overrules the **Wizard mode** preference. If users are not allowed to modify application definitions, the Wizard preference has no effect.

- **Default:** The **Default** setting is the same as Administrator setting.

3 Select the options you want to set.

4 Click **Apply** and **OK** to save and exit.

6 Deploying Application Definitions

If you use the Application Definition Wizard to create an application definition, the definition is stored in your user object in the directory.

Restrict the access to the Application Definition Wizard to administrators only. Create and test application definitions on a test account deploying them in the organization. For details on distributing the application definition configurations, see “Distributing Configurations” in the *NetIQ SecureLogin Administration Guide*.

For information on manually creating and editing an application definition, see the *NetIQ SecureLogin Application Definition Guide*.

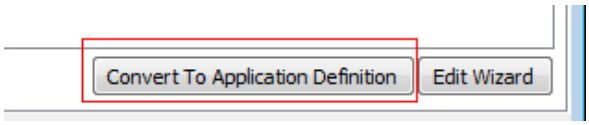
7 Compatibility with Earlier Versions

The Application Definition Wizard is designed for SecureLogin version 7.0 and later. You cannot use the Application Definition Wizard to edit application definitions created or edited manually by using previous versions. You can only manually edit the application definitions created in the earlier versions.

However, you can export the application definition created in previous versions for manual editing. For details on exporting the application definition configurations, see “Distributing Configurations” in the *NetIQ SecureLogin Administration Guide*.

To edit the old application,

1. Double-click the SecureLogin icon on the notification area (system tray).
2. From the **Applications** list, select the application definition you want to edit.
3. Click the **Definition** tab, then click **Convert to Application Definition**.



   The application definition pane opens in the **Definition** tab.
4. Manually add the application definition and export to the earlier version.

IMPORTANT: If you want to edit a particular application definition using the Wizard, delete the earlier application definition from the directory before editing the chosen application definition.

8 Limitations, Tips, and Troubleshooting

Some applications cannot be enabled for single sign-on using the Application Definition Wizard. This section provides information of the support for such applications.

- “Limitations” on page 125
- “Tips” on page 126
- “Troubleshooting” on page 129

Limitations

- “Support for .NET Framework” on page 125
- “Support for Non-Natively Supported UI Framework” on page 125
- “Defining Password Notification” on page 126
- “Specifying Reauthentication Rules” on page 126
- “Incorrect Login Notifications in Mozilla Firefox” on page 126
- “Single Sign-On For Microsoft Windows Vista Remote Desktop Client” on page 126

Support for .NET Framework

SecureLogin 8.1 supports .NET Framework 3.5 SP1 and later. However, the .NET Framework should already exist for SecureLogin to use it. So, ensure that the framework is available in your system before installing SecureLogin 8.1 or upgrading to SecureLogin 8.1.

Support for Non-Natively Supported UI Framework

You cannot enable single sign-on for applications that are built in on non-natively supported UI framework such as Microsoft .NET framework, Gecko, and QT.

For example, applications such as Mozilla Thunderbird 2.0.0.18, Novell iFolder cannot be enabled for single sign-on using the Wizard. The Wizard fails to detect the control to enable these applications. You can however, enable single sign-on for such applications without using the Wizard.

For some applications, such as Mozilla Thunderbird, though you can use the keystrokes, SecureLogin identifies the login fields wrongly. It identifies both the username and password fields only when the password dialog box appears.

To resolve this problem, deselect the **Navigate to field using keystroke** option for the username and proceed to enable single sign-on.

The buttons in Windows applications that contain QT controls are displayed as Edit fields.

This incorrect identification is because all QT controls are part of an unsupported Windows class framework, QWidget. As buttons are also QWidgets, they are identified and displayed as Edit fields.

Defining Password Notification

You cannot use the Application Definition Wizard password notification if the application displaying the password notification, such as invalid credentials is different from the application displaying the credentials.

For example, application definition for Novell iPrint Client fails because the Windows Wizard does not detect failed authentication.

This is a limitation in the design of the Wizard. The application prompting for credentials is different from the application displaying the authentication failure. The Wizard does not support this and it is handled by the `SetPlat` script. For information on the "SetPlat "script, refer to the *NetIQ SecureLogin Application Definition Guide*.

NOTE: The limitation applies to all applications where the notification dialog box is different from the application used by the Wizard.

Specifying Reauthentication Rules

If you have deployed SecureLogin in the Standalone mode, you cannot specify reauthentication rules. The reauthentication rule does not apply to SecureLogin in the Standalone mode. The Application Definition Wizard does not recognize the mode of deployment.

Incorrect Login Notifications in Mozilla Firefox

The Application Definition Wizard cannot define login notifications such as incorrect password or incorrect login that are displayed through browser popups in Mozilla* Firefox*. The Application Definition Wizard considers the popup windows as URL and tries to add them to the already defined definition for that URL.

Single Sign-On For Microsoft Windows Vista Remote Desktop Client

SecureLogin might not pass the correct domain name while performing a single sign-on operation for the Microsoft Windows Vista Remote Desktop client in either the Novell Client or LDAP mode.

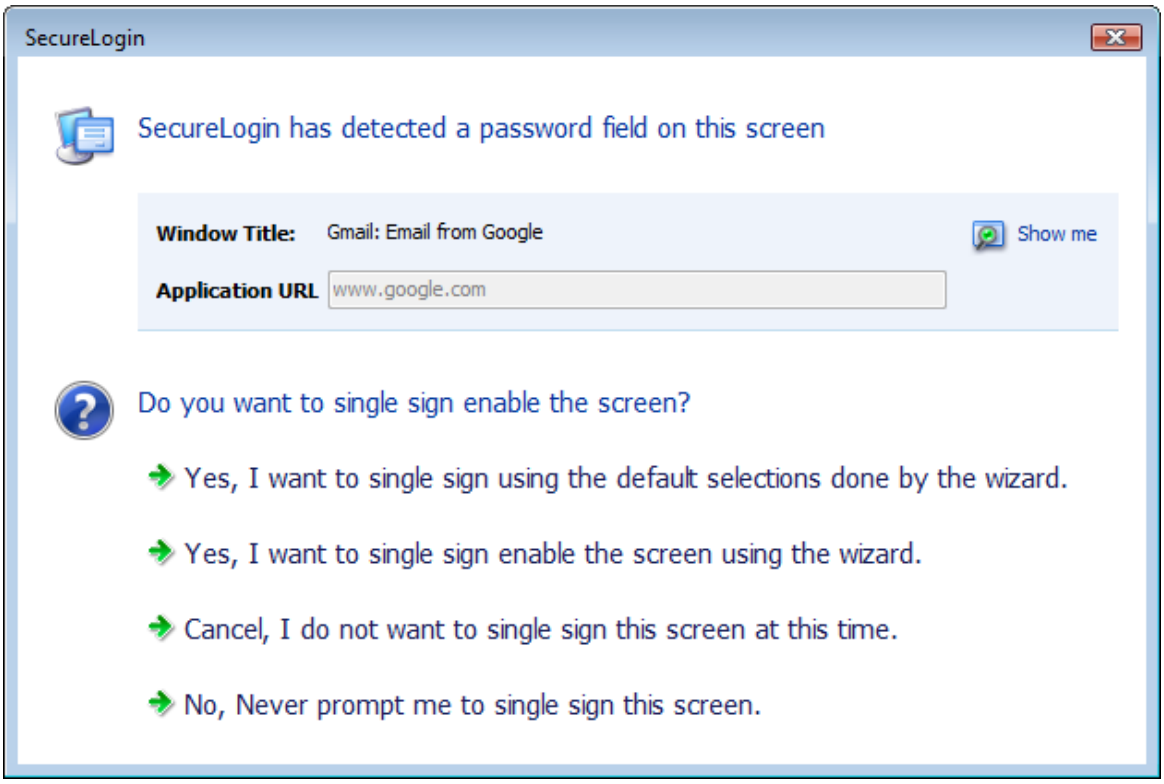
Tips

- "Detecting Multiple Controls" on page 126
- "Using Dynamic Controls" on page 128
- "Citrix Published Applications" on page 128
- "COM Applications" on page 128

Detecting Multiple Controls

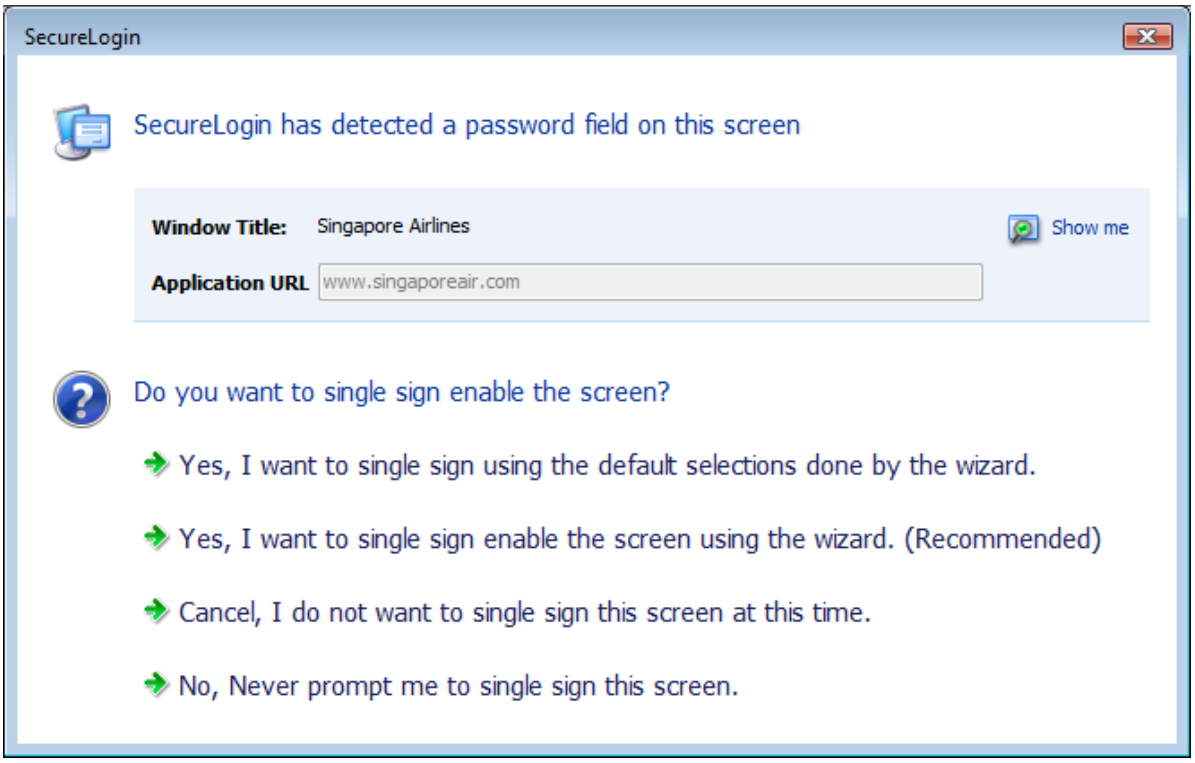
When SecureLogin detects a typical, simple login screen containing a username field, password field, and a submit button, it displays the following prompt:

Figure 8-1 *Prompt to Enable Simple Login Screens*



A complex login screen might offer users a choice to log in to different network, check the status of a flight, and similar multi-actions. When a complex login screen is detected, the following prompt is displayed.

Figure 8-2 *Prompt for Complex Screens*



Select **I want to single sign-on enable the screen using the wizard. (Recommended)** to review and if necessary edit the selection done by the Wizard.

Alternatively, you can define the application using the default selection done by the Wizard and edit the definition, later.

Using Dynamic Controls

You can use the Windows Finder tool to identify whether your application uses dynamic controls. For information on using the Windows Finder tool, see "Finding Application Details with Window Finder" in the *NetIQ SecureLogin Application Definition Guide*.

If an application uses dynamic controls, use the **Navigate to field using keystrokes** option to select and populate the fields. See "Recording Keystrokes" on page 61.

Citrix Published Applications

The Application Definition Wizard does not detect Citrix published applications. Run the applications on a workstation to manually create an application definition by using the Wizard.

COM Applications

The Application Definition Wizard cannot differentiate between a COM application (where Internet Explorer* is the top parent) prompt and a genuine Internet Explorer prompt. To create an application definition for COM applications, extend the default Internet Explorer script or create a new one based on the Internet Explorer model.

Troubleshooting

- “Redirecting to Login Page” on page 129
- “Remote Desktop Connection” on page 131

Redirecting to Login Page

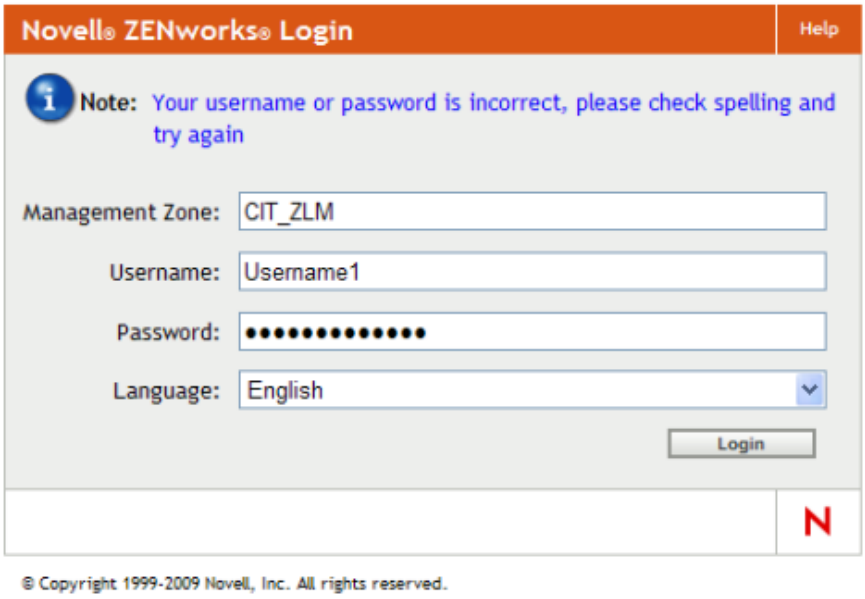
Some Web applications such as Novell iFolder, Quickfinder, ZENworks Configuration Management, and ZENworks Linux Management display the login failure notifications on the same page as the login notifications. When a Login Notification page is detected for such applications, it prompts for correct credentials. However, because the user has already provided the credentials, SecureLogin does not re-enter the new password.

To resubmit the new credentials, redirect users’ to main login page.

In the following example, the user has specified incorrect credentials when logging in to Novell ZENworks Control Center. The user must be redirected to the main login page to specify correct credentials.

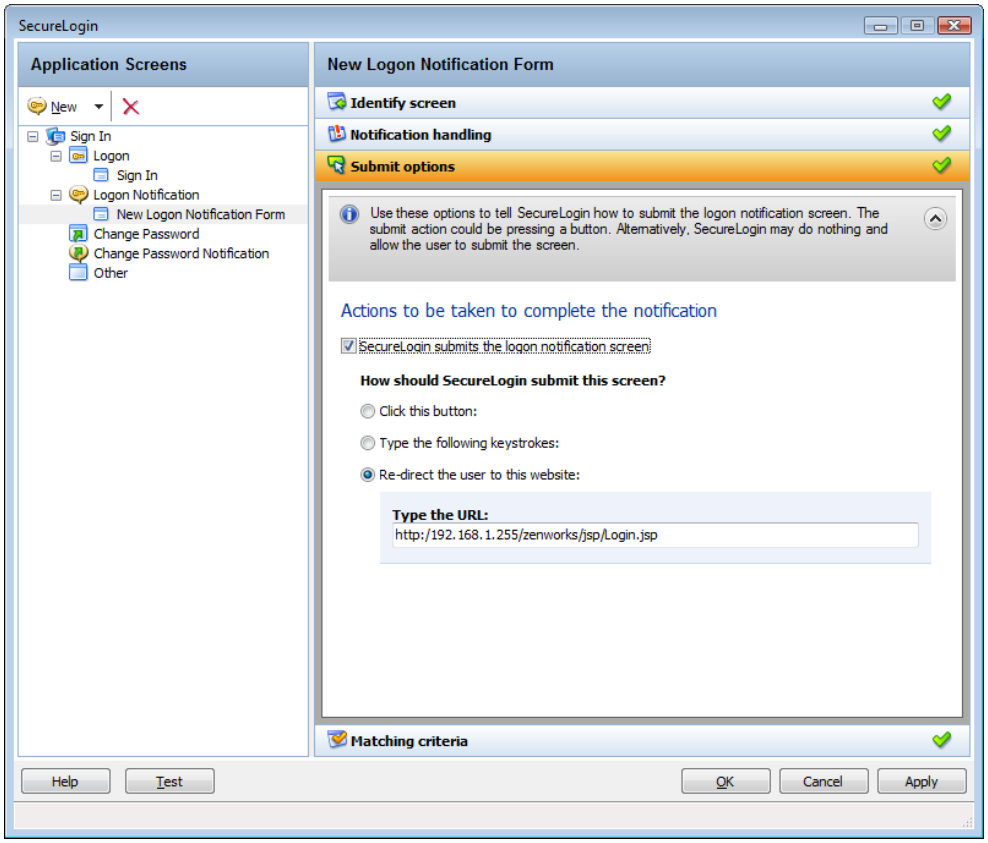
To redirect the user:

Figure 8-3 *Login Failure is Displayed on the Login Page*



1 While creating the login notification, under **Submit options**, select **Re-direct user to this website**.

2 Specify the URL for redirection.



The next time incorrect credentials are submitted, the following events occure.

1. The Login Notification is detected.

2. User is prompted for credentials.
3. User specifies correct credentials.
4. SecureLogin redirects to the login page.
5. SecureLogin submits the credentials and logs in the user successfully.

Remote Desktop Connection

When a Windows application is detected, SecureLogin scans the application to detect if there is a valid script or if it must be enabled for single sign-on.

Similarly, in a remote desktop connection when applications are inactive, SecureLogin scans for Windows applications and prompts you to enable them for single sign-on.

This is an expected behavior.

If you want to enable a remote desktop client, use a prebuilt script. By default, on Microsoft Windows Vista, the prebuilt passes the system credentials, that is, the network credentials are sent to connect to the RDP session. If you want to change the behavior, do one of the following:

- Set `$PassSysVariableOnly` to **No**. You are prompted to enter your system or other credentials.
- Set `$PromptForCredentialChangeOnEachLogin` to **Yes**. You are prompted to select a credential set each time you log in.

NOTE: The remote desktop client application has two different GUIs on Microsoft Windows XP and Microsoft Windows Vista*. This makes it complex if the application definition must run on both platforms. Particularly on Microsoft Windows Vista, the Wizard defines this application using the **Navigate to field using keystrokes** option.
