Oracle© Enterprise Single Sign-on Password Reset

Management Console Guide

Release 11.1.1.2.0

E15713-02

November 2010

ORACLE

Oracle Enterprise Single Sign-on Password ResetManagement Console Guide, Release 11.1.1.2.0

E15713-02

Copyright ©2006-2010, Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Table of Contents

Abbreviations and Terminology 4
ESSO-PR Management Console Overview 5
First-Time Setup 6
Setting up the Web Service Account 7
    Setting or Changing the Anonymous Logon 7
Setting Up the Enrollment Interview 8
    Enrollment Level Setting 8
    National Language Support 8
    Configuring System Questions 9
Configuring Reset Authentication 12
    Score Thresholds 12
Configuring Service Storage 13
Configuring the Reset Service Account 15
Multi-Domain Support 16
    Setting Up Multi-Domain Support 16
Edit Reset Service Settings 18
Password Complexity 20
    Password Constraint Options 20
Alerts 21
Logging 22
Reporting 23
Enrollment User Interface 24
Reset User Interface 26
    Customizing Reset Messages 28
Creating and Editing System Questions 32
Role/Group Support 36
Manage Users 40
View Enrollments 41
Manage Enrollments 42
View Resets 43
Manage Resets 44
External Validators 45
    Writing the External Validator Interface 45
    Installing the External Validator 46
    Directing ESSO-PR to the External Validator 46
    Deleting the External Validator 47

Abbreviations and Terminology

Following is a list of commonly-used abbreviations and terminology.

Abbreviation or Term	Full Name
Administrative Console	ESSO-LM Administrative Console
Agent	v-GO SSO Manager
FTU	First Time Use Wizard
ESSO-AM	Oracle Enterprise Single Sign-on Authentication Manager
ESSO-Anywhere	Oracle Enterprise Single Sign-on Anywhere
ESSO-PG	Oracle Enterprise Single Sign-on Provisioning Gateway
ESSO-KM	Oracle Enterprise Single Sign-on Kiosk Manager
ESSO-LM	Oracle Enterprise Single Sign-on Logon Manager
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset

ESSO-PR Management Console Overview

Oracle Enterprise Single Sign-on Password Reset (ESSO-PR) enables workstation users to reset their own Windows domain passwords without the intervention of administrative or help-desk personnel. It provides end users with an alternative means of authenticating themselves by taking a quiz comprising a series of passphrase questions.

Each question is weighted with point-values. As the end user answers the quiz questions, ESSO-PR keeps a running score. Points are added to the score for each correct response and points are deducted for each incorrect response. When the end user accumulates sufficient points to meet a preset "confidence level," ESSO-PR permits the end user to select a new password. If the end user's score does not achieve the required confidence level after all questions have been presented, or if it falls below a preset negative value, the quiz ends and the end user is not permitted to reset the password.

The reset service is available to each end user after completing a one-time enrollment interview to record passphrase answers. The ESSO-PR Management Console provides easy configuration of the enrollment interview and reset quiz, including question text, and point-values, and confidence-level limits. The console also affords convenient reports of enrollment and reset activity and status.

First-Time Setup

After you have installed the ESSO-PR server application, the first task is to configure the service for use with the directory-server or relational database and Web services. You perform this first-time configuration with the dialog pages in the **System** tab:

- Use the Web Service dialog page to set the Anonymous Logon account - the user account through which ESSO-PR users and administrators access the service.
- Use the Storage dialog page to configure the directory or database to create the ESSO-PR repository for system questions and user data.
- Use the Reset Service dialog page to set the Service account - the user account that ESSO-PR itself "logs on as" to the server.

When you have completed these steps, you can begin configuring the reset service itself. These tasks include:

- Setting up the Enrollment Interview by supplying a set of system questions and associated point values
- Setting the general reset service options. These options include the pass and fail score thresholds, user-lockout parameters, and administrator alerts.

Setting up the Web Service Account

Use the Web Service Account dialog box (under the System tab) to set or change the Anonymous Logon for IIS Web Services. This is the domain account through which all end users access ESSO-PR Web interface.

The Web Service Account dialog box displays the current Anonymous Logon account and provides a logon form for changing this account.

The account selected as the Anonymous Logon should have local administrator privileges, including permission to perform the following tasks:

- Start, stop, and change services
- Read from and write to Active Directory, ADAM-instance, or database server.
- Write to the local-machine registry (HKLM).

To create a new user account with administrator privileges, use the Users and Groups tool in the Windows Computer Management Console.

Setting or Changing the Anonymous Logon

1. Enter the User Name and Password of the account that you want to use.
2. Enter the password again to confirm.
3. Click **Submit**.

Setting Up the Enrollment Interview

When the user starts the enrollment program, ESSO-PR displays the Enrollment Interview.

The Enrollment Interview comprises a series of questions in two groups:

- Required questions
- Optional questions

The required and optional questions are called *system questions*. System questions are predefined and managed by the administrator using the Questions tab of the ESSO-PR Management Console. See Configuring System Questions and Question Examples for more information.

When the end user has answered enough questions to meet the defined enrollment level, the Enrollment Interview ends.

If the user skips any optional questions, they may not meet the enrollment level threshold. If this scenario occurs, ESSO-PR begins the optional question set again, prompting the user to answer any questions they may have skipped.

Enrollment Level Setting

Enrollment Level is a new feature in the 11.1.1.2.0 release The Enrollment Level is set on the Settings page.

This feature allows the administrator to set the total points value that end users must accumulate in order to complete the enrollment interview process. This threshold removes the previous requirement that the administrator had to configure required questions with enough total value in points to meet the Authentication Success Level (Settings -> Authentication thresholds).

ESSO-PR now allows administrators to configure questions with enough points to meet the Enrollment Level by counting both the required and optional questions. The Enrollment Level must be at least equal to or greater than the Authentication Success Level.

With both the Enrollment Level and Authentication Success Level thresholds, users now have the flexibility to select questions they want to answer out of a pool of questions.

During the enrollment interview, starting questions can be optional or required. A progress bar shows the user's progress (in percentage) in satisfying the enrollment level threshold.

If the user reaches the end of the question set without enough points to meet the enrollment level, ESSO-PR displays a message stating that "You have not answered enough optional questions to satisfy the enrollment requirement. In order to complete the enrollment process, you must continue to answer questions until the progress bar reaches 100%." ESSO-PR will then begin the optional question set prompting the user to answer questions they previously skipped.

National Language Support

The initial enrollment dialog can be presented in the preferred language for each business unit as required by National Language Support (NLS). NLS support is required for English, French, Spanish, Italian, German, Brazilian Portuguese, Czech, Dutch, Finnish, Polish, Korean, Simplified Chinese, and Japanese.

The text that is displayed on the initial page of the enrollment dialog box is stored in a XML file called `UserText.xml`. To implement this feature, you must create multiple XML files with the filenames `UserText.<language code>.xml`; for example, `UserText.de.xml`, `UserText.fr-ca.xml`.

The language code follows the RFC 1766 format that is used by .NET. Each XML file contains text in its respective language. The files are stored in the \WebServices folder.

ESSO-PR loads all the files with the above naming pattern and uses the appropriate version to display the 'Welcome' screen of the enrollment page.

On the client side, the Windows interface passes the language the user installed within the URL to tell ESSO-PR to show the enrollment page in that language.

Configuring System Questions

System questions are those prepared by the administrator. See Creating and Editing System Questions for the procedure.

Each system question has the following settings:

- **The text of the question.** The question text should include any special format instructions that will help keep the answer that the end user provides at enrollment identical to the answer he or she will give in the Reset Quiz. The answer given in the Reset Quiz must be a case-sensitive string match (that is, have exactly the same spelling, punctuation, capital-letter use, and white space). For example, if the question is "What is your Social Security number?" note whether or not the response should include dashes between number segments.
- **The language of the question.** The language of the question can be displayed in English (default), Czech, Dutch, Finnish, French, Spanish, Italian, German, Polish, Brazilian Portuguese, Korean, Simplified Chinese, or Japanese.
- **Whether the user is required to answer the question** in order to complete the Enrollment Interview. The user must provide an answer to any required questions. Optional questions are presented at the end of the Interview. Optional questions for which an end user declines to provide an answer will not appear in the Reset Quiz for that user.
- **The source of the answer.** By default, ESSO-PR requires that all the questions and weights used for reset are entered and set up by the administrator and answered by the user upon enrollment. ESSO-PR also works with external validator sources to simplify this process. An external validator can call data from various sources (such as a human resources database) that contain predefined answers. See External Validators for more information.
- **The point-value to be added** to the total score when the question is answered correctly during the Reset Quiz.
- **The point-value to be subtracted** from the total score when the question is answered incorrectly during the Reset Quiz.
- **Constraints on what the end user can enter** as a valid answer; including:
- The minimum length of the answer
- The format of the answer (such as numeric digit and punctuation usage), specified as a regular expression; for example, to require a Social Security number to be entered as digits separated by hyphens, use the expression
  \d{3}-**d{2**}-**d{4}**
  For more information about regular expressions, refer to the reference at http://msdn.microsoft.com/
- Case-sensitivity; that is, whether upper case and lower case characters used in Enrollment Interview answers must exactly match those in Reset Quiz answers..

Assigning Point Values to Questions

Secure implementation of self-service reset depends on the selection and weighting of the individual system questions. Here are some primary considerations for each question:

- **How secret the answer is.** How few people (ideally, none) are likely to know or be able to guess any given user's answer. The more secret the answer, the higher a point-value that can be assigned to the question if answered correctly in the Reset Quiz.
- **How personal the answer is.** How much a wrong answer ensures that the person taking the Reset Quiz is *not* the authorized user; for example, "Are you left-handed, right-handed, or ambidextrous?" Questions that call for personal answers can serve as "eliminators" in the Reset Quiz: few or zero points are awarded for a correct response, and more points deducted for an incorrect response.
- **How memorable and static the answer is.** This ensures that the user will recall the exact answer that he or she provided at enrollment. Questions that involve preferences (such as "what is your favorite ice cream") should have lower point-values for both correct and incorrect answers and are better suited as Optional questions. By comparison, questions that are based on unchanging and easily-recalled facts ("what is the name of the last high school you attended?") can have higher point-values for correct or incorrect responses; they are better candidates for Required questions.
- **The minimum number** of questions that must be answered in order to pass (or explicitly fail) the Reset Quiz. This is derived from the Success/Failure score thresholds and the point values you assign to each question for correct and incorrect responses.

See Question Examples for more information.

Question Examples

The following table provides some examples of system questions, recommended as Required or Optional, with suggested point-values based on the default score thresholds of -100 to 100 points.

Required Questions

These questions are good prospects for Required questions. Note that all of these questions have answers that are facts on record. Oracle strongly recommends that your selection of Required questions have answers that come from as many *different sources* as possible. For example, in some states, a driver's license may display the Social Security number and date of birth.

Question	Required?	Points if Correct	Points if Incorrect
What is your Social Security number (numbers only, no spaces)?	Y	10	-75
What is your date of birth (mmddyy)?	Y	25	-50
In which city were you born?	Y	25	-50
What is your mother's maiden name?	Y	25	-75
What was the name of the first school you attended? (or "...that you remember attending)?"	Y	25	-25
What is the name of the last high school that you attended?	Y	25	-25

Eliminators

These questions are "eliminators" because the authorized end user is very unlikely to answer them incorrectly. The answers are personal, and therefore have low or no point-value for correct answers and high negative point-value if answered incorrectly.

Question	Required?	Points if Correct	Points if Incorrect
What is your eye color?	Y	0	-75
Are you left/right handed, or ambidextrous (l, r, or a)	Y	5	-75
What is your gender (male or female)?	Y	0	-75

Optional Questions

These questions are acceptable as Optional questions only, because they may not apply to all enrollees.

Question	Required?	Points if Correct	Points if Incorrect
What was the name of your first or favorite pet?	N	25	-25
What color was your first car?	N	25	-25
What is your wife's maiden name?	N	25	-25
What is your blood type (O, A+/-, B+/-, AB)?	N	25	-25
How many siblings do you have?	N	25	-25
What is your spouse’s date of birth? (mmddyy)	N	25	-25

Configuring Reset Authentication

When an end user requests a password reset, ESSO-PR displays the Reset Quiz.

The Reset Quiz is a series of questions drawn from the system questions that the end user answered in the Enrollment Interview. The Reset Quiz presents all of the required questions one at a time, in random order, for the end user to enter a response. If there are no required questions set up, the Reset Quiz presents the optional questions only. With each response, the preset point-value for correct answers is added to the total score, or the point-value for incorrect answers is deducted.

After all of the required questions have been presented, the Reset Quiz continues until either: a) all Optional questions have been presented, or b) the end user answers a sufficient number of questions to meet either of two score thresholds:

- If the end user's score equals or exceeds a preset Success score threshold, the New Password dialog box appears. The end user then enters and confirms a new password, and returns to the initial logon dialog box.
- If the end user's score equals or falls below a preset Failure score threshold, the Reset Quiz ends with no password reset, and the end user returns to the initial logon dialog box. ESSO-PR records the quiz session as an explicit failure, indicating that the end-user failed the quiz by incorrectly answering questions.

If the end user answers all of the questions without achieving either score threshold, the Reset Quiz ends with no password reset, and the end user returns to the initial logon dialog box. ESSO-PR records the quiz session as an *implicit* failure indicating that the end-user failed the quiz with an insufficient score to pass or explicitly fail.

The Success and Failure score thresholds are set by the administrator in the Settings tab of the ESSO-PR Management Console. The text and point-values for individual system questions are set in the System Questions tab.

Score Thresholds

The score thresholds are the point-values that determine whether the end user passes or fails the Reset Quiz.

- The Success value determines the score (the point-value total achieved for the quiz) that end users must achieve in order to reset their passwords.
- The Failure value determines the minimum (that is, a negative) score that end users can accrue by answering Reset Quiz questions incorrectly. If the end user's score falls below this setting, the Reset Quiz ends without a password reset.

See Reset Service Settings for more information.

Configuring Service Storage

Use the Storage dialog box (under the System tab) to view or change connection settings for the database (SQL Server or Oracle Database) or directory service (Active Directory or ADAM) that is used as the repository for ESSO-PR system questions and user enrollments. To do this, use the settings in the System Configuration group. When you have completed your changes, click **Submit** to apply your new settings to ESSO-PR.

You also use the Storage dialog box to have ESSO-PR perform the first-time setup tasks that prepare the database or directory-server repository for use with the enrollment and reset services. These tasks include:

- Extending the schema to include directory types/database tables
- Creating the main container or database
- Granting read/write access to the Web service account
- Creating required child objects or tables.

To perform these tasks, use the controls in the Storage Configuration group:

1. Select **Initialize Storage for ESSO-PR**.
2. For **Connect As**, enter the user name of an administrator of the directory server.
3. Enter the administrator password.
4. Click **Submit** to save any changes or modifications. Your changes will be lost if you don't click the **Submit** button before closing the Storage page.

Storage Configuration	
Storage Type	The type of service used: SQL Server, Oracle Database, Active Directory, or ADAM.
Provide these four settings for Active Directory or ADAM storage only:	
Server Name /IP Address, Port Number	Enter either the name of the server or the IP address of the server in the first text box. In the second text box, enter the numerical port number used by the directory service. Click **Add** to add the connection to the Servers list. Multiple servers can be added for failover support. If more than one server address is entered, ESSO-PR iterates through the list in sequential order until either it has successfully connected or all connections have failed.
Servers	ESSO-PR attempts connections in the order that they appear in the list from top to bottom. Use the up and down arrows to arrange the servers in the order in which connections should be attempted. To delete a server from the list, select the server in the list box and click **Delete**. Note that you cannot delete a connection if it is the only connection present in the list. In some cases, such as long server names, the entire string is not displayed in the list box. Clicking on an item in the list box populates the Server Name/IP Address and Port text boxes with that item. The full string can then be viewed by scrolling in the text box and, if desired, modified and added as a new connection to the list.
Server Timeout	Enter a duration value (in seconds) that ESSO-PR should wait for a response from a server before moving on to the next server in the list.
Storage Location	The distinguished name or naming context of the connection node.
Use SSL	Select to enable secure socket layer.
Provide these settings for SQL Server or Oracle Database storage only:	
Connection String	The complete connection string to the database server; for example:

Storage Configuration	
	`Provider=SQLOLEDB.1;Integrated Security=SSPI;Initial Catalog=SSPR;Data Source=Servername; Trusted_Connection=Yes` Click **Add** to add the connection to the Database Connections list. Multiple connections can be added for failover support. If more than one connection is entered, ESSO-PR iterates through the list in sequential order until either it has successfully connected or all connections have failed.
Database Connections	ESSO-PR attempts connections in the order they appear in the list from top to bottom. Use the up and down arrows to arrange the connection strings in the order in which connections should be attempted. To delete a connection string from the list, select the string in the list box and click **Delete**. Note that you cannot delete a connection string if it is the only connection present in the list. In some cases, such as long database connection strings, the entire string is not displayed in the list box. Clicking on an item in the list box populates the Connection String text box with that item. The full string can then be viewed by scrolling in the text box and, if desired, modified and added as a new connection to the list.
Database Timeout	Enter a duration value (in seconds) that ESSO-PR should wait for a response from a database before moving on to the next database in the list. This value is not used in database connections if the connection string contains a Connect Timeout parameter.

Storage Initialization	
Initialize Storage	Activates the first-time configuration tasks. If this option is checked, ESSO-PR automatically iterates through the new connections in the list and attempts to initialize them sequentially. If a connection fails to initialize, initialization stops and connections further down in the list will not be initialized. If this occurs, resolve the issue and then retry initialization.
Connect As (User Name)	The user name of a directory or database administrator.
Password	The password of the administrator.

Configuring the Reset Service Account

Use the Reset Service dialog box(in the System tab) only to specify the credentials (username and password) of the user account that the ESSO-PR reset service uses to log on. The service account must have password-change privileges for the domain.

> Because the default user account for services (typically LocalSystem) does not have password-change privileges, you must create a user account (in the Windows Domain Manager) before specifying the credentials in this dialog.
>
> The service account you specify in this dialog box appears in the Log On As column of the Computer Management Services tool.

The Reset Service dialog box also displays the current status of ESSO-PR (Running or Not Running), and the port that the service uses to detect a password reset attempt.

Change Service Account	
User Name	The user name of the Reset Service Account.
Password and Confirm Password	The password of the Reset Service Account. Type the password in both fields.

Service Options	
Listening Port	The number of the port used to detect password reset activity (default is 45000).
Domain	The trusted domain where user accounts are located. This setting is required only if the user accounts are in a domain other than that of the ESSO-PR machine's domain. Changes to this setting take effect immediately and do not require a restart of the IIS or Password Reset Service.

Multi-Domain Support

You can configure ESSO-PR to reset Windows passwords and unlock Windows accounts in its own domain or any domain you designate as trusted.

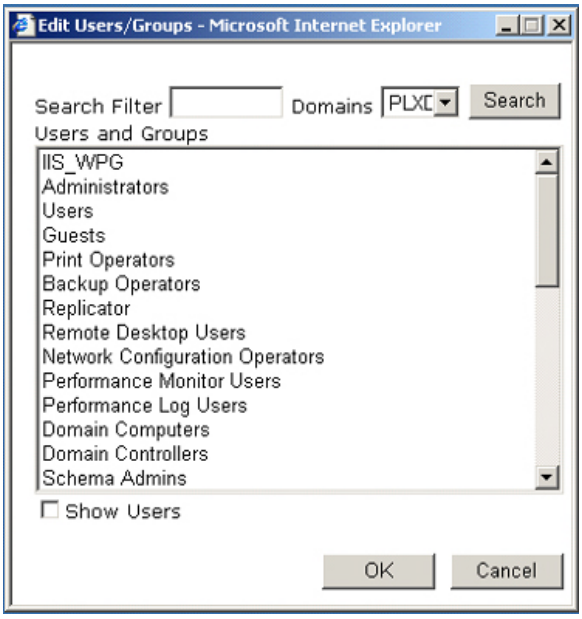
Multi-domain support requires the following conditions:

- There must be valid two-way trusts between the ESSO-PR domain and other domains.
- The ESSO-PR reset service user account must be a member of the local administrators group of the trusted domain.
- All the domains must share the same settings as the ESSO-PR server, such as password complexity, alerts, questions, and so forth.

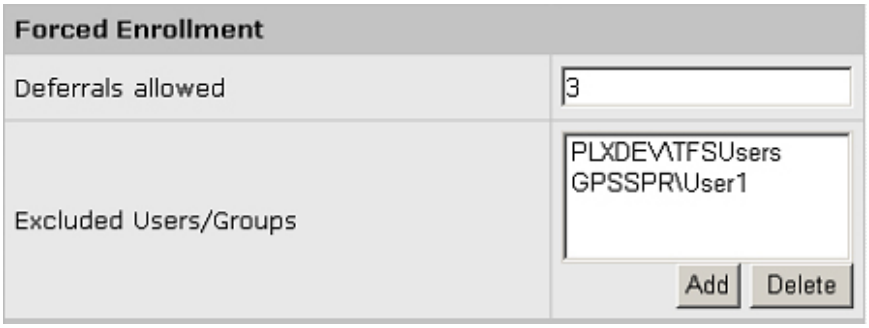
Setting Up Multi-Domain Support

In the Management Console, select the domain you want to designate as trusted from any of the following screens:

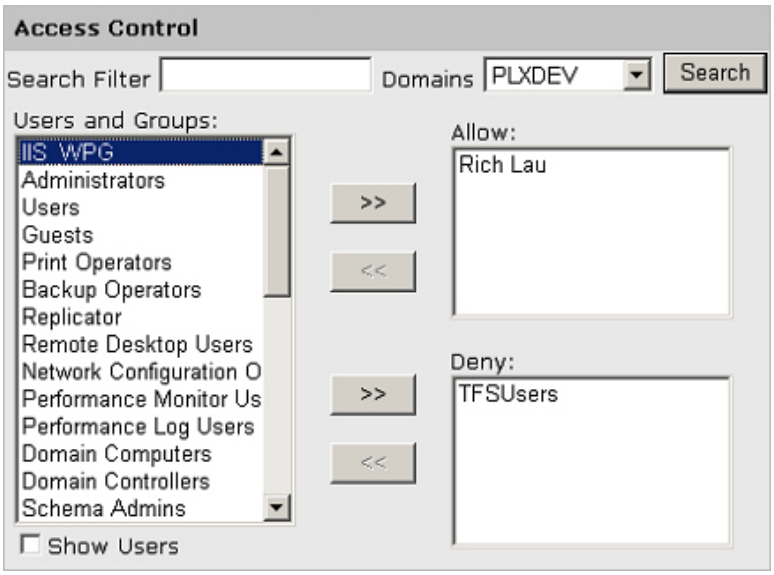
- The drop-down menu in the Edit Users/Groups dialog box



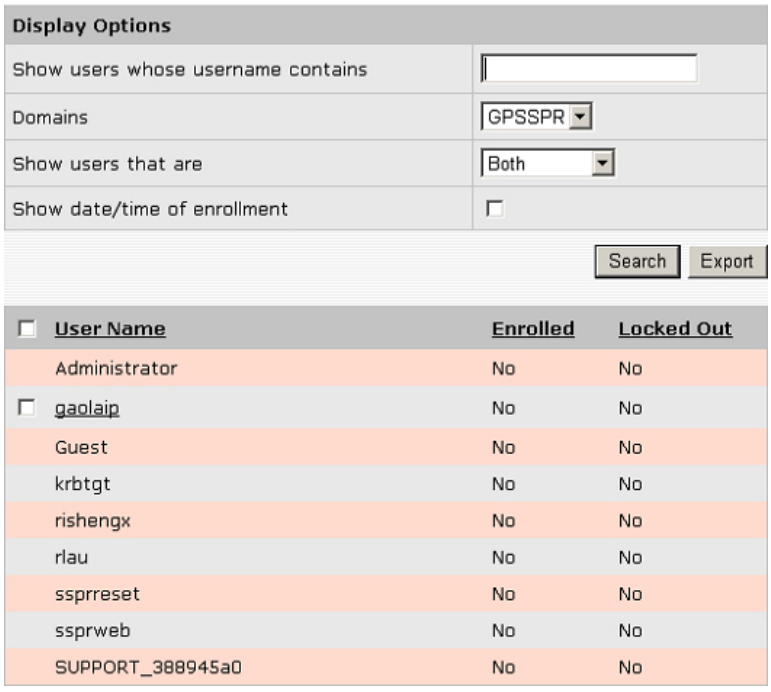
- The Forced Enrollment dialog box in the Settings tab



- The Questions Tab, when you edit existing questions or create a new one



- The Users tab.



When you make a domain selection on any one of these screens, that change is reflected in all the other screens. The domain that you select is saved in the registry value, HKLM\SOFTWARE\Passlogix\SSPR\SSPRService\DisplayDomain.

When performing queries again a trusted domain, you may receive the error message: "The server is not operational." This can occur if the guest account on the trusted domain is turned on, because that account does not have the rights to enumerate users

To eliminate this error, do one of the following:

- Turn off the guest account in the trusted domain.
- Create the same trusted domain user account in the trusted domain.

Edit Reset Service Settings

Use the Settings dialog (under the **Settings** tab) to modify general settings for the Reset Quiz. When you have completed your changes, click **Submit** to apply your new settings to ESSO-PR.

Also see Configuring Reset Authentication for more information.

Authentication Thresholds	
Authentication Success Level	The score (the point-value total achieved for the quiz) that end users must achieve in order to reset their passwords. The default value is 100.
Authentication Failure Level	The minimum (negative) score that end users can accrue. If the end user's score falls below this setting, the Reset Quiz ends without a password reset. The default value is −100.
Enrollment Level	The score (the point-value total achieved for the enrollment interview) that end users must achieve in order to complete the enrollment interview. The default value is 100. The **Enrollment Level** must be at least equal to or greater than the **Authentication Success Level**.

Reset Lockout	
Lockout Thresholds	The number of consecutive unsuccessful reset attempts permitted. If an end user fails the Reset Quiz this number of times in a row, no further Reset Quiz attempts are permitted for the Lockout Duration interval.
Lockout Duration	The time period, in hours, that an end user is not permitted to take the Reset Quiz. The Lockout Duration begins when the end user consecutively fails the Reset Quiz the number of times given for Lockout Thresholds. To override lockout for individual end users, click the **Users** tab, select the end user from the list, then click **Unlock**.

Forced Enrollments	
Deferrals allowed	The maximum number of times a user can defer ESSO-PR enrollment. When the user exceeds the maximum number of deferrals, he must complete the enrollment process in order to be allowed to log on.
Excluded Users/Groups	Users or groups that you want to exclude from forced enrollment. Click the **Add** button to display the Edit Users/Groups window. Enter a search filter term and select a domain from the dropdown menu, then click **Search**. From the resulting search, select the user or group that you want to exclude, and click **OK.** If you add a group to the exclusion list, this exclusion group cannot be the user's primary group. You must create a new group, add the user to that group (maintaining the user's original primary group), and exclude the new group in the ESSO-PR Forced Enrollment Exclusion list. If you add a group to the exclusion list, this exclusion group cannot be the user's primary group. You must create a new group, add the user to that group (maintaining the user's original primary group), and exclude the new group in the ESSO-PR Forced Enrollment Exclusion list.

User E-mails	
Required during enrollment	Controls whether or not users are required to enter an e-mail address during the enrollment process.
Email format (regular expression)	Controls the valid format of the user e-mail address. The default setting allows for most acceptable email formats.

Reset Experience	
Show 'Unlock account option' only	Controls whether or not a user is given the option to unlock his or her account rather than reset the password. This option is presented after a user passes the Reset Quiz.
Enable "Display temporary password" mode	Controls whether or not ESSO-PR should allow the end user to reset the password regardless of the Active Directory password policy. With this checkbox enabled, ESSO-PR overrides any AD restrictions that are in place and provides the user with a temporary password. The user can then log on with that temporary password and change it through Windows.

Password Complexity

Use the Password Complexity dialog box (under the **Settings** tab) only to adjust the password constraints to make certain that they match or are within the constraints of the Group Policy of the Windows domain. This setting does not apply to end- user passwords (see Note, below). In typical usage (that is for typical group policies), these settings need not be changed.

When you have completed your changes, click **Submit** to apply your new settings to ESSO-PR.

In order for ESSO-PR to reset end-user passwords, the Reset Service account performs an intermediate password reset as a proxy for the user. The Reset Service account generates a password internally that must conform to the domain's group policy, but is not subject to the domain's minimum password age policy. The password complexity settings in this dialog box apply only to that intermediate password, not to end-user passwords.

Password Constraint Options

Constraints	
Minimum Length	Minimum internal password length: 1-63 (default: 16)
Maximum Length	Maximum internal password length: 1-63 (default: 16)
Number of times characters can repeat	0-62, default: 7

Alphabetic Characters	
Allow Uppercase characters	Select to allow uppercase characters (default: allowed)
Allow lowercase characters	Select to allow lowercase characters (default: allowed)

Numeric Characters	
Allow Numeric Characters	Select to allow numeric characters (0-9), (default: allowed)
Minimum Occurrences	1-63, default: 1
Maximum Occurrences	1-63, default: 1

Special Characters	
Allow Special Characters	Select to allow special characters (non-alphabetical, non-numeric) (default: not allowed)
Minimum Occurrences	1-63, default: 1
Maximum Occurrences	1-63, default: 1
Special Characters List	Characters that may be used (default: !@#$%^&*()_-=+[]|.?)

Alerts

Use the Alerts dialog box (under the **Settings** tab) to configure ESSO-PR to notify an administrator by e-mail when an end user is "locked out," that is, prevented from taking the Reset Quiz because of one or more failures to pass the quiz.

All of the fields in this dialog box must be completed in order to activate the e-mail alert.

To test your settings, click **Send Test Email**. When you have completed your changes, click **Submit** to apply your new settings to ESSO-PR.

E-mail Settings	
Enable e-mail alerts	Select to activate e-mail alerts
"From" e-mail address	The e-mail address that originates the alert. This can be any valid email address for the SMTP mail server specified below.
Admin e-mail address	The e-mail address of the administrator to whom the alerts will be sent.
Admin name (displayed in emails)	The name of the administrator to whom alerts will be sent. This name will be displayed in the e-mails.
SMTP mail server	The name of the outbound mail server.

Send Alert When User:	
Fails a reset attempt	Select who should receive e-mail alerts if a user fails a reset attempt, Admin, the User, or both. This field is only active if **Enable e-mail alerts** is selected. Also see Reset Service Settings for the lockout controls.
Successfully resets password	Select who should receive e-mail alerts if a user successfully resets his password, the Admin, the User, or both. This field is only active if **Enable e-mail alerts** is selected.

Logging

Use the Logging dialog box (under the Settings tab) to configure ESSO-PR to enable logging, to specify the syslog server and port, and to select the types of events that should generate syslog messages. This logging feature allows ESSO-PR to generate syslog messages so that administrators can receive notifications of user enrollment and reset events. ESSO-PR generates the syslog messages that are received by a syslog listener. This enables the administrator to see the activities of ESSO-PR users.

Enter the following information and click **Submit** to apply your new settings to ESSO-PR.

SysLog Settings	
Enable	If checked, syslog logging will be enabled.
Server Name/IP Address	The name or IP address of the syslog server.
Server Port	The port where the syslog server is listening for Syslog messages (default port is 514).

Event Filter	
Start	Check to have ESSO-PR send a message when the user begins an enrollment or reset session.
Cancel	Check to have ESSO-PR send a message when the user cancels an enrollment or reset session.
Success	Check to have ESSO-PR send a message when the user successfully completes an enrollment or reset session.
Fail	Check to have ESSO-PR send a message when the user fails the reset session.
Locked Out	Check to have ESSO-PR send a message when the user gets locked out of the ESSO-PR system (by failing too many reset quizzes).

Reporting

The Reporting tool allows you to generate reports on user activities. Refer to the Oracle Enterprise Single Sign-on Suite Plus Reporting documentation for complete information on using this tool.

Use the settings on this page to configure the Reporting tool and database. Click **Submit** to apply your new settings.

Reporting Tool Settings

Enable	Check this box to enable Reporting.
Retry Interval	Defines timeout in minutes between sequential operations of the Reporting Service Cache offloading events to the database. Default is 30. An interval is necessary to reduce database connection load.
Batch Size	Defines the group size of events to be sent to the database Stored Procedure at one time. Default is 100. For example, if you have 1000 events in the Reporting Service cache and the Batch Size = 100, you will have 10 database Stored Procedure calls.
Cache Limit	Number of reporting events to be cached. Once this number is reached, the oldest events are discarded. Default is 4,294,967,295. For example, if the batch size is 100, and an end users system cannot connect to the reporting service, it will keep logging events. Once it gets to 4,294,967,295, the oldest events will be discarded.

Reporting Database Settings

Connection String	Database connection string in the OLE DB format: • "Provider=sqloledb; Data Source=myServerName; Initial Catalog=myDatabaseName; User Id=myUsername; Password=myPassword" or • Provider=SQLOLEDB.1;Integrated Security=SSPI;Persist Security Info=False;Initial Catalog=<Database>;Data Source=<DBServer>
Stored Procedure	The name of the stored procedure in the database. When encoded events are sent to the database, the stored procedure is called to decode the XML file and store the events in the database.

Enrollment User Interface

Use the Enrollment UI dialog box (under the Settings tab) to customize the Enrollment Interview User Interface.

You can edit the look and feel of all ESSO-PR Client pages (the Enrollment and Reset interviews, not the Management Console). This page allows you to adjust colors, fonts, and logos on the Enrollment user interface.

Logo	
Image	Select the logo image to appear in the top left area of the Enrollment UI. Click the **...** button to launch the Edit Property dialog box. Highlight the desired image and click **OK**. For images to appear in this dialog box, they must exist in the `%SSPR%\Images` folder. There is no size requirement for this image. For reference, the Oracle enrollment logo is 146x47.

Status Panel	
Text Color	Select the text color to be displayed for the text in the status panel. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Background	Select either a background image or solid color for the status panel. Click the **...** button to launch the Edit Property dialog box. Select the desired Property Type: Image or Solid Color. If Image is selected, highlight the desired image. For images to appear in this dialog, they must exist in the "%SSPR%\Images" folder. If Solid Color is selected, enter the appropriate RGB color values or color #. Click **OK**. There is no size requirement for this image. For reference, the Oracle status panel background image is 408x28.

Buttons	
Normal Color	Select the normal color for buttons in the Enrollment UI. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Hover Color	Select the hover color for buttons. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Text Color	Select the text color for buttons. Click the **...** button to launch the Edit Property dialog. Enter the appropriate RGB color values or color # and click **OK**.

Top Panel	
Text Color	Select the text color to be displayed for the text in the top panel of the Enrollment UI. Click the ... button to launch the Edit Property dialog. Enter the appropriate RGB color values or color # and click OK.
Background	Select either a background image or solid color for the top panel. Click the ... button to launch the Edit Property dialog. Select the desired Property Type: Image or Solid Color. If Image is selected, highlight the desired image. For images to appear in this dialog, they must exist in the "%SSPR%\Images" folder. If Solid Color is selected, enter the appropriate RGB color values or color #. Click **OK**. There is no size requirement for this image. For reference, the Passlogix top panel background image is 408x47.

Page	
Background	Select either a background image or solid color for the page background. Click the **...** button to launch the Edit Property dialog box. Select the desired Property Type: Image or Solid Color. If Image is selected, highlight the desired image. For images to appear in this dialog, they must exist in the "%SSPR%\Images" folder. If Solid Color is selected, enter the appropriate RGB color values or color #. Click **OK**. There is no size requirement for this image.
Border Color	Select the border color for the page. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Text Font	Select the font to be used for the Enrollment UI. Click the **...** button to launch the Edit Property dialog box. Highlight the desired font and click **OK**. The font list is generated from fonts installed on the SSPR Server. To add a font to the list, install it on the server.

Main Panel	
Text Color	Select the text color to be displayed for the text in the main panel of the Enrollment UI. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Background	Select either a background image or solid color for the main panel. Click the **...** button to launch the Edit Property dialog box. Select the desired Property Type: Image or Solid Color. If Image is selected, highlight the desired image. For images to appear in this dialog, they must exist in the "%SSPR%\Images" folder. If Solid Color is selected, enter the appropriate RGB color values or color #. Click **OK**. There is no size requirement for this image. For reference, the Oracle main panel background image is 408x273.

Side Panel	
Normal Text Color	Select the text color for the normal text in the side panel of the Enrollment UI. Click the … button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Current Step Text Color	Select the text color for the current step text in the side panel of the Enrollment UI. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Background	Select either a background image or solid color for the side panel. Click the **...** button to launch the Edit Property dialog box. Select the desired Property Type: Image or Solid Color. If Image is selected, highlight the desired image. For images to appear in this dialog, they must exist in the "%SSPR%\Images" folder. If Solid Color is selected, enter the appropriate RGB color values or color #. Click **OK**. There is no size requirement for this image.

Reset User Interface

Use the Reset UI dialog box (under the Settings tab) to customize the Reset User Interface.

You can edit the look and feel of all ESSO-PR Client pages (the Enrollment and Reset interviews, not the Management Console). This page allows you to adjust colors, fonts, and logos on the Reset User Interface.

Changing the Reset User Interface Through the Registry

Some user interface settings are configurable through registry settings only. For instance:

- The Reset User Interface, by default, has fields pre-populated with the username and domain of the last Windows account to log on to the workstation. You can set the message above these fields to display a prompt that reads, "To reset your network password, please type in your user name, choose the domain, and click OK to continue."

  See the *ESSO-PRServer Installation and Setup Guide* for more information on the registry settings for the above option.

- The title bar for the enrollment and reset windows, by default, reads, "Oracle Enterprise Single Sign-on Password Reset." You can change this window title to suit your company's needs.

  The password reset link message, by default, reads, "Forgot your password? Click here to reset it." You can change the message in this link (registry settings for this configuration differ between Windows XP and Windows Vista).

  See the *ESSO-PR Client Installation and Setup Guide* for more information on the registry settings for the above options.

Error messages can be customized. See the Customized Error Messages section for more information.

Window	
Border Color	Select the border color for the reset window. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Background	Select either a background image or solid color for the reset window. Click the **...** button to launch the Edit Property dialog box. Select the desired Property Type: Image or Solid Color. If Image is selected, highlight the desired image. For images to appear in this dialog, they must exist in the "%SSPR%\Images" folder. If Solid Color is selected, enter the appropriate RGB color values or color #. Click **OK**. There is no size requirement for this image. For reference, the Oracle reset window background image is 450x350.
Normal Text Color	Select the text color for the normal text in the reset window. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Error Color	Select the text color for error messages that appear during the reset process. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Version Info Color	Select the text color for version information shown on the reset window. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.

Buttons	
Normal Color	Select the normal color for buttons in the reset window. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Hover Color	Select the hover color for buttons. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.
Text Color	Select the text color for buttons. Click the **...** button to launch the Edit Property dialog box. Enter the appropriate RGB color values or color # and click **OK**.

Logo	
Image	Select the logo image to appear in the reset window. Click the **...** button to launch the Edit Property dialog box. Highlight the desired image and click **OK**. For images to appear in this dialog, they must exist in the `%SSPR%\Images` folder. There is no size requirement for this image. For reference, the Oracle reset logo is 106x29.

Page	
Background	Select either a background image or solid color for the page background. Click the **...** button to launch the Edit Property dialog box. Select the desired Property Type: Image or Solid Color. If Image is selected, highlight the desired image. For images to appear in this dialog, they must exist in the `%SSPR%\Images` folder. If Solid Color is selected, enter the appropriate RGB color values or color #. Click **OK**. There is no size requirement for this image.
Text Font	Select the font to be used for the Reset UI. Click the **...** button to launch the Edit Property dialog box. Highlight the desired font and click **OK**. The font list is generated from fonts installed on the ESSO-PR server. To add a font to the list, install it on the server.

Customizing Reset Messages

When the user attempts to change a password and cannot, due to either an account or password policy restriction that you have set, the user receives an error message explaining why the attempt was unsuccessful. The Administrator has the ability to customize the most common of these error messages through the Management Console to help the user to correct the error.

Following are the customizable error messages and the instances that would prompt their display:

Message	Message Code	Description
Password has been successfully reset.	Text_ ResetSuccess	The password reset attempt was successful.
Your account has been successfully unlocked.	Text_ UnlockSuccess	The attempt to unlock the account was succesful.
Your temporary password is "{0}".	Text_ TempPassword	Provides the user with a temporary password after completion of the reset quiz. Be certain to include the **{0}** syntax in this message. ESSO-PR replaces this string with the temporary password .
** Thank you for using $PRODUCT. ** ** You may not be able to log on immediately because it takes time for account updates to propagate throughout the network. **	Text_Success	Informational message that follows each of the succcess messages above. ESSO-PR replaces the **$PRODUCT** string with the product name.
Access Denied	Error_ AccessDenied	There is a configuration error that the Administrator needs to rectify in order for the user to continue.
Bad Password	Error_ BadPassword	The user entered a password that does not fulfill the password policy requirements.
Click here to reset the enrollment session.	Text_ResetSession	This text instructs the user to click to be directed to a URL that links to the reset session.
Session is invalid.	Error_ SessionInvalid	The user has exceeded the permissible interval of inactivity while taking the reset quiz.
The answers provided failed to satisfy the requirements necessary to continue with the reset.	Error_FailQuiz	The user provided enough incorrect answers to reach the failure threshold.
The reset service is currently not available. Please contact your administrator for more information.	Error_ ServiceNotRunning	The SSPRChangePasswordSvc service is not running on the ESSO-PR server.
Error retrieving user data. Please make sure the specified user is enrolled.	Error_ UnknownUser	The user who is attempting to log on has not enrolled in ESSO-PR.

Message	Message Code	Description
User Cannot Change	Error_ UserCannotChange	The user is attempting to change a password in a time frame or manner contrary to the policy that the Administrator has defined.
User Not Found	Error_ UserNotFound	The user's account has been deleted from Active Directory between the time of enrollment and the current attempt to access the account.
Your account has been locked out.	Error_LockedOut	The user has exceeded the permissible number of failures taking the reset quiz and has been locked out of ESSO-PR. The user must wait until the Administrator unlocks the account or the lockout interval elapses.

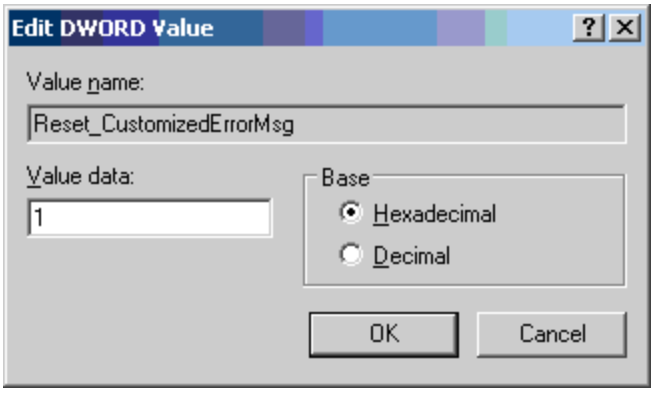
You add this setting to the Server registry. See the Registry Settings section of the *ESSO-PR Server Installation and Setup Guide* for more information.

Example

In the following example, you will change the 'Bad Password' error message. If the user enters a password that does not comply with the password policy, the user receives the following standard error message:

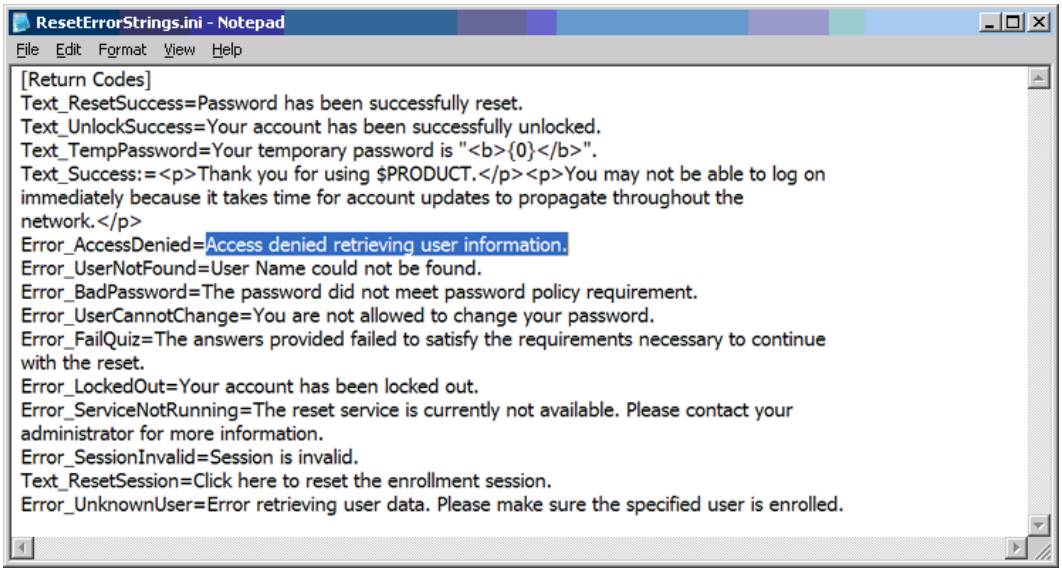
Perhaps you want to inform the user how to select a policy-compliant password, and so you want to add more information to this message. To change this message:

1. From the Start menu, select **Run...**
2. Open the registry by entering `regedit`.
3. Select the registry key: `HKLM > SOFTWARE > Passlogix > SSPR > SSPRService`.
4. Create a new DWORD value by right-clicking the SSPRService folder and clicking **New** > **DWORD value**.
5. Name the registry setting `Reset_CustomizedErrorMsg` and assign a value of **1** to activate it. This setting specifies the directory from which the Server retrieves the error message: `C:\Program Files|Passlogix\v-GO SSPR\ResetClient\App_Customizedresources`.



6. Select the .ini file that you want to edit and open it in a text editor.

The Server retrieves the error message in the language that the user selected during enrollment. If the user selected English, the Server uses the `ResetErrorStrings.ini` file. Otherwise it uses the corresponding language's .ini file. The messages available for editing are contained in this .ini file.



7. Open the .ini file in Notepad or another text editor.
8. Change the message to read as you want it to display to the end user.

> Be certain to enter the message as one continuous line. If you want to display the message to the end user as separate paragraphs, use the `<br>` tag.

9. Save your changes and close the file. The next time a user enters an unacceptable password, he will see your edited message.

Creating and Editing System Questions

Use the following settings to create, edit, and configure system questions.

Creating a New System Question

1. In the Questions tab, select the **Language** in which to enter the question.
2. Click **New Question**.
3. In the question-setting dialog box, enter the **Question Text**. Note that the Question Text is the only setting that can be modified when this question is created.
4. For **Correct Response Weight**, enter the number of points to add for a correct answer.
5. For **Wrong Response Weight**, enter a negative number, the points to subtract for an incorrect answer.
6. Do one of the following:
   - Select **Required** to require end user to provide an answer at enrollment.
   - Clear **Required** to make this question an optional question that end users may skip.
7. Do one of the following:
   - Select **Enabled** to include this question in the Enrollment Interview and Reset Quiz.
   - Clear **Enabled** to remove this question from the Enrollment Interview. Only end users who have answered this question in their most recent enrollment are asked this question in the Reset Quiz.
8. Select an **Answer Source**.
9. For **Minimum Answer Length**, enter the minimum number of characters allowed for a valid answer.
10. (optional) For Answer Format, enter a format (as a regular expression) that will control the valid format of the answer.
11. Do one of the following:
    - Select **Case-sensitive** to require that Reset Quiz answers match enrollment upper case and lower case usage.
    - Clear **Case-sensitive** to allow Reset quiz answers to match enrollment without regard to upper- or lower-case usage.
12. Select the **Users and Groups** to allow or deny access to the question.
13. Do one of the following:
    - Click **Create** to save your changes and return to the Questions tab.
    - Click **Cancel** to abandon your changes and return to the Questions tab.

Modifying or Disabling a System Question

1. In the Questions tab, select the **Language** in which to modify the question.
2. Click a question.
3. In the question settings dialog box, do any or all of the following:
   - Edit the text and then click **Modify**.
   - Edit the weights and then click **Modify**.

> If you change the Correct Response Weight or Wrong Response Weight, a Response Weights Changed dialog box appears. See Changing Question Weights below.

- Clear **Enable** to remove the question from the Enrollment Interview.

> After you create a question, you cannot change whether to require it or the answer constraints settings.

- Select or deselect the **Users and Groups** that you want to assign this question to.

> You cannot assign questions to users or groups when using a database (such as Microsoft SQL Server or Oracle Database) for your repository. The settings are available for editing, but the assignments will not be written to the database.

4. Click **Modify** to save your changes, or click **Cancel** to abandon your changes, and return to the Questions tab.

Changing Question Weights

The weight of a question may be modified if it is determined to be more or less effective in the reset test. A possible ramification of modifying a correct response weight after a question has been created is that enrolled users might not be able to pass the reset test due to an insufficient score, even if they answer all the questions correctly. To avoid such an occurrence, if a correct response weight is changed, a dialog box appears, presenting the option to:

- **Modify this question:** When this option is selected, the change will be made to this question. Note that users who answered this question during enrollment may not be able to reset their password if the correct response weight is set too low.

  or

- **Disable this question and create a new question:** Disables this question and creates a new question with the changes. The benefit is that currently enrolled users will not be affected by the changes. Note that disabled questions are shown as "disabled" (dimmed) in the System Questions list.

System Question Settings

See Question Examples for suggested text and settings for system questions.

Question Properties	
Question Text	The text of the question as it is displayed to the end user. Include formatting instructions or examples. For instance, if asking for a telephone number, provide an example, such as "(333) 555-1234" to insure consistency between the Enrollment Interview and the Reset Quiz.
<Language> Text	Enter the translated question text into this field.
Correct Response Weight	Specify the number of points to add to the end user's score if the question is answered correctly. If modifying this field, see Changing Question Weights above.
Wrong Response Weight	Specify a negative number to indicate the number of points to deduct from the end user's score if the question is answered incorrectly. If modifying this field, see Changing Question Weights above.
Required	**If checked:**This is a Required question. The end user must provide an answer to the question in order to complete enrollment. A Required question is always used in the Reset Quiz. **If unchecked:**This is an Optional question. The end user can skip this question in the Enrollment Interview, in which case the question will not be used in this end user's Reset Quiz. If the end user supplies an answer to an Optional question, the question is used in the Reset Quiz only after all Required questions have been asked.
Enabled	**If checked:** This question is used in the Enrollment Interview and in the Reset Quiz. **If unchecked:** This question is not used in the Enrollment Interview. It is used in a Reset Quiz only if :1) it has previously been enabled and 2) if the end user has answered the question in an Enrollment Interview.

Answer Constraints	
Answer Source	Specify the source from which the answer to this question should come. The default, User supplied, should be selected if the end user will supply the correct answer in the Enrollment Interview. An external validator source can also be used.
Minimum Answer Length	Specify the minimum number of characters the end user must type as an answer.
Answer Format	Specify the format and punctuation for the answer using a regular expression. For example, you can specify the date format "12/1/1983" with the expression \d*\d/*\d\d/\d{4} (allowing the entry of single or double-digit month and day and requiring a four-digit year). If you want to require the end user to type a Social Security number with dashes, use the expression \d{3}-\d{2}-\d{4}
Case Sensitive	**If checked:** The end user's answer is checked for consistent use of upper- and lower-case characters. **If unchecked:** The end user's answer is not checked for consistent use of upper- and lower-case characters.

Access Control	
Users and Groups	Displays a list of the users and groups in the domain. Use the filter and Search button to narrow the scope of the list. The list displays Groups in alphabetical order followed by Users in alphabetical order (if you choose to show users). See Role and Group Support for more information about assigning questions to users and groups.
Show Users	**If checked:** Individual users are shown in the Users and Groups list. **If unchecked:** Individual users are not shown in the Users and Groups list.
Allow	This list contains users and groups that will have to answer the question during the enrollment interview.
Deny	This list contains users and groups that will not have to answer the question during the enrollment interview. By default, if any user or group is denied access, all users and groups are denied access except those specified in the Allow list.

Role/Group Support

System questions can be assigned to particular roles or user groups. Role/Group assignment determines the questions a user will be asked during the enrollment interview.

You cannot assign questions to users or groups when using a database (such as Microsoft SQL Server or Oracle Database) for your repository. The settings are available for editing, but the assignments will not be written to the database.

The Access Control panel makes users and groups available so that you can assign question rights to them. The Users and Groups list is unpopulated until you check the Show Users box. Domain users and groups are not initially assigned Allow or Deny access for a given question.

When a user or group is selected, the arrow buttons (<< and >>) become enabled. You move users back and forth between the Users and Groups list and the Allow and Deny lists by clicking the arrow buttons. When you click Create or Modify, the Role/Group access rights are written to the back-end storage for the system question.

The rules for Access Control are as follows:

- **Allow/Deny lists empty:** All users and groups receive the question.
- **Allow list empty, Deny list populated:** All users and groups in the Deny list do not receive the question. All other users and groups receive the question; Allow is implicit.
- **Deny list empty, Allow list populated:** All users and groups in the allow list receive the question. All other users/groups do not. Deny is implicit.
- **Both lists populated:** Users and groups in the Allow list that are not in the Deny list receive the question. If a user or group in the Allow list is also in the Deny list, or belongs to a group in the Deny list, that user or group does not receive the question. Deny overrides Allow.

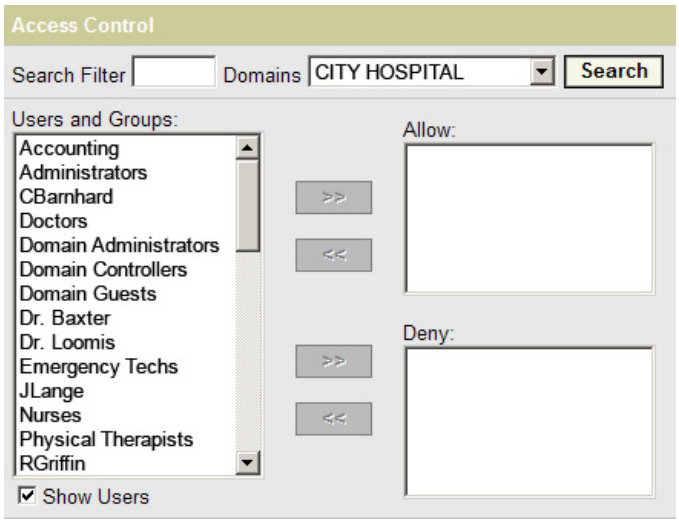
A user's or group's presence in the Deny list always supersedes its presence in the Allow list.

Scenario Number	Description	Allow	Deny	Outcome
1	No user or group specified in Allow and Deny lists	Ø	Ø	Everyone receives the question.
2	Dr. Baxter specified in Allow list; no one specified in Deny list	Dr. Baxter	Ø	Only Dr. Baxter receives the question. All others users are denied.
3	Dr. Baxter specified in Deny list; no one specified in Allow list	Ø	Dr. Baxter	Everyone receives the question except Dr. Baxter.
4	Doctors group specified in Allow list; Dr. Loomis, a member of Doctors group, specified in Deny list	Doctors	Dr. Loomis	All members—and only members—of Doctors group receive the question, except Dr. Loomis, who is denied the question.
5	Doctors group specified in Deny list, Dr. Loomis specified in Allow list	Dr. Loomis	Doctors	Everyone, including Dr. Loomis, is denied the question. The Deny list supersedes the Allow list.

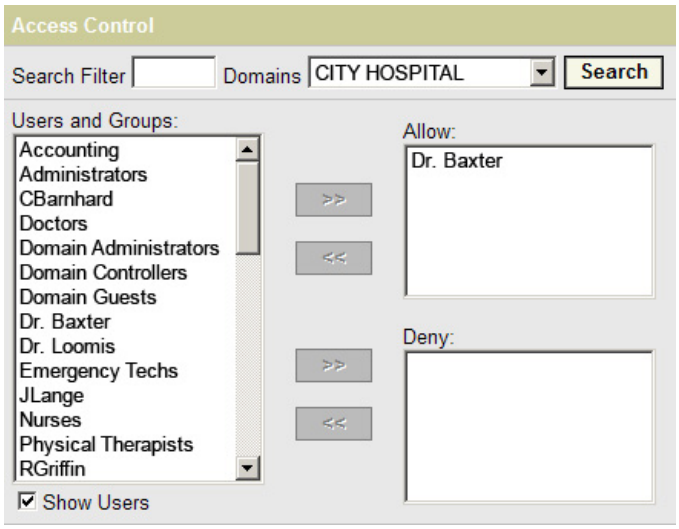
The scenarios below demonstrate how to apply these rules.

You have set up a group, Doctors, which includes members Dr. Baxter and Dr. Loomis.

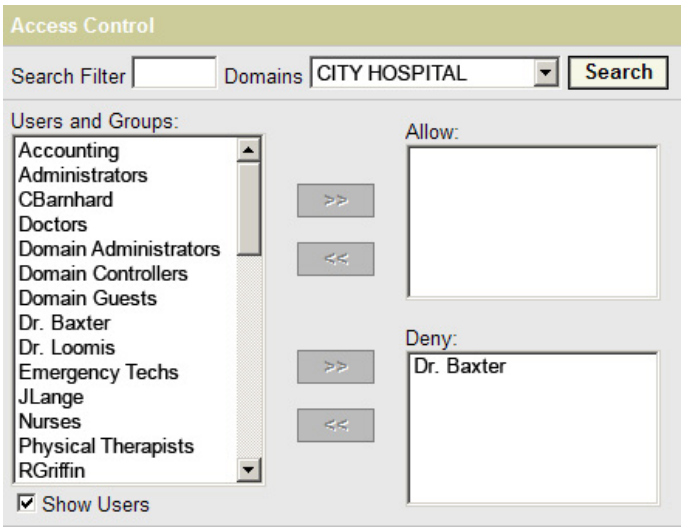
- **Scenario 1:** If the Allow and Deny lists are unpopulated, all users and groups receive the question.



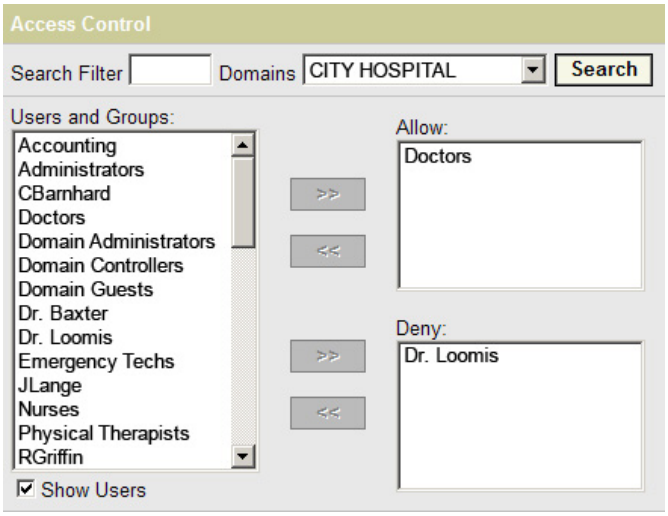
- **Scenario 2:** If the Deny list is unpopulated and the Allow list is populated, only users and groups in the Allow list receive the question.



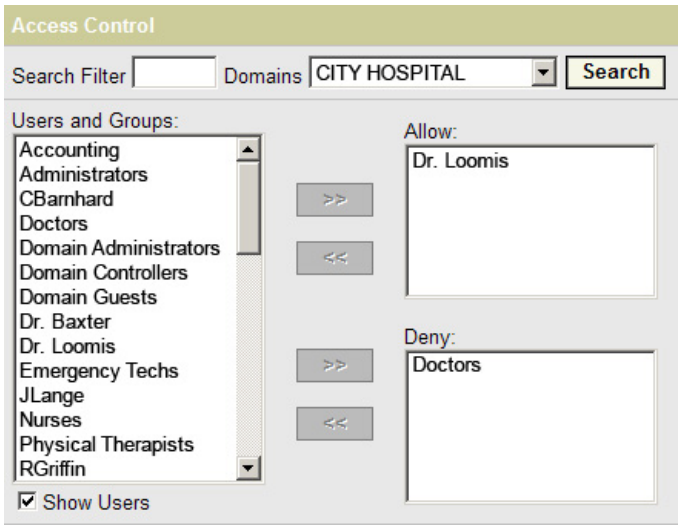
- **Scenario 3:** If any user or group is in the Deny list, and the Allow list is unpopulated, only the user or group in the Deny list does not receive the question.



- **Scenario 4:** If a group is in the Allow list but a member of that group is in the Deny list, all members of that group receive the question except the member in the Deny list.



- **Scenario 5:** If a group is in the Deny list but a member of that group is in the Allow list, that member will not receive the question.


Access Control
Search Filter
Domains
CITY HOSPITAL
Search
Users and Groups:
Accounting
Administrators
CBarnhard
Doctors
Domain Administrators
Domain Controllers
Domain Guests
Dr. Baxter
Dr. Loomis
Emergency Techs
JLange
Nurses
Physical Therapists
RGriffin
Show Users
>>
<<
>>
<<
Allow:
Dr. Loomis
Deny:
Doctors

Manage Users

Use the Users tab to generate a report on the enrollment status of end users. This report indicates whether or not users have completed the Enrollment Interview, the date and time of enrollment, and whether or not the user is currently locked out.

To generate a report, select the appropriate display options. Select **Export** to save the report as a CSV file or click **Search** to generate and display the report in the Web browser.

Display Options	
Show users that are:	Select the users to generate a report on: **Enrolled**, **Not Enrolled** or **Both**.
Show date/time of enrollment	Select to display the date and time of enrollment. Enabling this may slow down report generation time.

Enrollment Status Report Results	
Username	Click a User Name to view additional details about a particular end user's ESSO-PR activity: • The end user's current enrollment status. • Whether the end user has been locked out of the reset service for having repeatedly failed the Reset Quiz; the number of permitted consecutive failures and the duration of the lockout are set in the Settings dialog box (under the Settings tab). If you want to lock out this user, click **Lock**. If the user has been locked out, you can override the lockout by clicking **Unlock**. • The end user's e-mail address. • The end user's enrollment history, including the date and time of each enrollment or enrollment attempt, outcome of the enrollment session (Enrollment State) and the aggregate point-values for all questions answered in each session. • The reset activity for this end user, including date and time of each Reset Quiz taken, the quiz outcome (Reset State), the quiz score, and the IP address of the workstation used to take the quiz.
Delete Checkbox	Select to delete user. Check the box next to **User Name** to select all users for deletion. Click **Delete**.
Enrolled	• Users whose Enrolled status is Yes (or a Date/Time) have successfully completed the Enrollment Interview at least once. The date/time is displayed if the Show date/time of enrollment field was selected. • Users whose Enrolled status is No began the Enrollment Interview, but abandoned the interview (by clicking **Cancel**) before completing it.
Locked Out	• Users whose Locked Out status is Yes have been locked out of the reset service for having repeatedly failed the Reset Quiz. The number of permitted consecutive failures and the duration of the lockout are set in the Settings dialog (under the Settings tab). If the user has been locked out, you can override the lockout by selecting the **Username** and then clicking the **Unlock** button. • Users whose Locked Out status is No have not been locked out. If you want to lock out this user, select the Username and then click **Lock**.

View Enrollments

Use the View Enrollments dialog box(under the Enrollments tab) to view the enrollment log. This log records all enrollment activity for all users who have taken (or at least started) the Enrollment Interview, the current enrollment status for each end user, the total point-values of all system questions (Required and Optional) that the end user answered during enrollment, and the date and time of each enrollment activity.

To view log entries within a specific date range, enter a **Start Date** and an **End Date** (or click the **Choose** button to select a date from a pop-up calendar), then click **Submit**.

See Setting Up the Enrollment Interview for more information.

Manage Enrollments

Use the Manage Enrollments dialog box (under the Enrollments tab) to export or delete enrollment log entries within a specified date range.

1. Enter a **Start Date** and an **End Date** for the date range (or click **Choose** to select a date from a pop-up calendar).
2. Select an **Action**:

- **Export to File** saves all log entries within the specified date range to a file in comma-separated-value format. Select the **Delete entries after export** checkbox if you want to remove the exported log entries after they are saved to file.
- **Delete** removes all log entries within the specified date range, without saving them.

3. Click **Submit**. If you have selected **Export to File**, in the File Save dialog box, enter a file name and click **OK**.

See Setting up the Enrollment Interview for more information.

View Resets

Use the View Resets dialog (under the Resets tab) to view the reset log. The record for each Reset Quiz given shows the username, the date and time of the quiz, the quiz score, the current reset status, and the IP address of the workstation used to take the quiz.

To view log entries within a specific date range, enter a **Start Date** and an **End Date** (or click **Choose** to select a date from a pop-up calendar), then click **Submit**.

See Configuring Reset Authentication for more information.

Manage Resets

Use the Manage Resets dialog box (under the Resets tab) to export or delete reset log entries within a specified date range.

1. Enter a **Start Date** and an **End Date** for the date range (or click **Choose** to select a date from a pop-up calendar).
2. Select an **Action**:

- **Export to File** saves all log entries within the specified date range to a file in comma-separated-value format. Select the **Delete entries after export** checkbox if you want to remove the exported log entries after they are saved to file.
- **Delete** removes all log entries within the specified date range, without saving them.

3. Click **Submit**. If you have selected **Export to File**, in the File Save dialog box, enter a file name and click **OK**.

See Configuring Reset Authentication for more information.

External Validators

By default, ESSO-PR requires that all the questions and weights used for reset are entered and set up by the administrator and answered by the user upon enrollment. ESSO-PR can also work with external validator sources to simplify this process. External validators allow organizations to write an interface to their backend which can be accepted by ESSO-PR. This validator can call data from various sources (for example, the HR database) that contain pre-defined answers.

For example, lets say one of the reset questions is "What is your Social Security Number?". By default, when a user enrolls, the enrollment interview asks him to supply his social security number. Then when a user resets his password,he is asked to enter his social security number. With an external validator in place, an administrator can direct ESSO-PR to an external data source which contains a pre-defined list of social security numbers. The validator supplies the answer to that question upon user enrollment so that the user does not even have to see that question. A user will only have to enter the answer to that question when attempting to reset his password. If all system questions are answered by an external validator, users can be automatically enrolled.

Follow these basic steps to implement the use of external validators:

1. Write an external validator.
2. Install the validator.
3. Direct ESSO-PR to the external validator.

Writing the External Validator Interface

The external validator must be written in .Net 2.0. To write an implementation, add a reference to the library Passlogix.PasswordReset.dll. Within your assembly, a class implementing the interface, ISSPRValidator, must be written. The interface has the following five methods:

- Initialize
- Cleanup
- IsValidQuestion
- IsValidAnswer
- FriendlyName

Validators that do not implement the ISSPRValidator interface or fail on startup will be ignored.

The validator interface definition is as follows:

```
interface ISSPRValidator

{

     // Called by SSPR on first use of validator.
     void Initialize();


     // Called once by SSPR when the service shuts down.
     void Cleanup();


     // Returns true/false if question is valid for a given user
     bool IsValidQuestion(ISSPRQuery iquery);
```

```
    // Returns true/false if question/answer pair is correct
    bool IsValidAnswer(ISSPRQuery iquery, string strAnswer);

    // The friendly name for SSPR to display
    string FriendlyName { get; }
}
```

The ISSPRQuery interface is supplied by the SSPR service and contains the following properties:

```
interface ISSPRQuery
{
    // The guid of the question
    Guid QuestionGuid { get; }
    // The users identity (in SID format)
    string UserIdentity { get; }
}
```

After this interface has been implemented, the following attribute must be declared referencing the implementation:

```
[assembly: ISSPRValidatorType("<Validator class>")]
```

Replace the string <Validator class> with the full name of the class (including namespace) that implements this interface.

Installing the External Validator

After the validator .dll is written, follow these steps:

1. Create a directory called Validators under <INSTALL_DIR> \Vg-oSelfServiceReset\WebServices. The actual validator directory is defined in web.config and can be changed if a different folder for discovery is preferred.
2. Copy the validators into this directory.
3. Restart the ESSO-PR Web Service.

Directing ESSO-PR to the External Validator

After the validators are installed, follow these steps:

1. Open the ESSO-PR Management Console.
2. Click **Questions** from the top menu and then select **System Questions**. Select an existing question or create a New Question.
3. The Answer Source dropdown field lists the available external validators that can be used. The default is User Supplied, which indicates that the user must answer that question during enrollment. If a validator is installed and detected, its friendly name will now be listed here. Select the appropriate validator and save the question settings.

User Enrollment

Enrollment can contain a mix of User Supplied and Validator Supplied questions. Questions that require external validation will be checked against IsValidQuestion and allowed / discarded based

on the result. A user will only be prompted for answers on questions that are user supplied. In a pure external validation case, the user will be automatically enrolled.

Reset

During a password reset, questions with answers supplied by an external validator will be sent to IsValidAnswer to determine a pass or fail for a particular question.

Deleting the External Validator

To delete an external validator:

1. Remove the .dll from the directory in which you placed it.
2. Return to the Management Console, and individually select for editing the questions that relied on the external validator.

   You will be presented with the error message, "The validator <*validator details*> cannot be found. Answer Source will default to User Supplied."
3. Click the **Modify** button.

Deleting an external validator results in users' failing the reset quiz, but does not force them to re-enroll. In order to force their re-enrollment, you must delete users whose enrollment was dependent on the external validator.