Oracle® Enterprise Single Sign-on Password Reset

How-To: Understanding the ESSO-PR Database Schema

Release 11.1.1.2.0

20420-01

December 2010

Oracle Enterprise Single Sign-on Logon Manager How-To: Understanding the ESSO-PR Database Schema

Release 11.1.1.2.0

20420-01

Copyright © 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

Introduction

About This Guide

This document describes the data stored by ESSO-PR in the database using examples from the operation of a typical ESSO-PR installation. Log messages corresponding to the actions included in the examples are also shown for reference.

This document details the information that is stored by ESSO-PR during the configuration of the system questions and the enrollment and reset activities of the end users. In addition, this document details the logging information that is sent to SYSLOG. The examples in this guide are based on an ESSO-PR installation deployed with an Oracle 10g database.

Prerequisites

Readers of this document should have a solid understanding of ESSO-PR, the Structured Query Language (SQL), and database systems, including data structures and management.

Note: The procedures in this guide require that the ESSO-PR server environment and accounts have been set up as outlined in the *ESSO-PR Server Installation and Setup Guide*.

Terms and Abbreviations

The following table describes the terms and abbreviations used throughout this guide:

Term or Acronym	Description
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset
Server	ESSO-PR Server
Client	ESSO-PR -Side Software
Console	ESSO-PR Administrative Console

Accessing ESSO-PR Documentation

We continually strive to keep ESSO-PR documentation accurate and up to date. For the latest version of this and other ESSO-PR documents, visit http://download.oracle.com/docs/cd/E15624_01/index.htm.

Understanding ESSO-PR Data Structures

Overview

This document shows examples of the data stored in the database by ESSO-PR during its operation, and how this data is stored in the database. The following types of data are illustrated:

- ESSO-PR Database Tables
- Main Configuration Data (SYSTEMPARAMETERS Table)
- Logging Configuration Data (SYSTEMPARAMETERS Table)
- System Challenge Question Data (SYSTEMPARAMETERS Table)
- User Enrollment Data (ENROLLMENTINFORMATION, USERQUESTIONS, and USER Tables)
- Password Reset Data (RESETINFORMATION Table)
- Log Message Data (SYSLOG)

Note: This guide is intended as a reference only and does not provide the actual configuration steps the results of which are illustrated in the examples shown. For information on how to access the configuration forms and settings described in this guide, see the *ESSO-PR Installation and Setup Guide*.

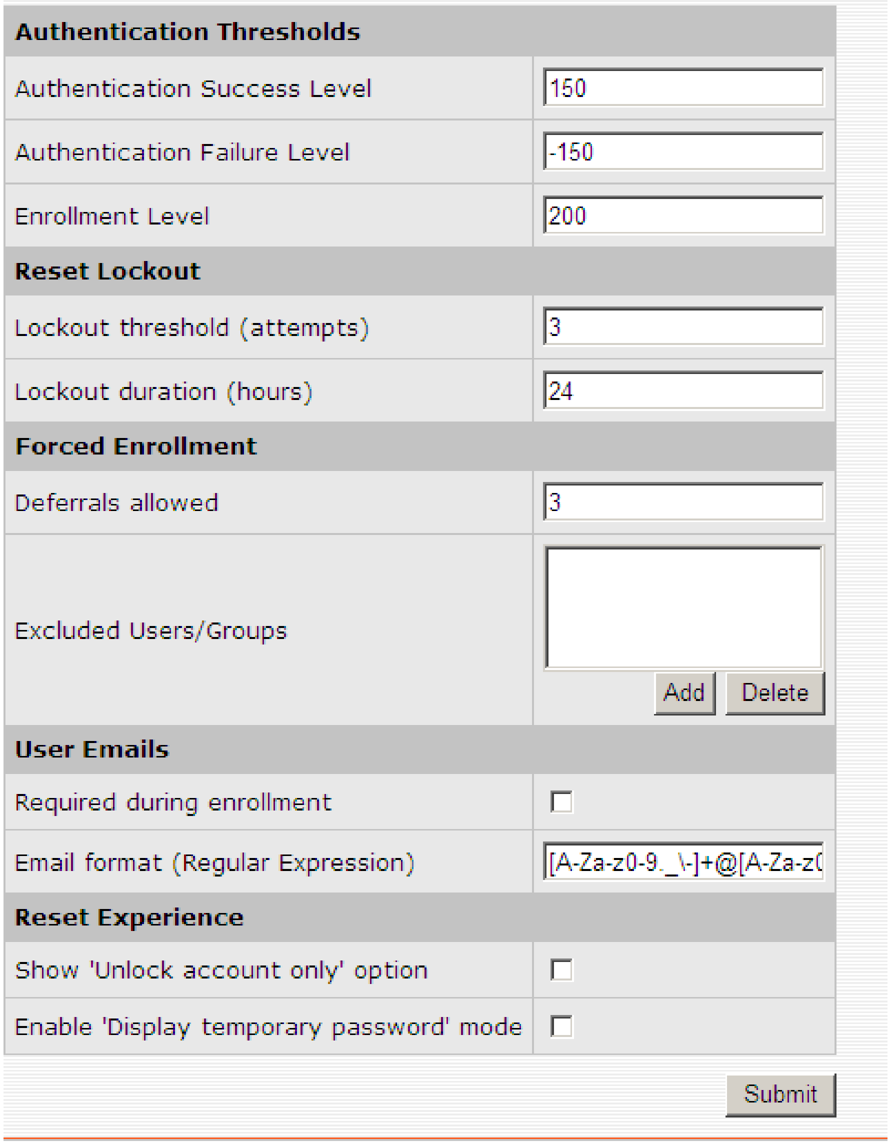
ESSO-PR Database Tables

The ESSO-PR database schema initialization process results in the creation of the following tables:

- `SYSTEMPARAMETERS` – stores main ESSO-PR configuration data.
- `ENROLLMENTINFORMATION` – stores user enrollment data.
- `RESETINFORMATION`– stores password reset data.
- `USERQUESTIONS` – stores user-created enrollment challenge questions.
- `USER` – stores user accounts enrolled with ESSO-PR.
- `SYSTEMQUESTIONS` – stores mandatory system-wide enrollment challenge questions.

Main Configuration Data (SYSTEMPARAMETERS Table)

In this example, we configure ESSO-PR as shown below and submit the changes to the server.



Authentication Thresholds	
Authentication Success Level	150
Authentication Failure Level	-150
Enrollment Level	200
Reset Lockout	
Lockout threshold (attempts)	3
Lockout duration (hours)	24
Forced Enrollment	
Deferrals allowed	3
Excluded Users/Groups	Add Delete
User Emails	
Required during enrollment	□
Email format (Regular Expression)	[A-Za-z0-9._\-]+@[A-Za-z0
Reset Experience	
Show 'Unlock account only' option	□
Enable 'Display temporary password' mode	□

When you click **Submit**, the following data is written to the `SYSTEMPARAMETERS` table as an XML string:

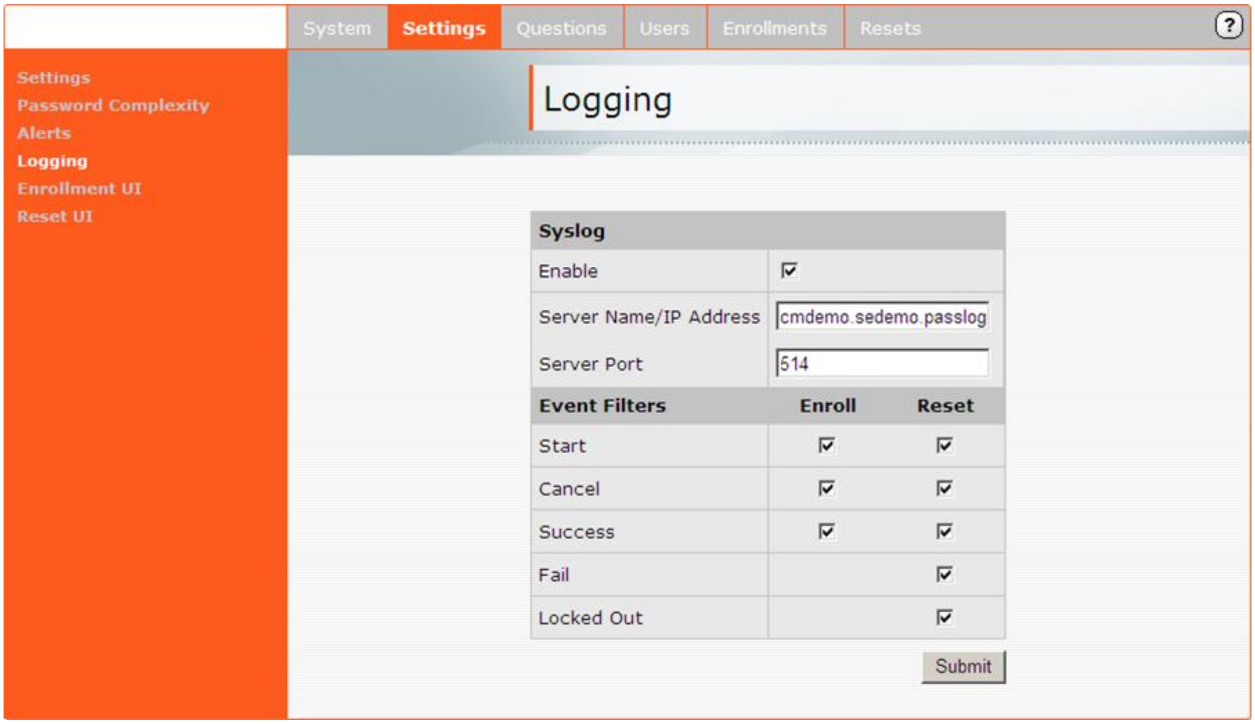
- `AuthSuccessLevel="150"`
- `AuthFailureLevel="-150"`
- `EnrollLevel="200"`
- `UserQuestionCorrectResponseWeight="0"`
- `UserQuestionWrongResponseWeight="0"`
- `MinUserDefinedQuestions="0"`
- `MaxUserDefinedQuestions="0"`
- `AdminServiceStatus="0"`
- `OperationalServiceState="0"`
- `UserLockoutCount="3"`
- `UserLockoutHours="24"`
- `ByPassForceEnrollment="3"`
- `ExcludedUsers=""`
- `UserEmailRequired="0"`
- `UserEmailFormat="[A-Za-z0-9._\-]+@[A-Za-z0-9._\-]+[.][A-Za-z][A-Za-z][A-Za-z]?"`
- `ShowUnlockOption="false"`
- `EnableTempPasswordMode="false"`

Additionally, the following logging configuration data is written to the `SYSTEMPARAMETERS` table as an XML string:

- `SyslogEnable="false"`
- `SyslogPort="514"`
- `EventFilter="0"`

Logging Configuration Data (`SYSTEMPARAMETERS` Table)

In this example, we configure ESSO-PR logging as shown below and submit the changes to the server.



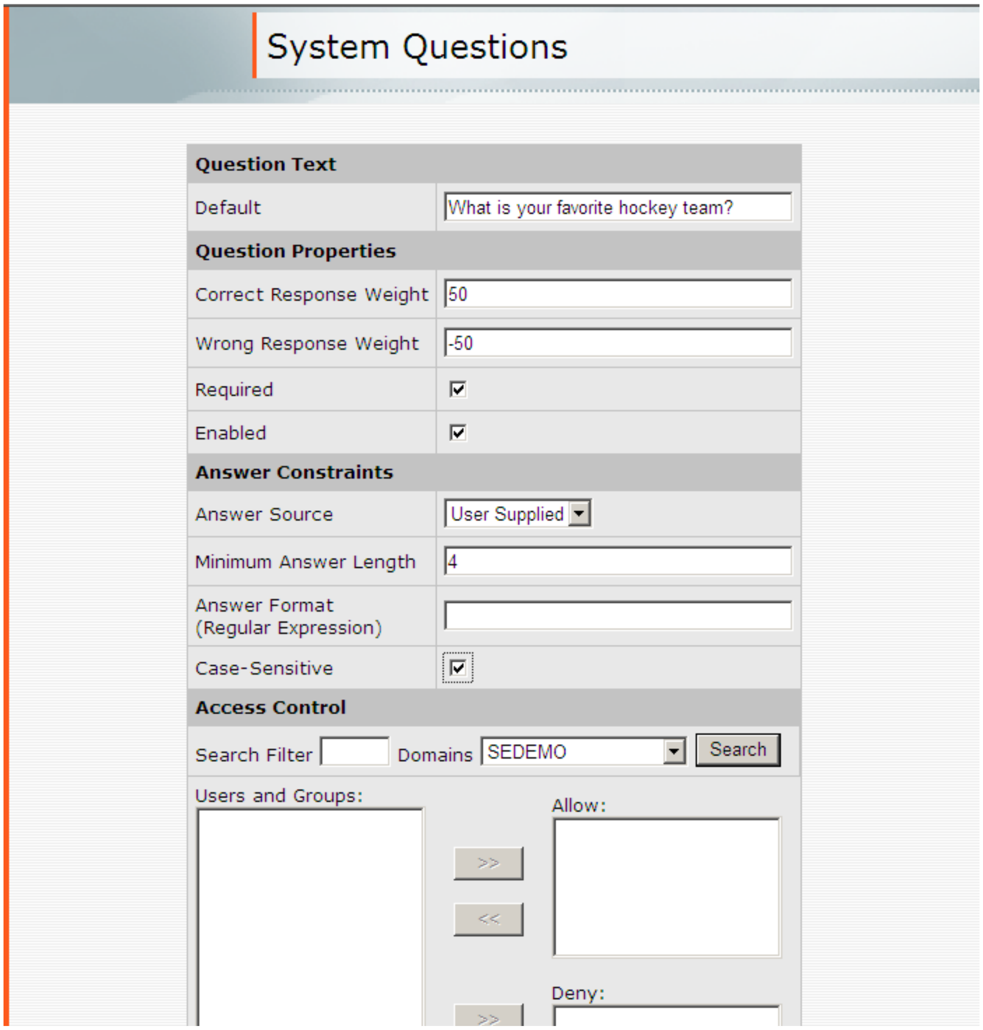
Syslog		
Enable	☑	
Server Name/IP Address	cmdemo.sedemo.passlog	
Server Port	514	
Event Filters	**Enroll**	**Reset**
Start	☑	☑
Cancel	☑	☑
Success	☑	☑
Fail		☑
Locked Out		☑

When you click **Submit**, the following data is written to the `SYSTEMPARAMETERS` table as an XML string:

- `SyslogEnable="true"`
- `SyslogServer="cmdemo.sedemo.passlog"`
- `SyslogPort="514"`
- `EventFilter="2031623"`

System Challenge Question Data (`SYSTEMPARAMETERS` Table)

In this example, we configure ESSO-PR system challenge questions as shown below and submit the changes to the server.



System Questions

Question Text	
Default	What is your favorite hockey team?
Question Properties	
Correct Response Weight	50
Wrong Response Weight	-50
Required	☑
Enabled	☑
Answer Constraints	
Answer Source	User Supplied
Minimum Answer Length	4
Answer Format (Regular Expression)	
Case-Sensitive	☑
Access Control	
Search Filter	Domains SEDEMO

When you click **Submit**, the following data is written to the SYSTEMPARAMETERS table as XML strings:

QUID	99a96ea2-671c-4db6-941c-058a6986123b

QUESTION	QuestionText="What is your favorite hockey team?"
	AnswerSource="1"
	CorrectResponseWeight="50"
	DisableState="1"
	Required="true"
	SystemQUID="99a96ea2-671c-4db6-941c-058a6986123b"
	QUID="99a96ea2-671c-4db6-941c-058a6986123b"
	WrongResponseWeight="-50"
	Flags="1"
	Language=""
	MinLength="4"
	RegExp=""

A new row is added for each system challenge question created.

User Enrollment Data (ENROLLMENTINFORMATION, USERQUESTIONS, and USER Tables)

The following example illustrates the data written to the database during user enrollment.

1. User accesses the enrollment page via the following URL:

http://<hostname>:<port>/vgoselfservicereset/enrollmentclient/enrolluser.aspx

The ESSO-PR enrolment page is displayed.

2. User clicks **Start**. A new row with the following data (in XML string format) is written to the USER table:

USER.USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137
USER.ENROLLED	FALSE

USER.USERINFORMATION	UserName="SEDEMO\jraymond"
	strSid="S-1-5-21-1607104245-2398925301-1456127008-1137"
	bEnrolled="false"
	LockOutTime="0001-01-01T00:00:00-05:00"
	LockoutCount="0"
	Email=""
	EnrollmentByPassCount="0"
	<Language />
	<ConnectorUsername />

3. When the user answers the required challenge question, a confirmation screen is displayed and a row with the following data is added to the `ENROLLMENTINFORMATION` table:

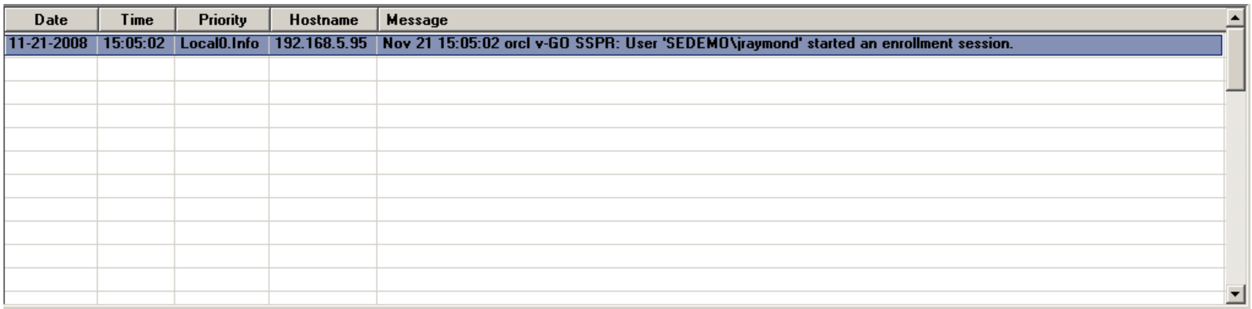
USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137

ENROLLMENTINFORMATION	StartTime="2008-11-21T15:05:02.8386162-05:00"
	EndTime="0001-01-01T00:00:00-05:00"
	Weight="0"
	Activity="1"
	State="2"
	UserNameSelect="SEDEMO\jraymond"
	GUID="d9d3c610-dd78-4292-924c-f21f9c9b9217"

CREATETIME	21- NOV-08

4. When the user clicks **Next** to begin answering the optional challenge questions.

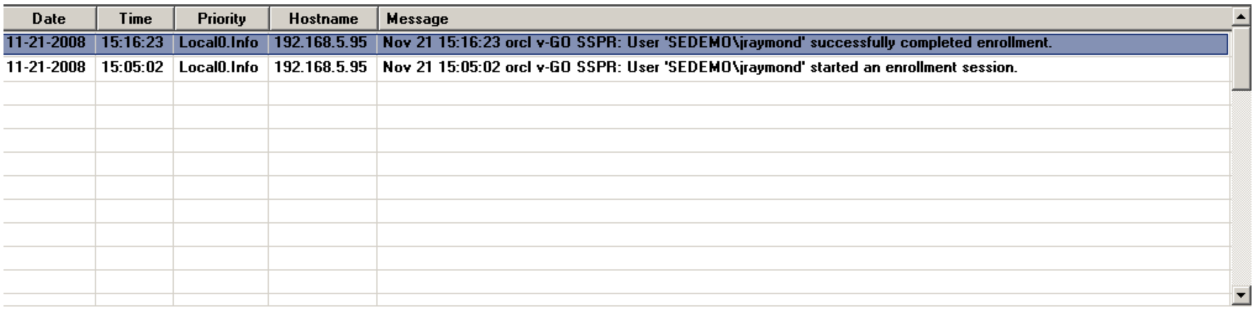
   At this point, the following message is logged:



Date	Time	Priority	Hostname	Message
11-21-2008	15:05:02	Local0.Info	192.168.5.95	Nov 21 15:05:02 orcl v-GO SSPR: User 'SEDEMO\jraymond' started an enrollment session.

   When the user has answered the optional questions (six in our example), the “Enrollment Finished” screen appears.

5. When the user clicks **Close**, the following events occur:
   a. A message is logged:



Date	Time	Priority	Hostname	Message
11-21-2008	15:16:23	Local0.Info	192.168.5.95	Nov 21 15:16:23 orcl v-GO SSPR: User 'SEDEMO\jraymond' successfully completed enrollment.
11-21-2008	15:05:02	Local0.Info	192.168.5.95	Nov 21 15:05:02 orcl v-GO SSPR: User 'SEDEMO\jraymond' started an enrollment session.

b. A row for each answered question is added to the USERQUESTIONS table with the following data:

USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137
QUID	53412afd-af16-4a1a-9ddb-ecdf5414ff51

USERQUESTIONS	QuestionAnswer="BoNGMYmBe5KUp5Zqzu5QtOGylJl6QJtnupKIkQ8TxSnQGIU0" SystemQuestion="true"
	SystemQUID="99a96ea2-671c-4db6-941c-058a6986123b"
	QUID="53412afd-af16-4a1a-9ddb-ecdf5414ff51"

c. The following data is written to the USER table:

USER.USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137
USER.ENROLLED	TRUE

USER.USERINFORMATION	UserName="SEDEMO\jraymond"
	Sid="S-1-5-21-1607104245-2398925301-1456127008-1137" Enrolled="true"
	LockOutTime="0001-01-01T00:00:00-05:00"
	LockoutCount="0"
	Email=""
	EnrollmentByPassCount="0"
	Language />
	ConnectorUsername />

d. The following data is written to the ENROLLMENTINFORMATION table:

USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137

ENROLLMENTINFORMATION	StartTime="2008-11-21T15:05:02.8386162-05:00"
	EndTime="2008-11-21T15:16:23.1736578-05:00"
	Weight="200"
	Activity="1"
	State="6"
	UserNameSelect="SEDEMO\jraymond"
	GUID="71c2739f-b192-42b3-a326-271bec9323da"

CREATETIME	21- NOV-08

Password Reset Data (RESETINFORMATION Table)

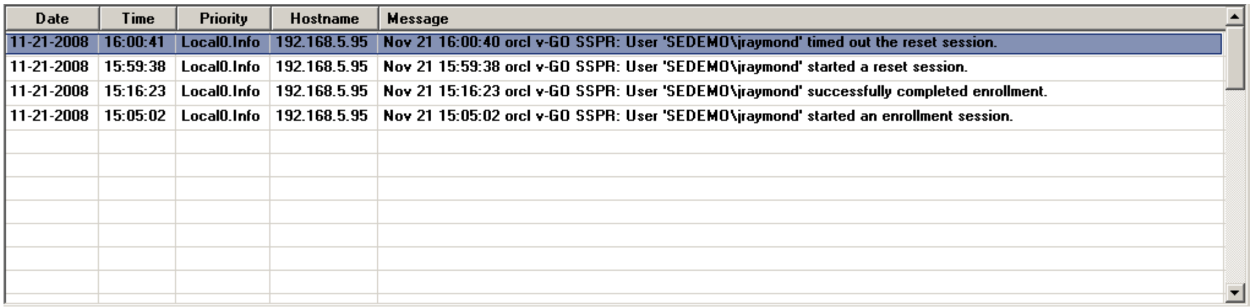
The following example illustrates the data written to the database during password reset.

1. User accesses the password reset page via the following URL:

   http://<hostname>:<port>/vgoselfservicereset/resetclient/default.aspx

   The ESSO-PR logon page appears.

2. When the user enters the required information and waits too long before clicking the **OK** button, the “Session is invalid” screen appears providing a link allowing the user to reset the enrollment session. At this point, the following message is logged:



Date	Time	Priority	Hostname	Message
11-21-2008	16:00:41	Local0.Info	192.168.5.95	Nov 21 16:00:40 orcl v-GO SSPR: User 'SEDEMO\jraymond' timed out the reset session.
11-21-2008	15:59:38	Local0.Info	192.168.5.95	Nov 21 15:59:38 orcl v-GO SSPR: User 'SEDEMO\jraymond' started a reset session.
11-21-2008	15:16:23	Local0.Info	192.168.5.95	Nov 21 15:16:23 orcl v-GO SSPR: User 'SEDEMO\jraymond' successfully completed enrollment.
11-21-2008	15:05:02	Local0.Info	192.168.5.95	Nov 21 15:05:02 orcl v-GO SSPR: User 'SEDEMO\jraymond' started an enrollment session.

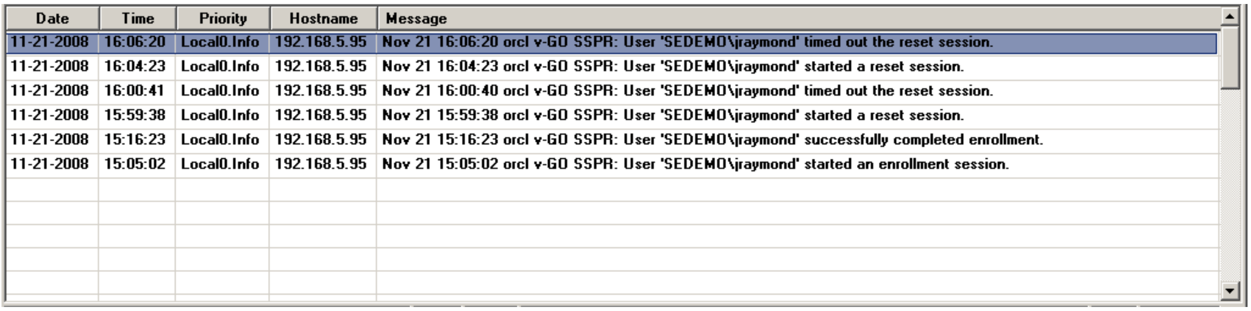
3. When the user retries the reset procedure and arrives at the password reset page, the following data is written to the RESETINFORMATION table:

USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137

RESETINFORMATION	StartTime="2008-11-21T15:59:38.436503-05:00"
	EndTime="2008-11-21T16:00:40.5771384-05:00"
	Weight="0"
	State="2"
	HostAddress="192.168.5.101"

CREATETIME	21-NOV-08

   At this point, the following message is logged:



Date	Time	Priority	Hostname	Message
11-21-2008	16:06:20	Local0.Info	192.168.5.95	Nov 21 16:06:20 orcl v-GO SSPR: User 'SEDEMO\jraymond' timed out the reset session.
11-21-2008	16:04:23	Local0.Info	192.168.5.95	Nov 21 16:04:23 orcl v-GO SSPR: User 'SEDEMO\jraymond' started a reset session.
11-21-2008	16:00:41	Local0.Info	192.168.5.95	Nov 21 16:00:40 orcl v-GO SSPR: User 'SEDEMO\jraymond' timed out the reset session.
11-21-2008	15:59:38	Local0.Info	192.168.5.95	Nov 21 15:59:38 orcl v-GO SSPR: User 'SEDEMO\jraymond' started a reset session.
11-21-2008	15:16:23	Local0.Info	192.168.5.95	Nov 21 15:16:23 orcl v-GO SSPR: User 'SEDEMO\jraymond' successfully completed enrollment.
11-21-2008	15:05:02	Local0.Info	192.168.5.95	Nov 21 15:05:02 orcl v-GO SSPR: User 'SEDEMO\jraymond' started an enrollment session.

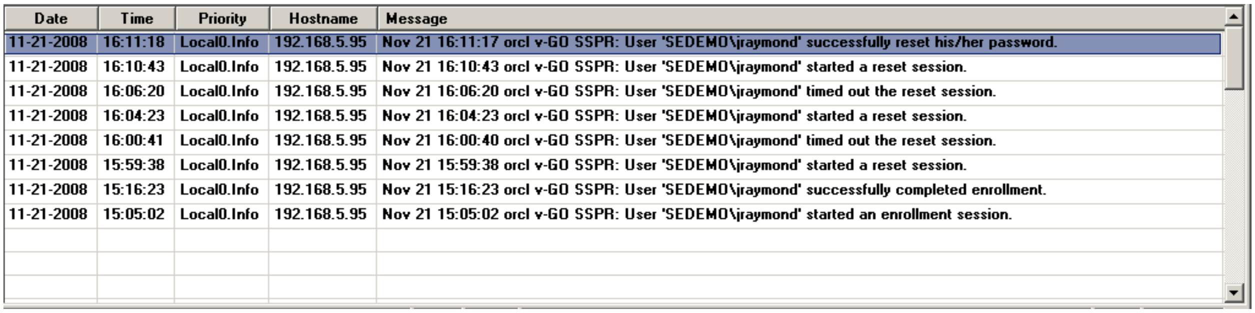
4. When the user has successfully reset the password, ESSO-PR displays a message confirming the successful password reset and the following data is written to the `RESETINFORMATION` table:

USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137

RESETINFORMATION	StartTime="2008-11-21T16:10:43.7618874-05:00"
	EndTime="0001-01-01T00:00:00-05:00"
	Weight="100"
	State="6"
	HostAddress="192.168.5.101"

CREATETIME	21-NOV-08

At this point, the following message is logged:



Date	Time	Priority	Hostname	Message
11-21-2008	16:11:18	Local0.Info	192.168.5.95	Nov 21 16:11:17 orcl v-GO SSPR: User 'SEDEMO\jraymond' successfully reset his/her password.
11-21-2008	16:10:43	Local0.Info	192.168.5.95	Nov 21 16:10:43 orcl v-GO SSPR: User 'SEDEMO\jraymond' started a reset session.
11-21-2008	16:06:20	Local0.Info	192.168.5.95	Nov 21 16:06:20 orcl v-GO SSPR: User 'SEDEMO\jraymond' timed out the reset session.
11-21-2008	16:04:23	Local0.Info	192.168.5.95	Nov 21 16:04:23 orcl v-GO SSPR: User 'SEDEMO\jraymond' started a reset session.
11-21-2008	16:00:41	Local0.Info	192.168.5.95	Nov 21 16:00:40 orcl v-GO SSPR: User 'SEDEMO\jraymond' timed out the reset session.
11-21-2008	15:59:38	Local0.Info	192.168.5.95	Nov 21 15:59:38 orcl v-GO SSPR: User 'SEDEMO\jraymond' started a reset session.
11-21-2008	15:16:23	Local0.Info	192.168.5.95	Nov 21 15:16:23 orcl v-GO SSPR: User 'SEDEMO\jraymond' successfully completed enrollment.
11-21-2008	15:05:02	Local0.Info	192.168.5.95	Nov 21 15:05:02 orcl v-GO SSPR: User 'SEDEMO\jraymond' started an enrollment session.

Log Message Data (SYSLOG)

When enabled, the logging feature of ESSO-PR will write the following data to SYSLOG:

- Date
- Time
- Priority
- Host name
- Message

The following are examples of typical log messages generated by ESSO-PR during normal operation:

Example User Enrollment Log Messages

```
Nov 21 16:21:46 orcl v-GO SSPR: User 'SEDEMO\lchristine' started an
enrollment session.

Nov 21 16:22:42 orcl v-GO SSPR: User 'SEDEMO\lchristine' cancelled the
enrollment session.

Nov 21 15:16:23 orcl v-GO SSPR: User 'SEDEMO\jraymond' successfully completed
enrollment.
```

Example Password Reset Log Messages

```
Nov 21 16:10:43 orcl v-GO SSPR: User 'SEDEMO\jraymond' started a reset
session.

Nov 24 11:21:51 orcl v-GO SSPR: User 'SEDEMO\jraymond' cancelled the reset
session.

Nov 21 16:11:17 orcl v-GO SSPR: User 'SEDEMO\jraymond' successfully reset
his/her password.

Nov 24 09:43:08 orcl v-GO SSPR: User 'SEDEMO\jraymond' failed the reset quiz.

Nov 24 10:00:15 orcl v-GO SSPR: User 'SEDEMO\jraymond' has been locked out!

Nov 21 16:06:20 orcl v-GO SSPR: User 'SEDEMO\jraymond' timed out the reset
session.

Nov 24 10:13:28 orcl v-GO SSPR: User 'SEDEMO\jraymond' successfully unlocked
his/her account.
```

For additional information on logging see the *ESSO-PR Management Console Guide*.