

Oracle® Enterprise Single Sign-on
Password Reset
How-To: Configuring the Minimum Required Permissions
for ESSO-PR
Release 11.1.1.2.0
20419-01

Oracle Enterprise Single Sign-on Password Reset How-To: Configuring the Minimum Required Permissions for ESSO-PR

Release 11.1.1.2.0

20419-01

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

Table of Contents.....	3
Introduction	4
About This Guide.....	4
Prerequisites	4
Terms and Abbreviations	4
Accessing ESSO-PR Documentation	4
Setting the Required Permissions for the ESSO-PR User Account.....	5
Overview	5
Assigning Properties Using the Delegation of Control Wizard	5
Adding the SSPRESET User to the 'Account Operators' Group.....	7

Introduction

About This Guide

This document describes the minimum permissions required for proper operation of Oracle Enterprise Single Sign-on Password Reset (ESSO-PR). Use this document in conjunction with the ESSO-PR product documentation to configure your ESSO-PR environment. This document is provided as a configuration reference meant to aid you in deploying ESSO-PR. It does not cover the steps necessary to achieve the recommended configuration.

Prerequisites

Readers of this document should have a solid understanding of access control lists and group policy management in Microsoft Active Directory. Depending on your configuration, you may need to manually modify the ACLs of various containers within the directory.

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 client-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.

Setting the Required Permissions for the ESSO-PR User Account

Overview

In order to install and run ESSO-PR, you must grant specific permissions to the `SSPRRESET` user account. There are two ways to configure these permissions for proper operation of ESSO-PR:

- Assign properties using the **Delegation of Control** wizard. Use the wizard to grant **Write All Properties**, **Modify Permissions**, and **Reset Password** privileges to the `SSPRRESET` account.
- Add the `SSPRRESET` account to the domain's **Account Operators** group.

Both methods are explained in the remainder of this document.

Assigning Properties Using the Delegation of Control Wizard

Use the “Delegation of Control” wizard to grant the `SSPRRESET` account the following permissions to all objects of type `user` in the directory:

- **Write All Properties.** Allows the `SSPRRESET` user to modify the properties of user objects. Does not grant permissions to create or delete objects.
- **Reset Password.** Allows the `SSPRRESET` user to reset user passwords.

Figure 1 shows the permissions for an SSPRESET account configured as described earlier:

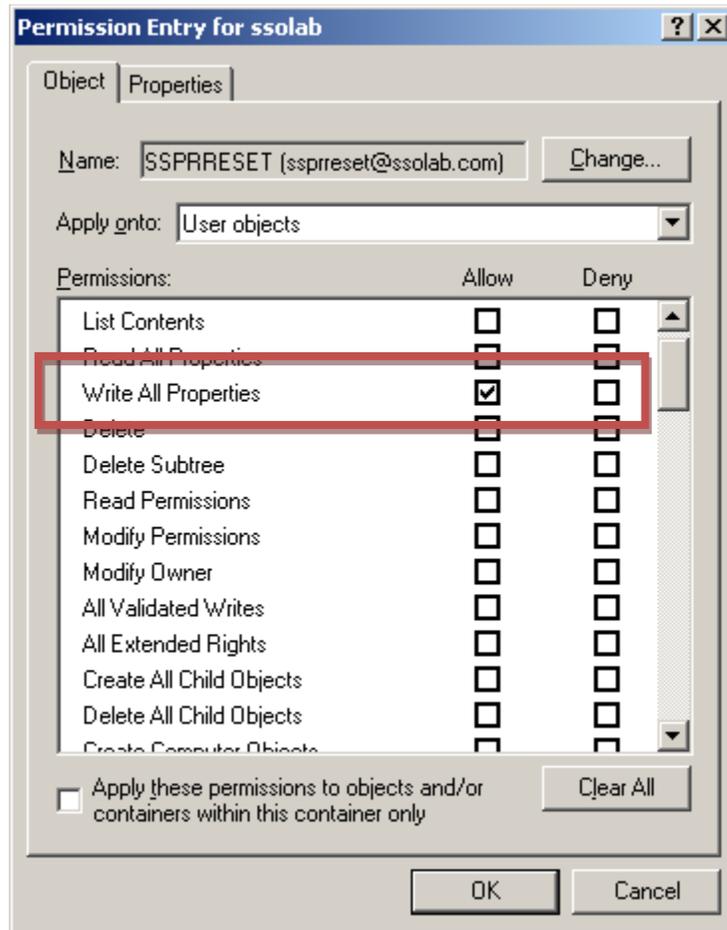


Figure 1 Explicit **Allow** permissions for the SSPRESET account.
(Reset Password permission not shown.)

Adding the SSPRESET User to the 'Account Operators' Group

Membership in the domain's **Account Operators** group gives the SSPRESET user the permissions required for proper operation of ESSO-PR in a more secure way than the manual option described earlier in this guide. We highly recommend that you configure SSPRESET account permissions using this method, as it provides the following benefits:

- Eliminates the need to grant **Domain Administrator** rights.
- Eliminates the need to explicitly grant the **Modify Permissions** privilege.
- Allows you to additionally restrict the SSPRESET account as follows:
 - Explicitly deny the right to modify permissions of all objects within the domain at the root of the domain. This prevents the SSPRESET account from elevating its own (or another user's) privileges.
 - Explicitly deny the right to create and delete child objects at the root of the domain. This prevents the SSPRESET user from creating and deleting objects (such as users).
 - Configure your group policy to explicitly deny the SSPRESET account local logon rights. This prevents other users from gaining unauthorized elevated access by logging on to workstations locally.

Figure 2 and Figure 3 (on the next page) show the permissions for an SSPRESET account configured as described above:

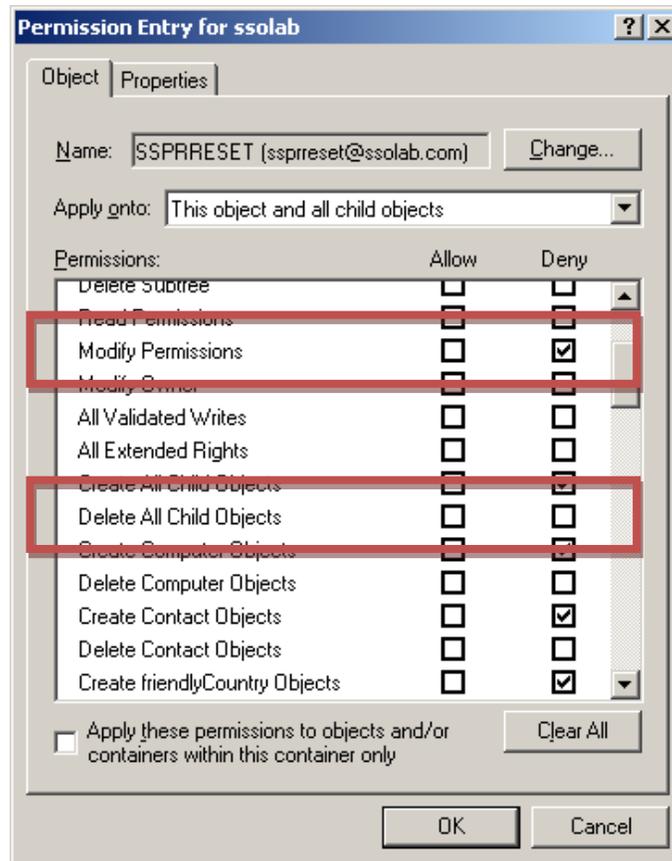


Figure 2. Explicit Deny permissions for the SSPRESET account.

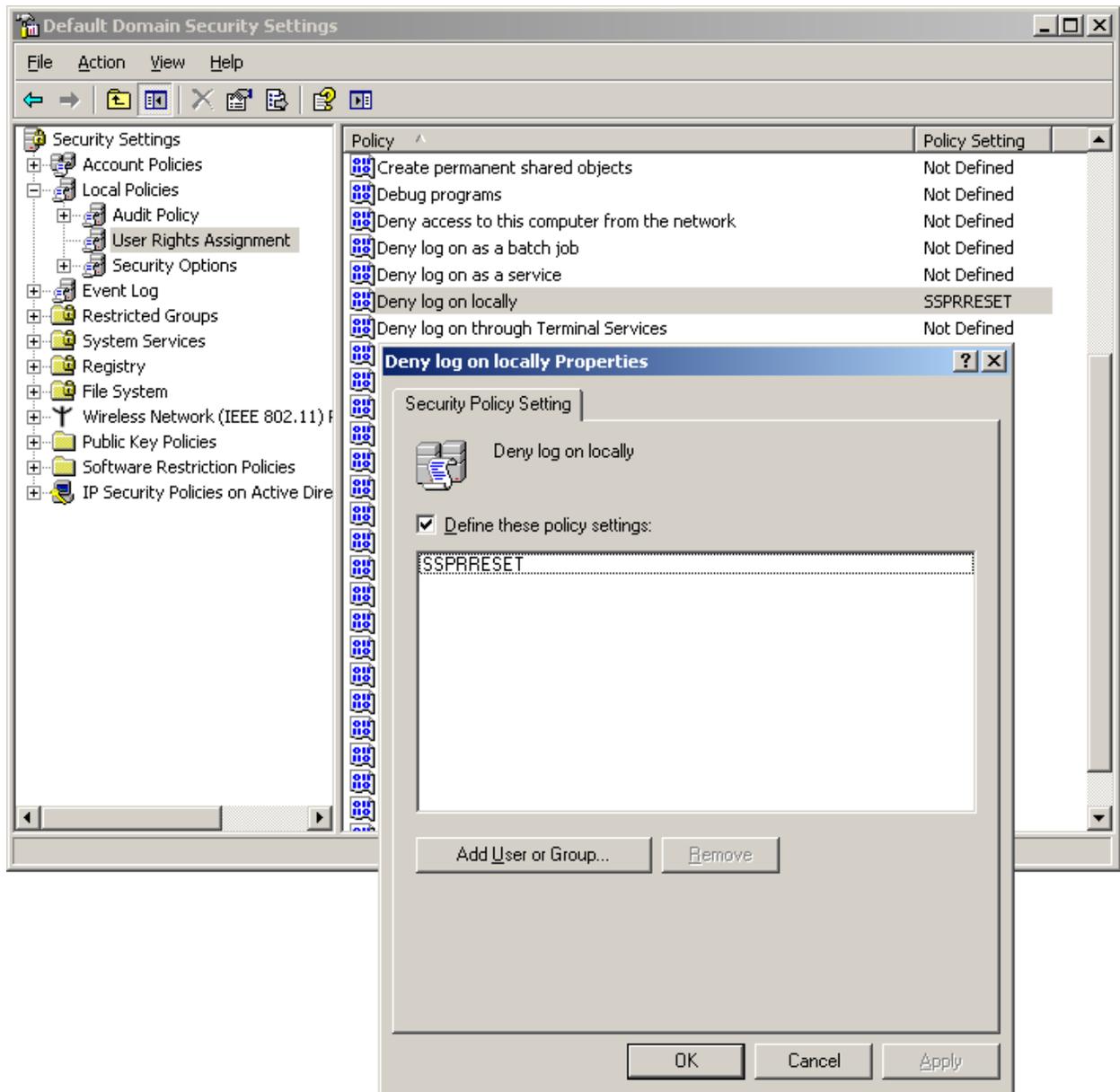


Figure 3- Domain policy setting (Deny logon locally) for the SSPRESET account.