

**Oracle® Enterprise Single Sign-on  
Password Reset**

How-To: Configuring the Minimum Required Permissions  
for ESSO-PR

Release 11.1.1.5.0

**20996-01**

March 2011

Release 11.1.1.5.0

20996-01

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. 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, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

# 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/E21040\\_01/index.htm](http://download.oracle.com/docs/cd/E21040_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.

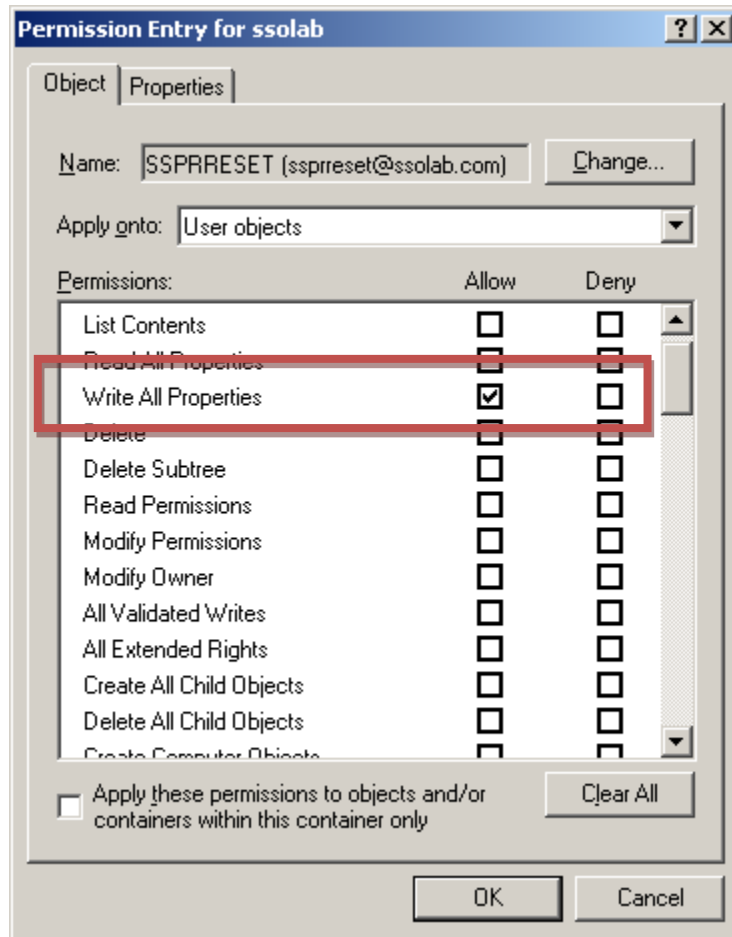
Both methods are explained in the remainder of this document.

## 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:

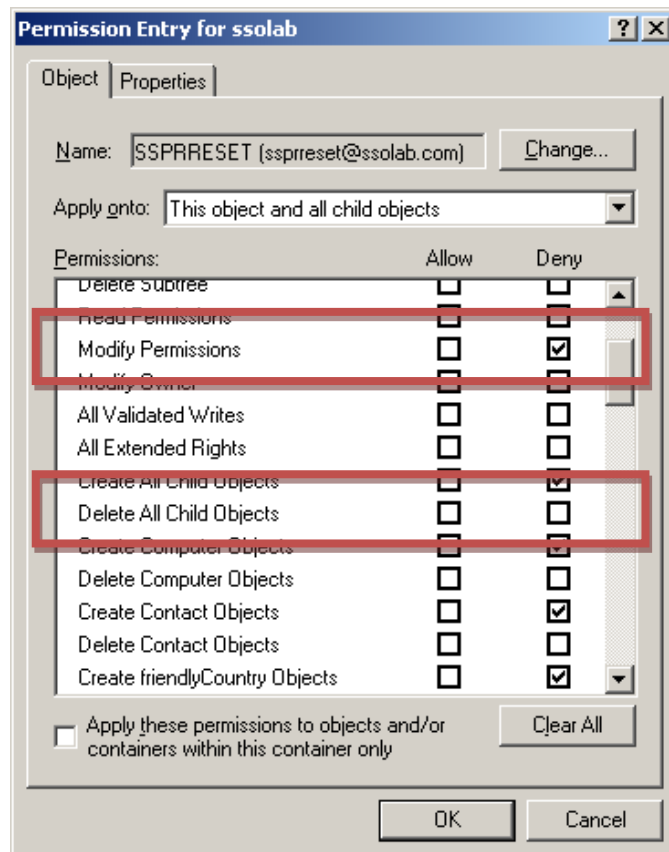


Figure 2 Explicit Deny permissions for the SSPRESET account.

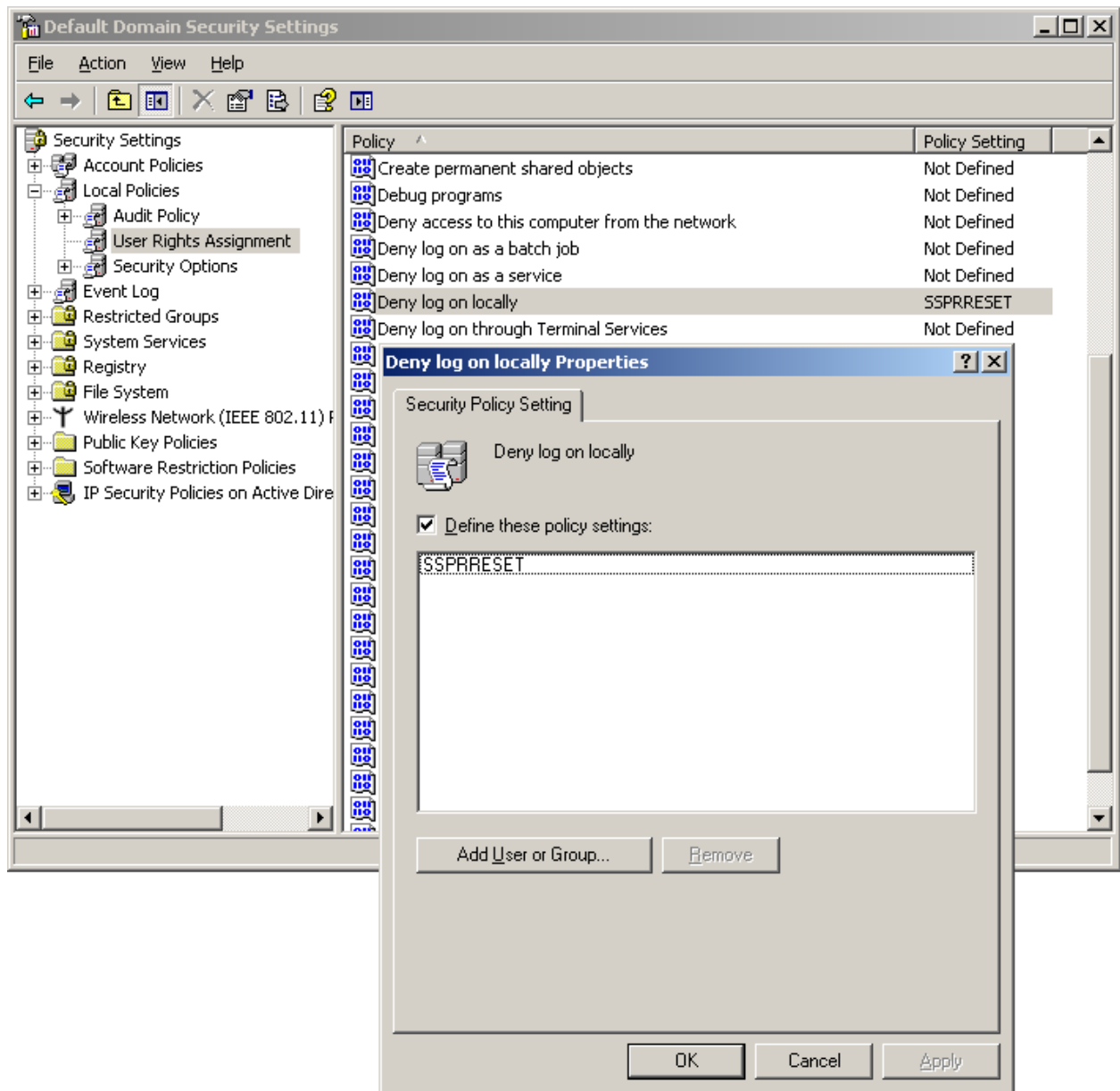


Figure 3 Domain policy setting (Deny logon locally) for the SSPRESET account.