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

Table of Contents

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.

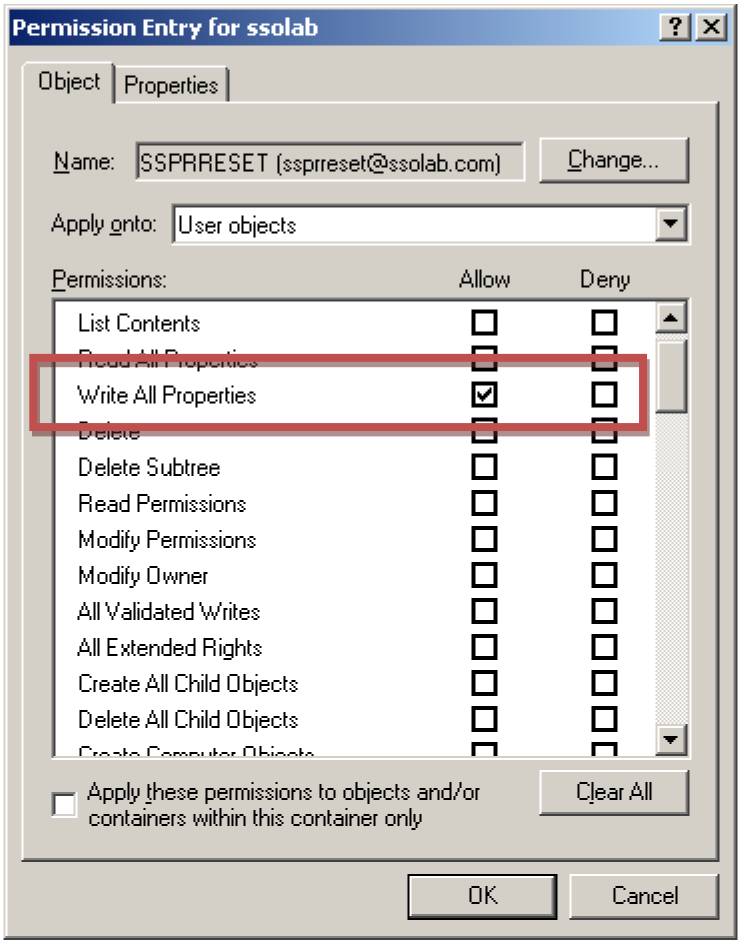
Both methods are explained in the remainder of this document.

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 SSPRRESET account configured as described earlier:



Name: SSPRRESET (ssprreset@ssolab.com)

Apply onto: User objects

Permissions:	Allow	Deny
List Contents	□	□
Read All Properties	□	□
Write All Properties	☑	□
Delete	□	□
Delete Subtree	□	□
Read Permissions	□	□
Modify Permissions	□	□
Modify Owner	□	□
All Validated Writes	□	□
All Extended Rights	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Create Computer Objects	□	□

□ Apply these permissions to objects and/or containers within this container only

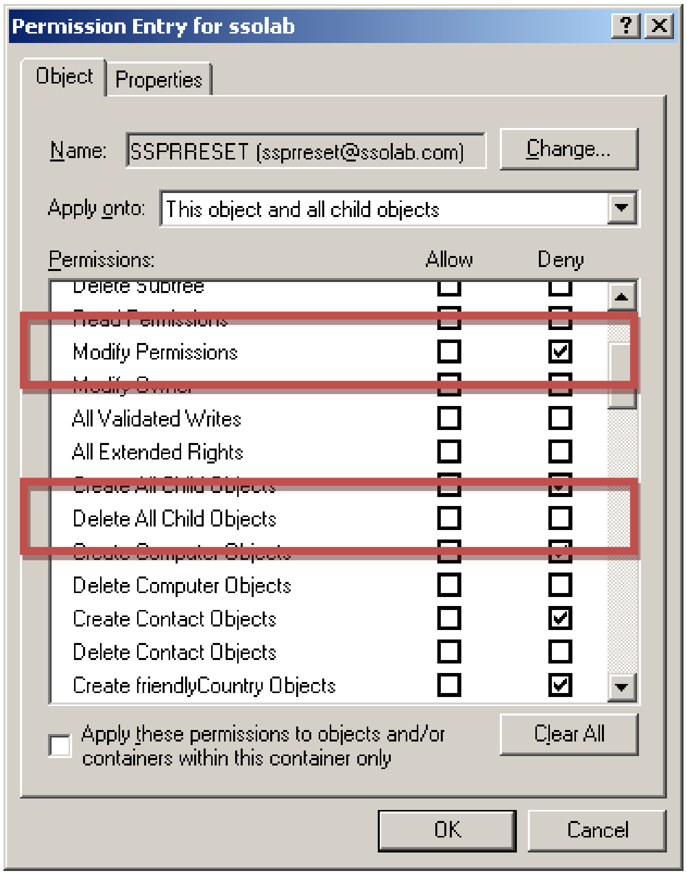
Figure 1 Explicit **Allow** permissions for the SSPRRESET account.
(**Reset Password** permission not shown.)

Adding the SSPRRESET User to the 'Account Operators' Group

Membership in the domain's **Account Operators** group gives the SSPRRESET 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 SSPRRESET 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 SSPRRESET 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 SSPRRESET 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 SSPRRESET user from creating and deleting objects (such as users).
    - Configure your group policy to explicitly deny the SSPRRESET 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 SSPRRESET account configured as described above:



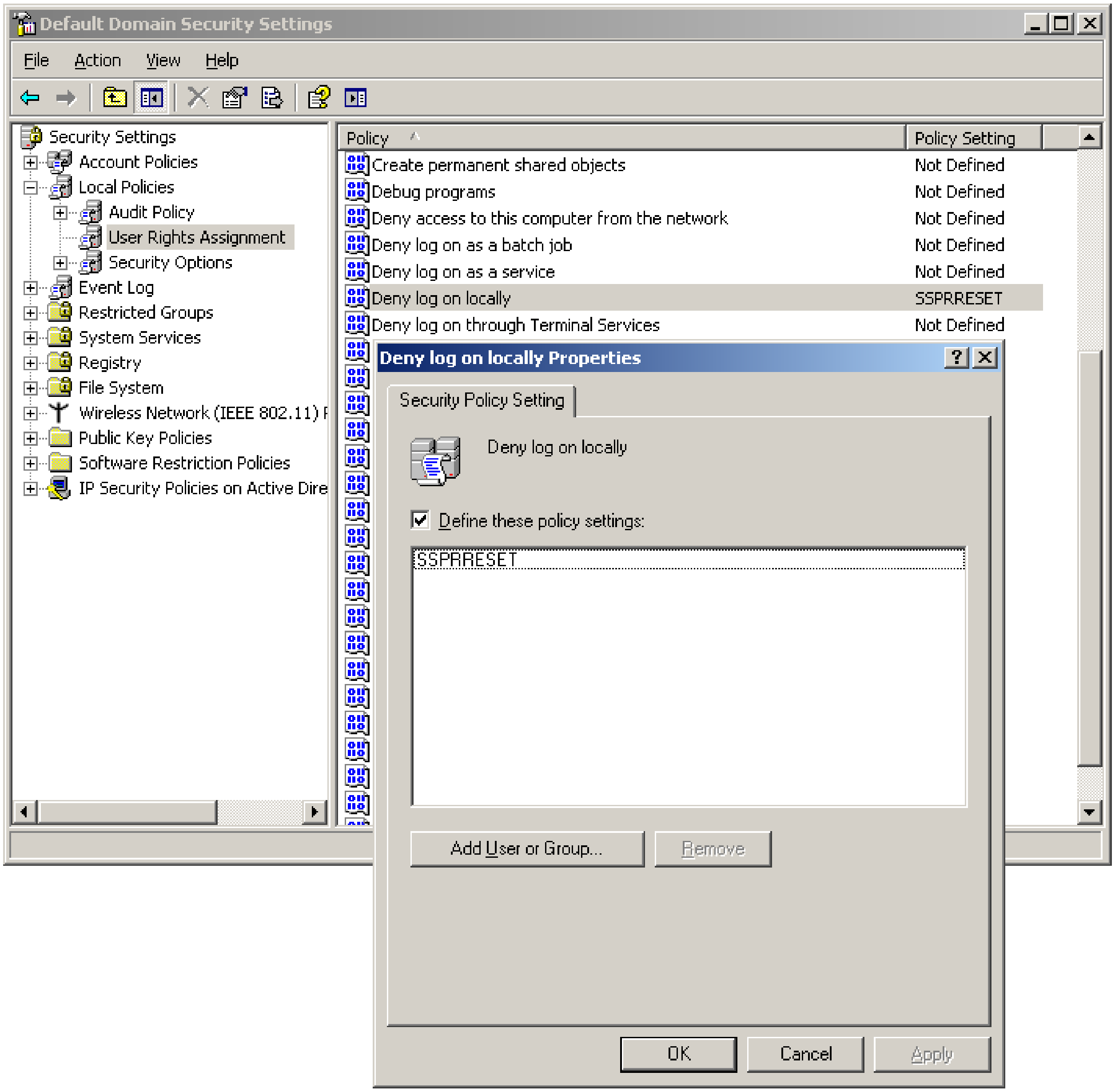
Name: SSPRRESET (ssprreset@ssolab.com)

Apply onto: This object and all child objects

Permissions:	Allow	Deny
Delete Subtree	□	□
Read Permissions	□	□
Modify Permissions	□	☑
Modify Owner	□	□
All Validated Writes	□	□
All Extended Rights	□	□
Create All Child Objects	□	☑
Delete All Child Objects	□	□
Create Computer Objects	□	☑
Delete Computer Objects	□	□
Create Contact Objects	□	☑
Delete Contact Objects	□	□
Create friendlyCountry Objects	□	☑

□ Apply these permissions to objects and/or containers within this container only

Figure 2. Explicit **Deny** permissions for the SSPRRESET account.



- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Event Log
  - Restricted Groups
  - System Services
  - Registry
  - File System
  - Wireless Network (IEEE 802.11) P
  - Public Key Policies
  - Software Restriction Policies
  - IP Security Policies on Active Dire

Policy	Policy Setting
Create permanent shared objects	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	SSPRRESET
Deny log on through Terminal Services	Not Defined

Deny log on locally Properties

Security Policy Setting

Deny log on locally

☑ Define these policy settings:

SSPRRESET

Figure 3~~.~~ Domain policy setting (**Deny logon locally**) for the `SSPRRESET` account.