

**Oracle® Enterprise Single Sign-on  
Provisioning Gateway**

Minimum Permissions Guide

Release 10.1.4.1.0

**E12620-01**

November 2008

Copyright © 2006-2008, 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

About Minimum Permissions ..... 4

    Audience..... 4

    Welcome to the ESSO-PG Minimum Permissions Guide ..... 5

General Recommendations and Notes ..... 6

Installing ESSO-LM and ESSO-LM Agent ..... 7

Installing ESSO-PG Server-Side Components ..... 8

Verifying the ESSO-PG Server-Side Installation .....10

Configuring the ESSO-PG IIS Server .....11

Granting Special Permissions within AD to the PMSERVICE Account .....12

# About Minimum Permissions

When you install Oracle Enterprise Single Sign-On Provisioning Gateway (ESSO-PG), you must create a specific service account, at the domain level, in order for ESSO-PG to function properly. This guide describes how to increase security by creating such an account with a specific set of permissions to certain objects within Active Directory.

## Audience

This guide is intended for experienced administrators and software engineers who are responsible for the installation, configuration, and maintenance of ESSO-PG and ESSO-LM. Administrators are expected to understand the installation, configuration, maintenance, and troubleshooting of the following Microsoft products and technologies:

- Windows® Server 2003
- Microsoft Active Directory
- Microsoft Internet Information Server (version 6.0)
- Oracle ESSO-LM software in a Microsoft Active Directory environment, including installation of the ESSO-LM Administrative Console and the ESSO-LM Agent, schema extension, and configuring the ESSO-LM agent through the ESSO-LM Administrative Console.

Acronym or Abbreviation	Full Name
SSO Agent	ESSO-LM Agent
SSO Administrative Console	ESSO-LM Administrative Console
ESSO-LM	Oracle Enterprise Single Sign-On Logon Manager
ESSO-AM	Oracle Enterprise Single Sign-On Authentication Manager
ESSO-KM	Oracle Enterprise Single Sign-On Kiosk Manager
ESSO-PG	Oracle Enterprise Single Sign-On Provisioning Gateway
ESSO-PR	Oracle Enterprise Single Sign-On Password Reset
SSO	ESSO-LM
FTU	First Time Use
SSO Agent	ESSO-LM Agent

### Welcome to the ESSO-PG Minimum Permissions Guide

ESSO-PG requires a specific service account, at the domain level, in order to function properly. Previously, such an account was a member of the Domain Administrator's group, which presented potential security liabilities.

In order to increase security, Passlogix recommends that this service account be created as a member of an account other than the Domain Users group. (For the purposes of this document, the service account is named PMSERVICE; however, you can follow any naming convention you choose).

The instructions in this document describe how to:

- [create the service account](#) (PMSERVICE) as a member of the Domain Users group
- [grant a specific set of permissions](#) to certain objects within Active Directory to the serviced account
- [configure the ESSO-PG Administrative Console](#)
- [create templates for provisioning](#)
- [provision a user](#).



The PMSERVICE account must also be a member of the local administrator's group on the IIS server that the ESSO-PG server-side components are installed on.



You will need an account with Domain Admin and Schema Admin privileges in order to complete certain tasks involving the installation of ESSO-LM, extending the schema, installing software, and modifying certain permissions within Active Directory.

# General Recommendations and Notes

Oracle recommends that you *not* install Internet Information Server (IIS) on a Domain Controller. Passlogix recommends that you install the ESSO-PG server-side components on a member server, not a Domain Controller.

The procedures and recommendations presented in this document have been tested in a controlled environment where the desired results were achieved. Passlogix recommends that you test these procedures in a non-production environment that resembles your working network as closely as possible.

The procedures outlined in this document involve changes that can affect your entire domain. Specialized policies, trust, inheritance issues, and intra- and inter-site replication issues, particularly as they exist in large enterprises, cannot be fully tested outside of the actual environment.

As with any issues that could affect a large number of users, Passlogix recommends a prudent, *error-on-the-side-of-caution* approach to testing and deploying this product by those who are responsible for installing, configuring, and maintaining it.

## Installing ESSO-LM and ESSO-LM Agent

1. Install and configure ESSO-LM on a workstation within your domain. Install the ESSO-LM Administrative Console, the ESSO-LM Agent, and extend your schema. Refer to the *ESSO-LM Installation and Setup Guide* for more information.
2. Verify that ESSO-LM is functioning properly.
3. Install the ESSO-LM client-side components on the workstation where you installed ESSO-LM. Refer to the *ESSO-PG Installation and Setup Guide* for more information.



When you deploy the ESSO-LM Agent to workstations, you must also deploy the ESSO-PG client-side component to each workstation where ESSO-LM will reside.

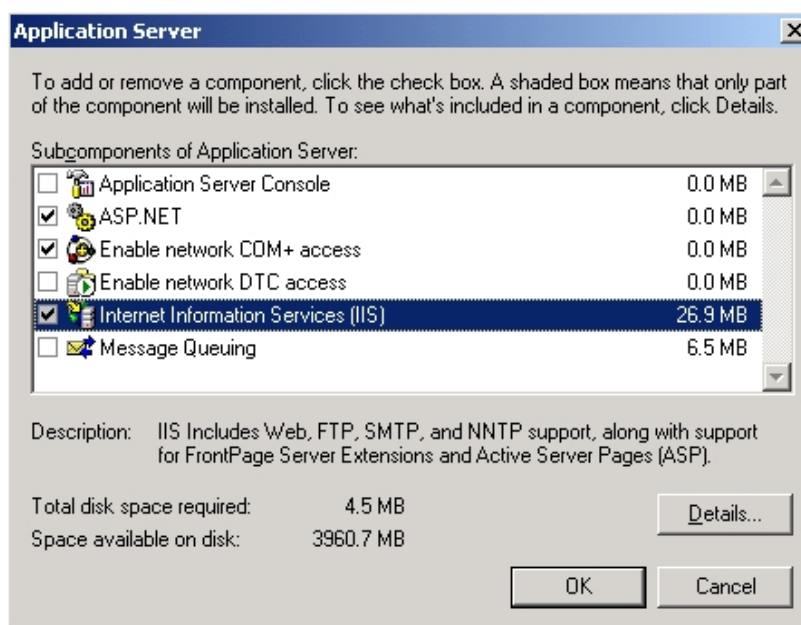


Insert at least *one* application template in the SSOConfig container or you will encounter an error later on during the configuration of the ESSO-PG server-side components.

## Installing ESSO-PG Server-Side Components

To install the ESSO-PG server-side components:

1. On a domain controller, through a Terminal Server session to a domain controller, or through a workstation that has the Active Directory Users and Computers snap-on installed, create an account called PMSERVICE.
2. Provide the account with a very secure password.
3. Verify that the account is *not* required to change its password on next logon. This account need only be a member of the domain users group.
4. On a member server in your domain, log onto that machine as a domain-level administrator.
5. In the Application Server dialog box, verify that Internet Information Server 6.0, as well as the ASP.NET components, are installed:

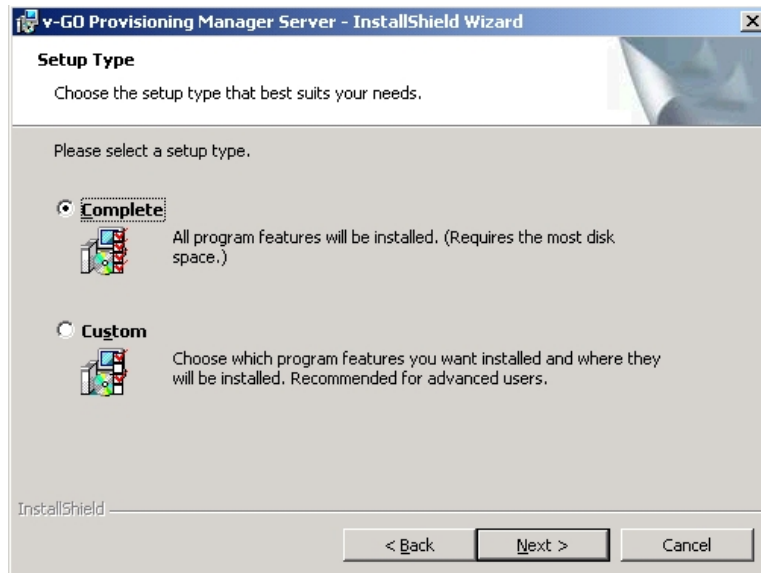


You can install the .NET framework, version 2.0, manually by downloading it from the Microsoft website.

6. There are no special configurations or options to consider during the installation of the ESSO-PG server-side components. Accept the defaults after agreeing to the End-User License Agreement.



7. In the Setup Type dialog box, **Complete**.



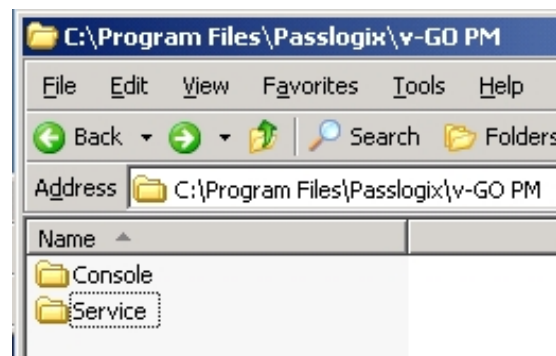
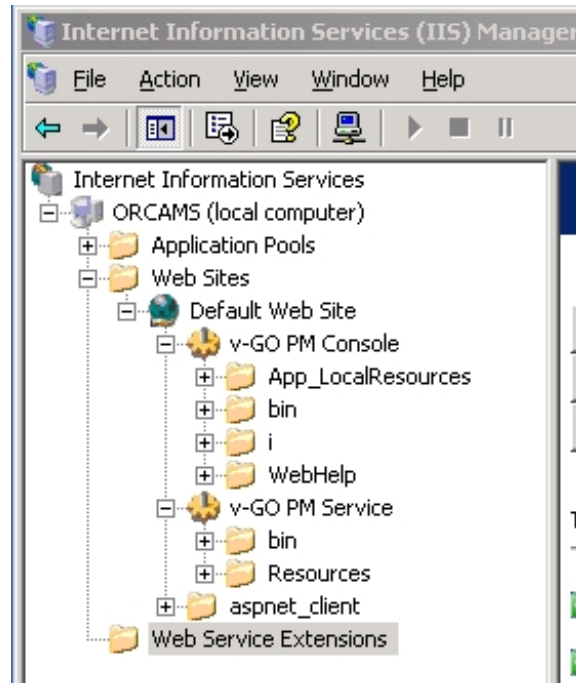
As part of the installation process, one or more DOS windows will flash momentarily on this server as services start and stop. This is normal behavior during the installation process.

# Verifying the ESSO-PG Server-Side Installation

To verify that you have successfully installed the ESSO-PG server-side components on your IIS Member Server, look for the following:

- virtual directories within IIS Manager
- folders and files in the C:\Program Files\Passlogix directories on the server.

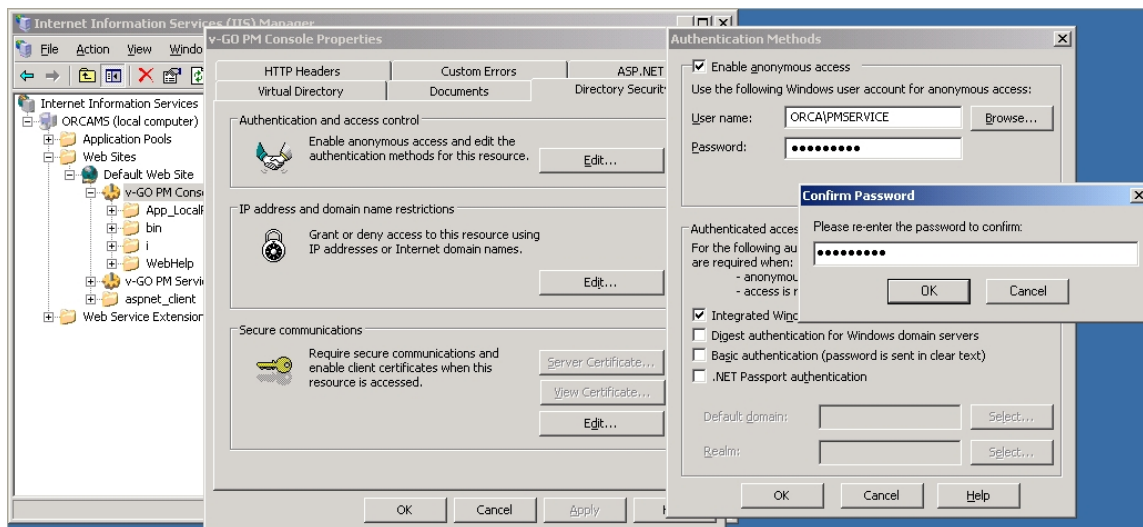
Examples of these entities are shown in the following illustrations:



## Configuring the ESSO-PG IIS Server

In order for the ESSO-PG server-side components to function properly, you must make the PMSERVICE account a member of the local administrator's group on the IIS Server that houses the ESSO-PG server-side components.

1. In the Computer Management tool of the ESSO-PG IIS member server, click on the Local Users and Groups icon.
2. Add the PMSERVICE account to the Administrators group.
3. Open the Internet Information Server, then Default Website.
4. Locate the ESSO-PG Console and ESSO-PG Service virtual directories. For *both* directories, make the PMSERVICE account responsible for anonymous access.



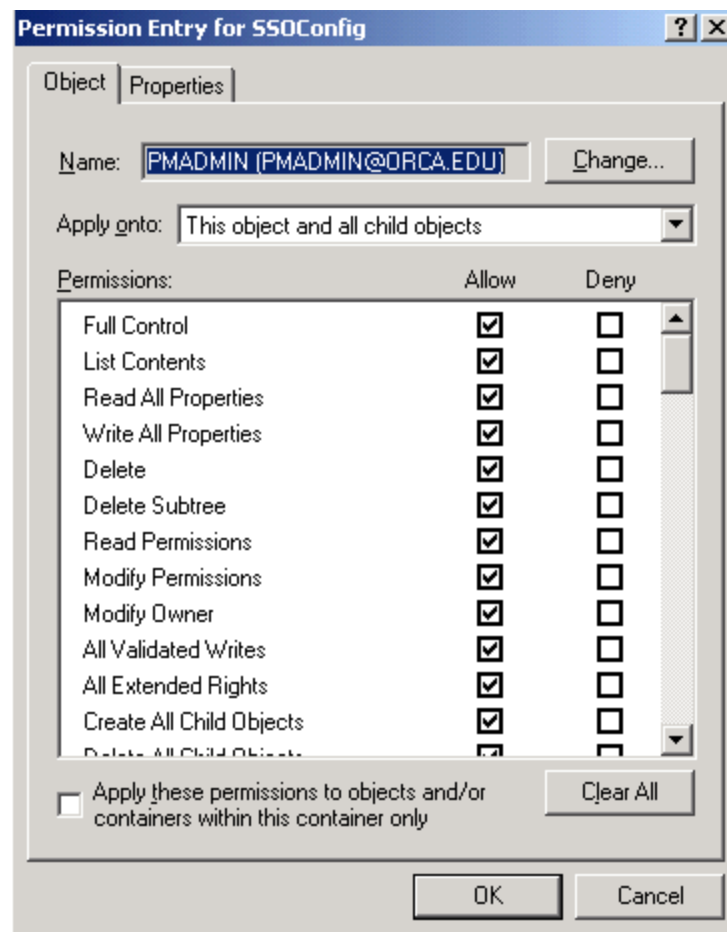
5. From the RUN line, type `iisreset` to restart the IIS service.

## Granting Special Permissions within AD to the PMSERVICE Account

The next procedure is to grant special rights to specific containers within Active Directory to the PMSERVICE account. Remember that, to Active Directory, the PMSERVICE account is simply an ordinary user account.

To grant the special permissions:

1. In the Permission Entry for SSOConfig dialog box, grant the PMSERVICE account advanced full control of the SSOConfig container (the container where the application templates are stored) as shown in the following illustration:



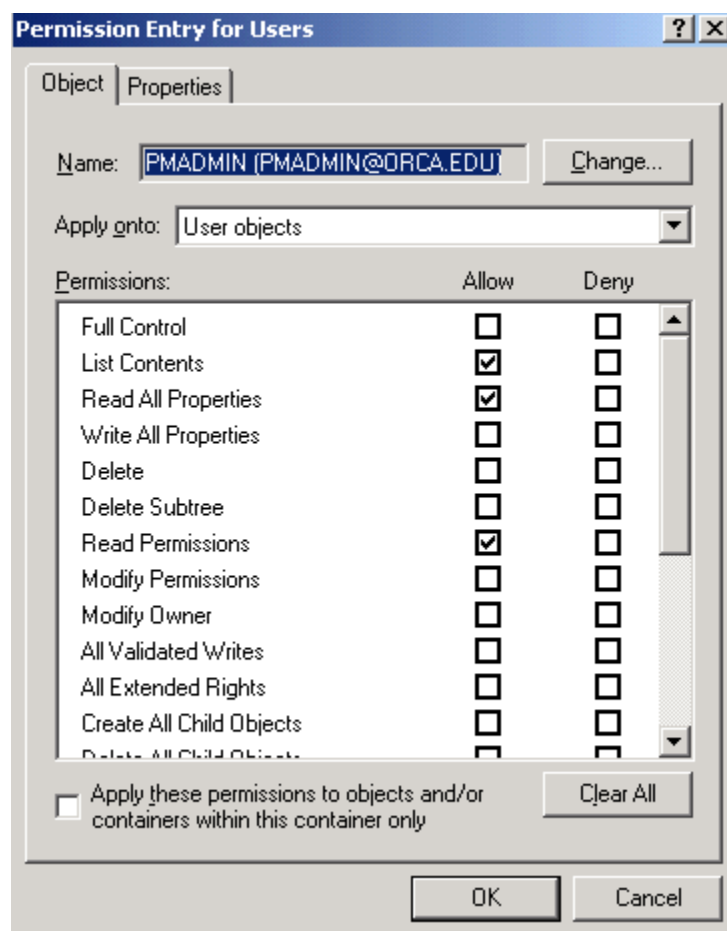
- a. In the Permission Entry for the Users container, grant the PMSERVICE the ALLOW permission applied onto the User objects as it pertains to both the Create vGOUserData Objects and Delete vGOUserData Objects.



Steps 2 through 8, [Granting Special Permissions within Active Directory Users and Computers to the PMSERVICE Account](#), must be repeated for each Organizational Unit that exists within your organization that contains users.

Permissions:	Allow	Deny
Modify	<input type="checkbox"/>	<input type="checkbox"/>
Modify Owner	<input type="checkbox"/>	<input type="checkbox"/>
All Validated Writes	<input type="checkbox"/>	<input type="checkbox"/>
All Extended Rights	<input type="checkbox"/>	<input type="checkbox"/>
Create All Child Objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete All Child Objects	<input type="checkbox"/>	<input type="checkbox"/>
Create vGOConfig Objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete vGOConfig Objects	<input type="checkbox"/>	<input type="checkbox"/>
Create vGOUserData Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete vGOUserData Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Allowed to Authenticate	<input type="checkbox"/>	<input type="checkbox"/>
Change Password	<input type="checkbox"/>	<input type="checkbox"/>
Receive As	<input type="checkbox"/>	<input type="checkbox"/>
Reset Password	<input type="checkbox"/>	<input type="checkbox"/>

- b. Grant List Contents, Read all Properties, and Read Permissions to the User Objects containers.



## Granting Special Permissions within AD to the PMSERVICE Account

- c. Grant the ALLOW permission applied onto the User objects as it pertains to both the Create vGOConfig Objects and Delete vGOConfig Objects.

**Permission Entry for Users**

Object | Properties

Name: PMADMIN (PMADMIN@ORCA.EDU) [Change...]

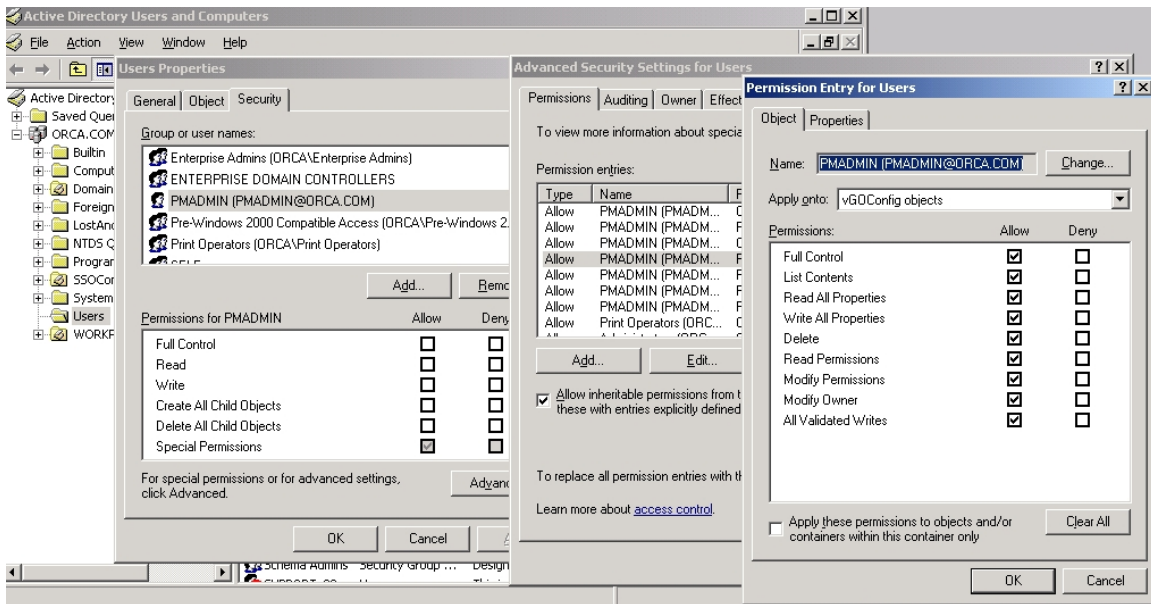
Apply onto: User objects

Permissions:	Allow	Deny
Modify Permissions	<input type="checkbox"/>	<input type="checkbox"/>
Modify Owner	<input type="checkbox"/>	<input type="checkbox"/>
All Validated Writes	<input type="checkbox"/>	<input type="checkbox"/>
All Extended Rights	<input type="checkbox"/>	<input type="checkbox"/>
Create All Child Objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete All Child Objects	<input type="checkbox"/>	<input type="checkbox"/>
Create vGOConfig Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete vGOConfig Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create vGOUserData Objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete vGOUserData Objects	<input type="checkbox"/>	<input type="checkbox"/>
Allowed to Authenticate	<input type="checkbox"/>	<input type="checkbox"/>
Change Password	<input type="checkbox"/>	<input type="checkbox"/>
Receive As	<input type="checkbox"/>	<input type="checkbox"/>

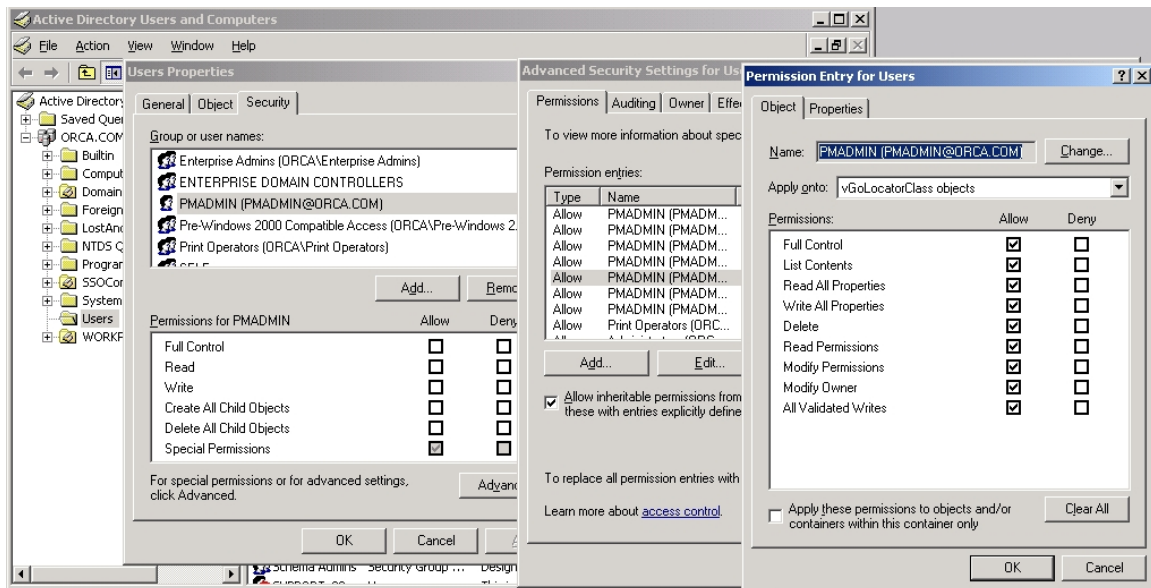
☐ Apply these permissions to objects and/or containers within this container only [Clear All]

OK Cancel

- Grant FULL CONTROL to the PMSERVICE account as it applies to the vGOConfig objects.

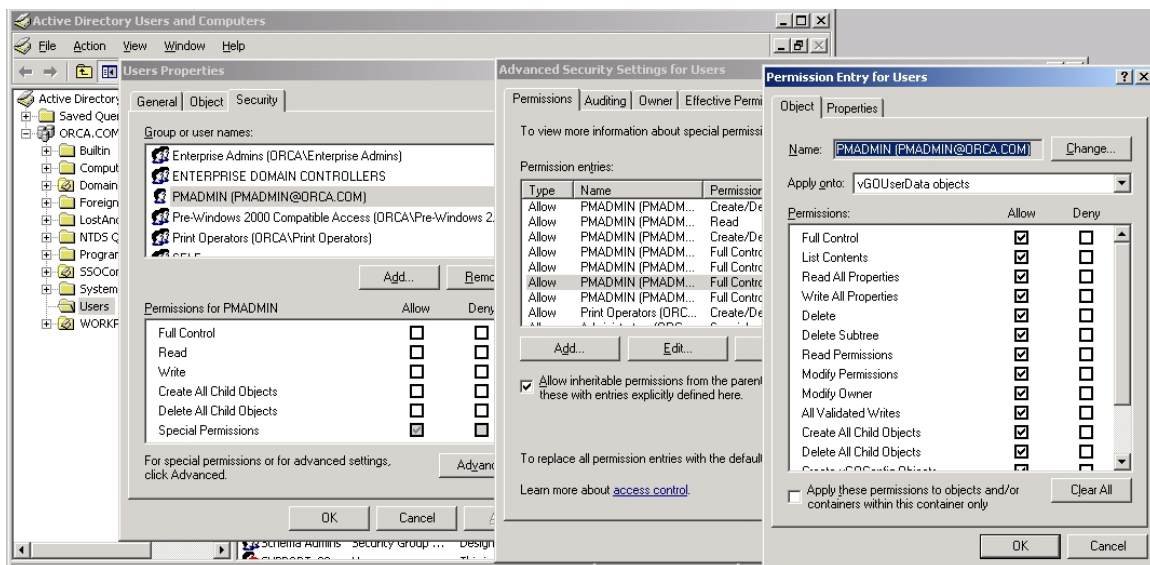


- Grant FULL CONTROL to the PMSERVICE account as it applies to the vGOLocatorClass objects.





- Grant FULL CONTROL to the PMSERVICE account as it applies to the vGOUserData objects.



- Grant FULL CONTROL to the PMSERVICE account as it applies to the vGOSecret objects.

