Oracle® Enterprise Single Sign-on Provisioning Gateway

Minimum Permissions Guide

Release 11.1.1.5.0

E20988-01

March 2011

Oracle Enterprise Single Sign-on Provisioning Gateway, Minimum Permissions Guide, Release 11.1.1.5.0

E20988-01

Table of Contents

Abbreviations and Terminology

Following is a list of commonly-used abbreviations and terminology.

Abbreviation or Terminology	Full Name
Administrative Console	ESSO-LM Administrative Console
Agent	ESSO-LM Agent
FTU	First Time Use Wizard
ESSO-Anywhere	Oracle Enterprise Single Sign-on Anywhere
ESSO-PG	Oracle Enterprise Single Sign-on Provisioning Gateway
ESSO-LM	Oracle Enterprise Single Sign-on Logon Manager
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset
ESSO-UAM	Oracle Enterprise Single Sign-on Universal Authentication Manager

About the ESSO-PG Minimum Permissions Guide

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.

In order to increase security, Oracle now recommends that this service account be created as a member of 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-LM 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.

This guide is intended for experienced administrators and software engineers who are responsible for the installation, configuration, and maintenance of ESSO-PG and Oracle Enterprise Single Sign-on Logon Manager (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-PG Agent through the ESSO-LM Administrative Console.

General Recommendations and Notes

Microsoft recommends that you not install Internet Information Server (IIS) on a Domain Controller. Oracle 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. Oracle recommends that you test these procedures in a non-production environment that resembles your working network as closely as possible.

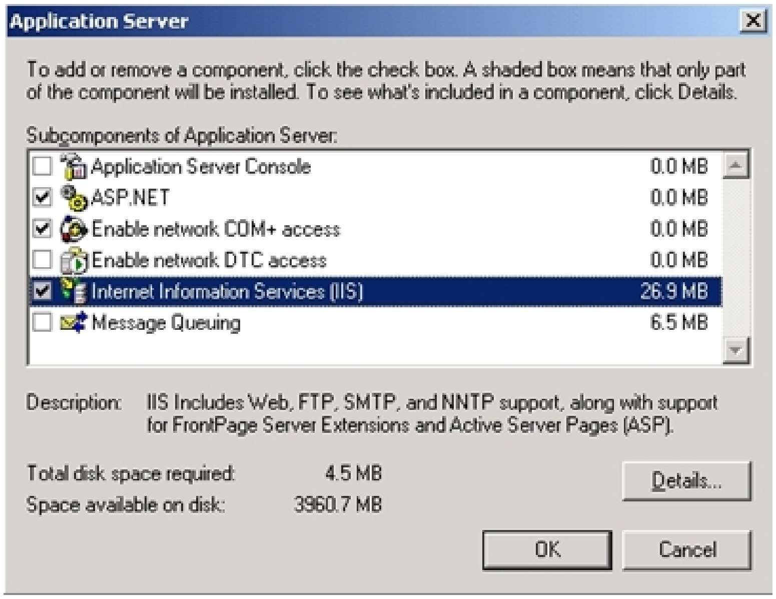
The procedures outlined in this document involve changes that can affect your entire domain. Specialized policies, trust, inheritance issues, and intra- and inter-site replication issues, particularly as they exist in large enterprises, cannot be fully tested outside of the actual environment.

As with any issues that could affect a large number of users, Oracle 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 the 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:



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Application Server:

☐	Application Server Console	0.0 MB
☑	ASP.NET	0.0 MB
☑	Enable network COM+ access	0.0 MB
☐	Enable network DTC access	0.0 MB
☑	Internet Information Services (IIS)	26.9 MB
☐	Message Queuing	6.5 MB

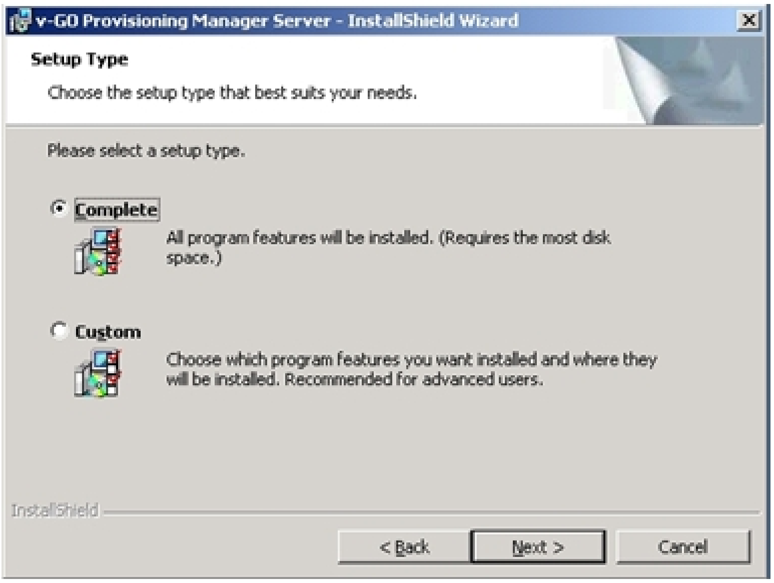
Description: IIS Includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP).

Total disk space required: 4.5 MB

Space available on disk: 3960.7 MB

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

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, select **Complete**.



v-GO Provisioning Manager Server - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● Complete

All program features will be installed. (Requires the most disk space.)

○ Custom

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

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.

Installing ESSO-LM and the ESSO-PG 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-PG client-side components on the workstation where you installed ESSO-PG. Refer to the *ESSO-PG Installation and Setup Guide* for more information.

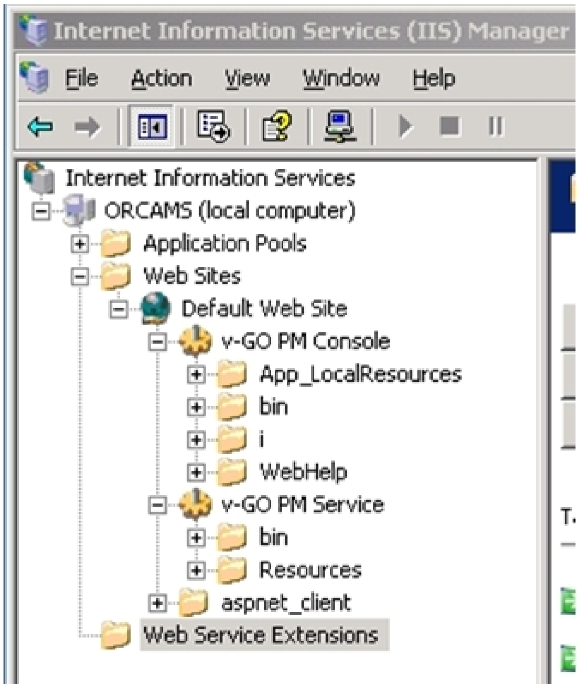
> When you deploy the ESSO-LM Agent to workstations, you must also deploy the ESSO-PG client-side component to each workstation where ESSO-LM will reside.

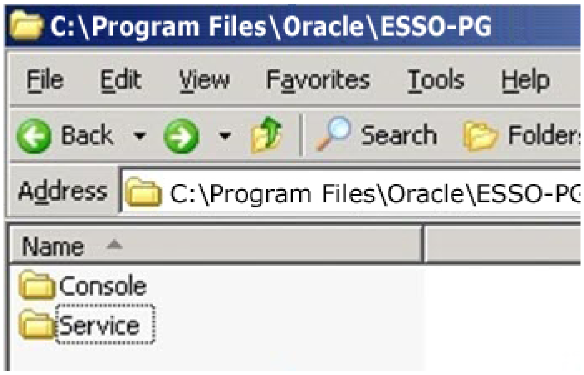
Verifying the ESSO-PG Server-Side Installation

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\Oracle directories on the server.

Examples of these entities are shown in the following illustrations:



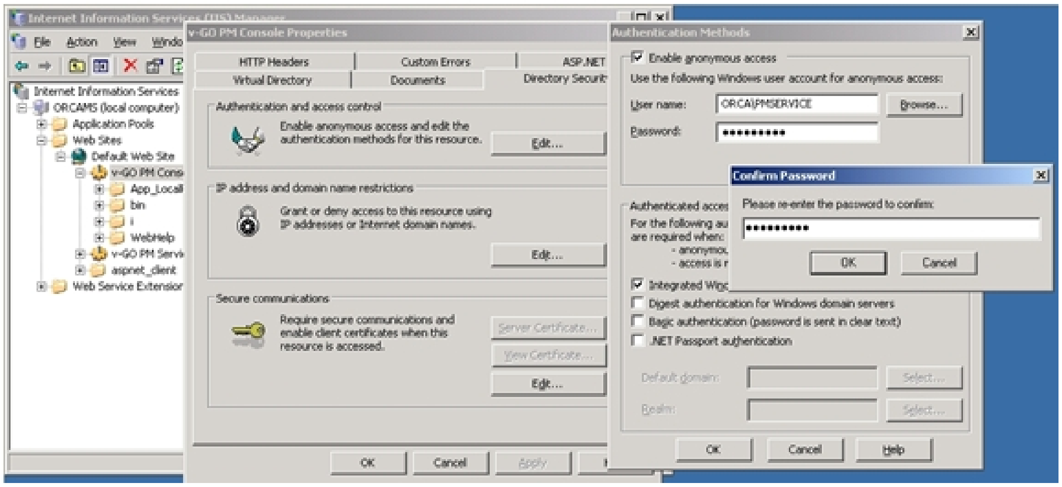


C:\Program Files\Oracle\ESSO-PG
File Edit View Favorites Tools Help
Back Search Folder
Address C:\Program Files\Oracle\ESSO-PG
Name
Console
Service

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 Oracle server-side components.

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



Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or Internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

☑ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: ORCA\PMSERVICE

Password: ••••••••••

Authenticated acces

For the following au are required when:

- anonymou
- access is r

☑ Integrated Wi

☐ Digest authentication for Windows domain servers

☐ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

Default domain:

Realm:

Please re-enter the password to confirm:

••••••••••

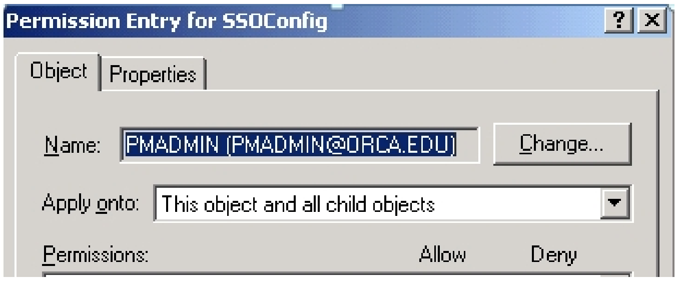
5. From the RUN line, type `iisreset` to restart the IIS service.

Granting Special Permissions to the PMSERVICE Account

The next procedure is to grant special rights to specific containers within Active Directory on a domain controller 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 read-only access to the SSOConfig container (the container where the application templates are stored) as shown in the following illustration:



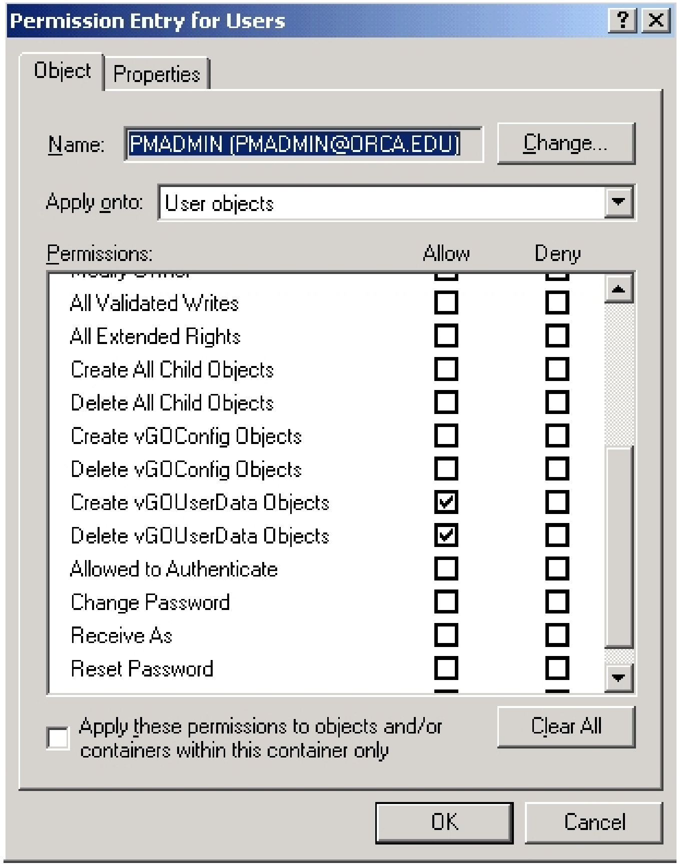
Permission Entry for SSOConfig

Name: PMADMIN (PMADMIN@ORCA.EDU)

Apply onto: This object and all child objects

Steps 2 through 8 must be repeated for each Organizational Unit that exists within your organization that contains users.

2. 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.



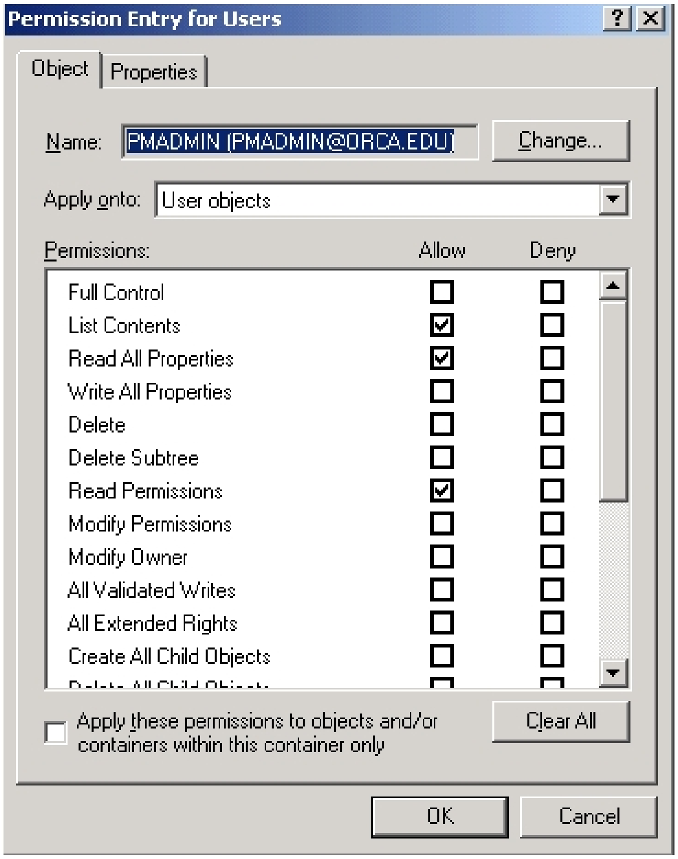
Name: PMADMIN (PMADMIN@ORCA.EDU)

Apply onto: User objects

Permissions:	Allow	Deny
All Validated Writes	□	□
All Extended Rights	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Create vGOConfig Objects	□	□
Delete vGOConfig Objects	□	□
Create vGOUserData Objects	☑	□
Delete vGOUserData Objects	☑	□
Allowed to Authenticate	□	□
Change Password	□	□
Receive As	□	□
Reset Password	□	□

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

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



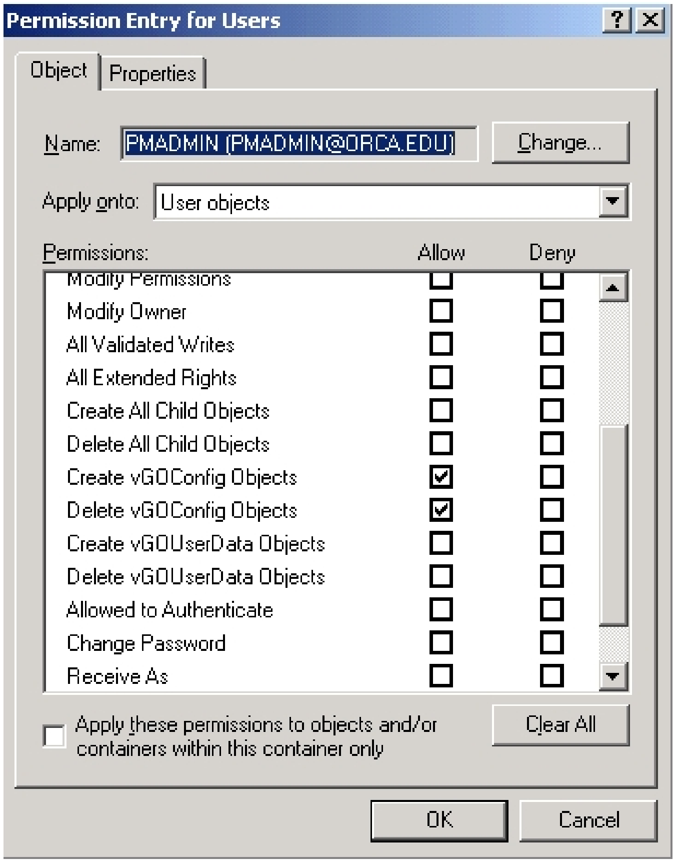
Name: PMADMIN (PMADMIN@ORCA.EDU)

Apply onto: User objects

Permissions:	Allow	Deny
Full Control	□	□
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	□	□

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

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



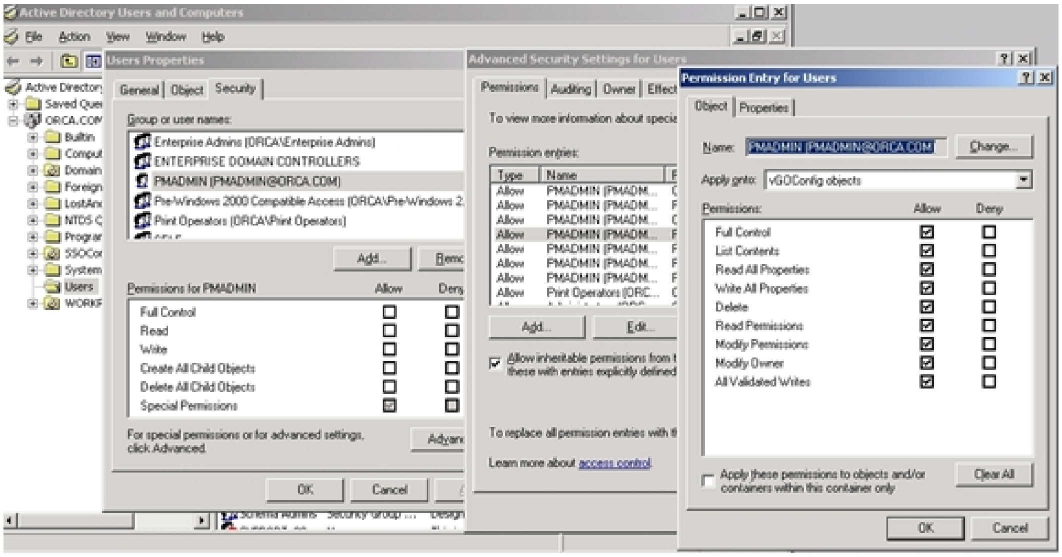
Name: PMADMIN (PMADMIN@ORCA.EDU)

Apply onto: User objects

Permissions:	Allow	Deny
Modify Permissions	□	□
Modify Owner	□	□
All Validated Writes	□	□
All Extended Rights	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Create vGOConfig Objects	☑	□
Delete vGOConfig Objects	☑	□
Create vGOUserData Objects	□	□
Delete vGOUserData Objects	□	□
Allowed to Authenticate	□	□
Change Password	□	□
Receive As	□	□

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

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



Group or user names:

- Enterprise Admins (ORCA\Enterprise Admins)
- ENTERPRISE DOMAIN CONTROLLERS
- PMADMIN (PMADMIN@ORCA.COM)
- Pre-Windows 2000 Compatible Access (ORCA\Pre-Windows 2
- Print Operators (ORCA\Print Operators)

Permissions for PMADMIN	Allow	Deny
Full Control	□	□
Read	□	□
Write	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced.

To view more information about specia

Permission entries:

Type	Name	
Allow	PMADMIN (PMADM...	C
Allow	PMADMIN (PMADM...	F
Allow	PMADMIN (PMADM...	C
Allow	PMADMIN (PMADM...	F
Allow	PMADMIN (PMADM...	F
Allow	PMADMIN (PMADM...	F
Allow	PMADMIN (PMADM...	F
Allow	Print Operators (ORC...	C

☑ Allow inheritable permissions from t these with entries explicitly defined

To replace all permission entries with t

Learn more about access control.

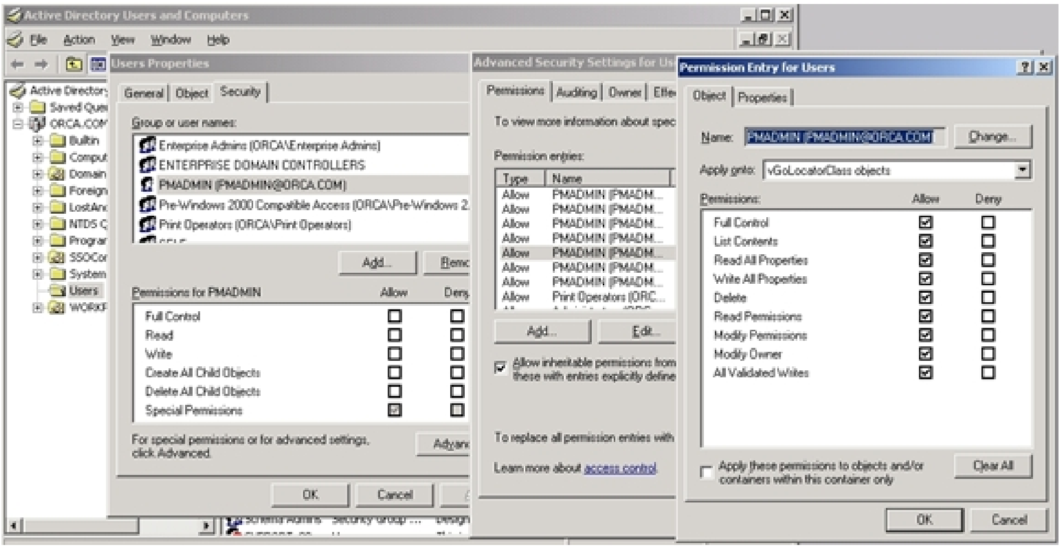
Name: PMADMIN (PMADMIN@ORCA.COM)

Apply onto: vGOConfig objects

Permissions:	Allow	Deny
Full Control	☑	□
List Contents	☑	□
Read All Properties	☑	□
Write All Properties	☑	□
Delete	☑	□
Read Permissions	☑	□
Modify Permissions	☑	□
Modify Owner	☑	□
All Validated Writes	☑	□

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

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



Group or user names:

- Enterprise Admins (ORCA\Enterprise Admins)
- ENTERPRISE DOMAIN CONTROLLERS
- PMADMIN (PMADMIN@ORCA.COM)
- Pre-Windows 2000 Compatible Access (ORCA\Pre-Windows 2
- Print Operators (ORCA\Print Operators)

Permissions for PMADMIN

	Allow	Deny
Full Control	☐	☐
Read	☐	☐
Write	☐	☐
Create All Child Objects	☐	☐
Delete All Child Objects	☐	☐
Special Permissions	☑	☐

For special permissions or for advanced settings, click Advanced.

To view more information about spec

Permission entries:

Type	Name
Allow	PMADMIN (PMADM...
Allow	PMADMIN (PMADM...
Allow	PMADMIN (PMADM...
Allow	PMADMIN (PMADM...
Allow	PMADMIN (PMADM...
Allow	PMADMIN (PMADM...
Allow	PMADMIN (PMADM...
Allow	Print Operators (ORC...

☑ Allow inheritable permissions from these with entries explicitly define

To replace all permission entries with

Learn more about access control.

Name: PMADMIN (PMADMIN@ORCA.COM)

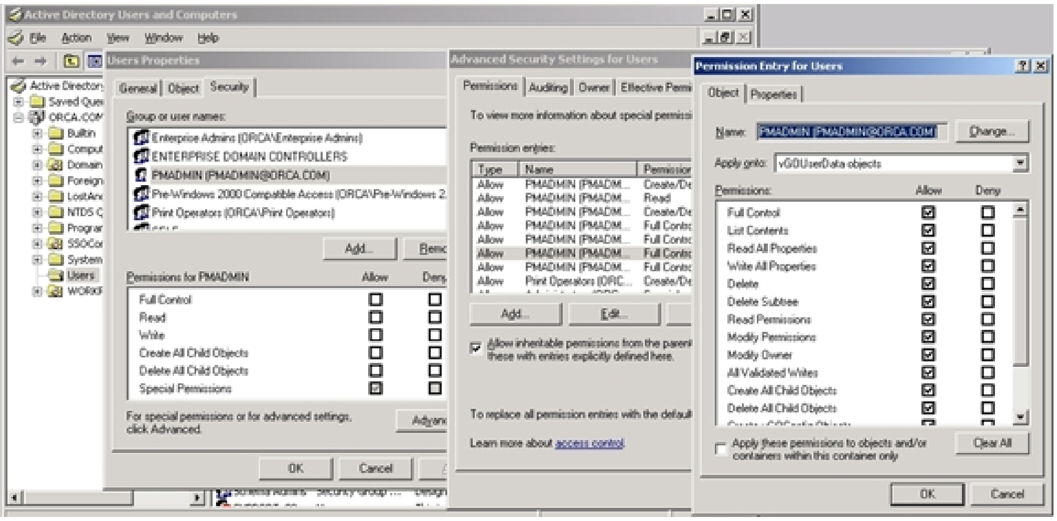
Apply onto: vGoLocatorClass objects

Permissions:

	Allow	Deny
Full Control	☑	☐
List Contents	☑	☐
Read All Properties	☑	☐
Write All Properties	☑	☐
Delete	☑	☐
Read Permissions	☑	☐
Modify Permissions	☑	☐
Modify Owner	☑	☐
All Validated Writes	☑	☐

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

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



Group or user names:

- Enterprise Admins (ORCA\Enterprise Admins)
- ENTERPRISE DOMAIN CONTROLLERS
- PMADMIN (PMADMIN@ORCA.COM)
- Pre-Windows 2000 Compatible Access (ORCA\Pre-Windows 2
- Print Operators (ORCA\Print Operators)

Permissions for PMADMIN

	Allow	Deny
Full Control	☐	☐
Read	☐	☐
Write	☐	☐
Create All Child Objects	☐	☐
Delete All Child Objects	☐	☐
Special Permissions	☑	☐

For special permissions or for advanced settings, click Advanced.

To view more information about special permissi

Permission entries:

Type	Name	Permission
Allow	PMADMIN (PMADM...	Create/De
Allow	PMADMIN (PMADM...	Read
Allow	PMADMIN (PMADM...	Create/De
Allow	PMADMIN (PMADM...	Full Contr
Allow	PMADMIN (PMADM...	Full Contr
Allow	PMADMIN (PMADM...	Full Contr
Allow	PMADMIN (PMADM...	Full Contr
Allow	Print Operators (ORC...	Create/De

☑ Allow inheritable permissions from the parent these with entries explicitly defined here.

To replace all permission entries with the defaul

Learn more about access control.

Name: PMADMIN (PMADMIN@ORCA.COM)

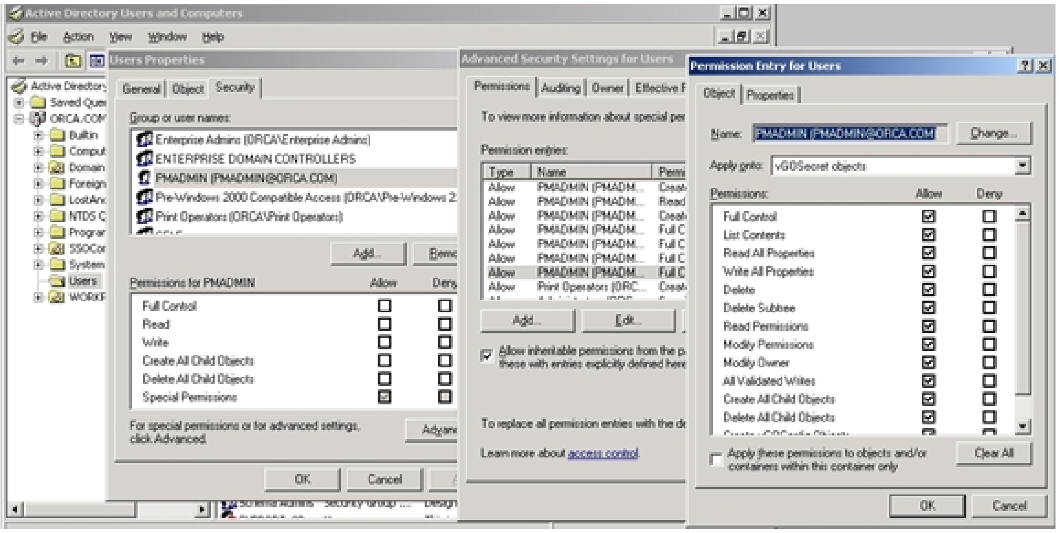
Apply onto: vGOUserData objects

Permissions:

	Allow	Deny
Full Control	☑	☐
List Contents	☑	☐
Read All Properties	☑	☐
Write All Properties	☑	☐
Delete	☑	☐
Delete Subtree	☑	☐
Read Permissions	☑	☐
Modify Permissions	☑	☐
Modify Owner	☑	☐
All Validated Writes	☑	☐
Create All Child Objects	☑	☐
Delete All Child Objects	☑	☐

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

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



Users Properties

General | Object | Security

Group or user names:

- Enterprise Admins (ORCA\Enterprise Admins)
- ENTERPRISE DOMAIN CONTROLLERS
- PMADMIN (PMADMIN@ORCA.COM)
- Pre-Windows 2000 Compatible Access (ORCA\Pre-Windows 2
- Print Operators (ORCA\Print Operators)

Permissions for PMADMIN	Allow	Deny
Full Control	□	□
Read	□	□
Write	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced.

Advanced Security Settings for Users

Permissions | Auditing | Owner | Effective F

To view more information about special per

Permission entries:

Type	Name	Permi
Allow	PMADMIN (PMADM...	Creat
Allow	PMADMIN (PMADM...	Read
Allow	PMADMIN (PMADM...	Creat
Allow	PMADMIN (PMADM...	Full C
Allow	PMADMIN (PMADM...	Full C
Allow	PMADMIN (PMADM...	Full C
Allow	PMADMIN (PMADM...	Full C
Allow	Print Operators (ORC...	Creat

☑ Allow inheritable permissions from the p these with entries explicitly defined here

To replace all permission entries with the de

Learn more about access control.

Permission Entry for Users

Object | Properties

Name: PMADMIN (PMADMIN@ORCA.COM)

Apply onto: vGOSecret objects

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

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

Granting Provisioning Rights to Domain Users

If you want regular domain users (users who do not have administrative permissions to the AD repository) to have the ability to provision other users, you must create a security group for them in AD. Grant permissions to this new group as outlined in this manual. Add to this group the names of any users you want to enable to view provisioning activity using the PM Console.

> The ESSO-PG Service User account should be included in this security group by default.

For details on creating user groups, see the ESSO-PG *Administrator Guide*.