# Oracle® Enterprise Single Sign-on Provisioning Gateway

Installation and Setup Guide

Release 11.1.1.2.0

**E15699-02**

Novmber 2010

Oracle Enterprise Single Sign-on Provisioning Gateway, Installation and Setup Guide, Release 11.1.1.2.0

E15699-02

# Table of Contents

Abbreviations and Terminology 4
About ESSO-PG 5
Installation Overview 6
Installing the Server 7
Installing the Server on Windows Server 2008 8
Before Installing the ESSO-PG Server 8
After Installing the ESSO-PG Server 9
Configuring a 64-bit OS to Run ESSO-PG Server 10
Creating or Identifying a User Account for Anonymous Logon 12
Give the IIS Anonymous Account Access to ADAM 12
Give the ASPNET Account Additional Privileges 13
Granting Provisioning Rights to Domain Users 14
Enabling SSL 15
Configuring Syslog 20
Installing the Client CLI 21
Installing Support for the Agent 22
Setting the CycleInterval Registry Key 22
Upgrade Notes 24
ESSO-PG Server 24
ESSO-PG Agent 24
Uninstalling ESSO-PG 25
Reference and Troubleshooting 26
Customization Notes 26
Installation and Configuration Notes 26

# 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-AM | Oracle Enterprise Single Sign-on Authentication Manager |
| ESSO-ODE | Oracle Enterprise Single Sign-on On Demand Edition |
| ESSO-PG | Oracle Enterprise Single Sign-on Provisioning Gateway |
| ESSO-KM | Oracle Enterprise Single Sign-on Kiosk Manager |
| ESSO-LM | Oracle Enterprise Single Sign-on |
| ESSO-PR | Oracle Enterprise Single Sign-on Password Reset |

# About ESSO-PG

Oracle Enterprise Single Sign-on Provisioning Gateway (ESSO-PG) enables an administrator to automatically provision ESSO-LM with a user’s ID and password by using a provisioning system.

An administrator is able to add, modify, and delete IDs and passwords for particular applications within the provisioning system and have the changes reflected in ESSO-LM. From the provisioning system, an administrator can delete all usernames and passwords inside of ESSO-LM so that a user’s access to all protected applications is eliminated.

This guide describes the ESSO-PG functionality and provides instructions for installation and configuration.

This guide is intended for experienced administrators responsible for the planning, implementation, and deployment of ESSO-PG. Administrators are expected to understand single sign-on concepts and be familiar with Internet Information Services, Windows Registry settings, and the ESSO-LM Administrative Console. Persons completing the installation and configuration procedure should also be familiar with their company’s system standards.

# Installation Overview

ESSO-PG is installed as an add-on component to Oracle Enterprise Single Sign-on (ESSO-LM). ESSO-LM must be installed prior to installing ESSO-PG. ESSO-LM automatically recognizes ESSO-PG when it is installed. The following list contains the procedures that must be followed to successfully install ESSO-PG.

Before you begin the installation and configuration process, carefully review the system requirements and verify that your system meets those requirements.

There are several procedures that you must complete to install and configure ESSO-PG:

- Installing the Server
- Creating or identifying a User Account for Anonymous Logon
- Enabling SSL
- Installing the Client CLI
- Installing support for the Agent

If you are upgrading from an earlier version of ESSO-PG, refer to the Upgrade Notes.

# Installing the Server

To install and configure the ESSO-PG Server:

1. Close all programs.
2. Insert the installation CD in your CD-ROM drive (or start the installation from a shared network drive).
3. In the \Server folder, double-click the Server file. Wait while the installer loads.
4. On the Welcome Panel, click **Next**.
5. On the Customer Agreement screen, enter your user name, organization name, and select who to **Install this application for**: **All Users** or **Only for you**. Click **Next**.
6. On the Setup Type screen, select **Complete** or **Custom**. **Complete** installs all program files. **Custom** allows you to choose which program files are installed and where they are installed. Custom installations are only recommended for advanced users. Click **Next**.
7. ESSO-PG is ready to be installed. Click **Install**. Wait for the installation to complete. When it is done, click **Finish**.

# Installing the Server on Windows Server 2008

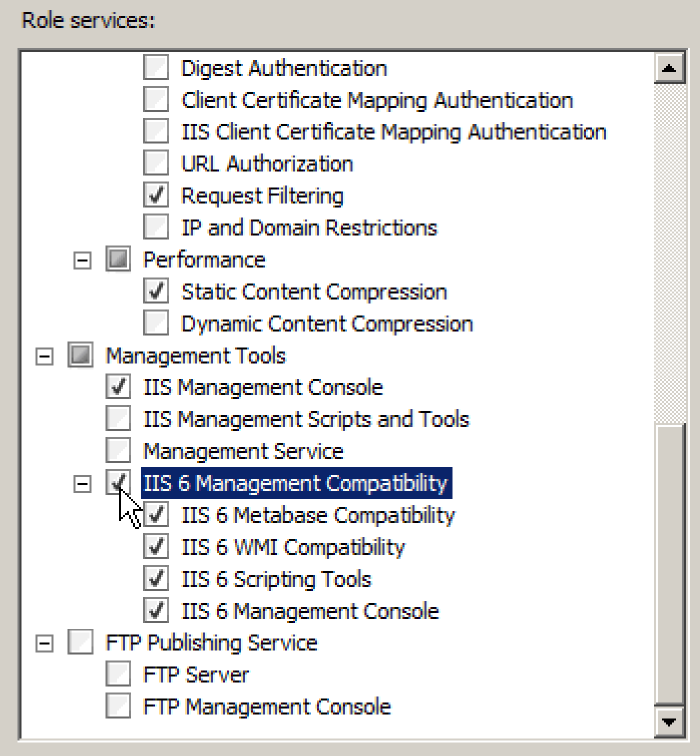
If you are installing the ESSO-PG Server on a Windows 2008 machine, you need to take some extra steps to ensure that the server installs and runs properly.

## Before Installing the ESSO-PG Server

Because Windows 2008 uses a newer version of IIS (Internet Information Services), you must turn on IIS compatibility mode for the previous version of IIS if you are installing the ESSO-PG Server on a Windows 2008 Server machine.

To add the IIS 6 Management Compatibility role service to IIS:

1. Start your Windows 2008 Server.
2. From the Initial Configuration Tasks screen, under **Customize This Server**, click **Add Roles**.
3. In the Roles window, select **Web Server (IIS)**; click **Next**.
4. In the Role services window, select the **Windows Authentication** service under Web Server > Security.
5. In the Role services window, scroll down and select **IIS 6 Management Compatibility**.



Role services:

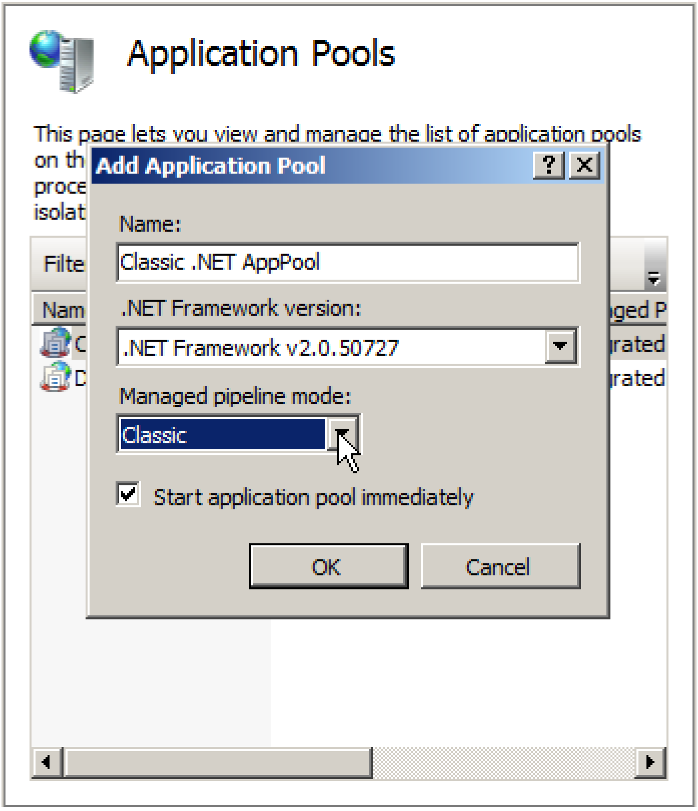
- ☐ Digest Authentication
- ☐ Client Certificate Mapping Authentication
- ☐ IIS Client Certificate Mapping Authentication
- ☐ URL Authorization
- ☑ Request Filtering
- ☐ IP and Domain Restrictions
- ⊟ ▣ Performance
  - ☑ Static Content Compression
  - ☐ Dynamic Content Compression
- ⊟ ▣ Management Tools
  - ☑ IIS Management Console
  - ☐ IIS Management Scripts and Tools
  - ☐ Management Service
  - ⊟ ☑ IIS 6 Management Compatibility
    - ☑ IIS 6 Metabase Compatibility
    - ☑ IIS 6 WMI Compatibility
    - ☑ IIS 6 Scripting Tools
    - ☑ IIS 6 Management Console
- ⊟ ☐ FTP Publishing Service
  - ☐ FTP Server
  - ☐ FTP Management Console

6. Click **Next**.
7. From the Confirmation screen of the Add Roles wizard, click **Install**.
8. After configuring IIS 6 Management Compatibility, install the ESSO-PG Server. See "Installing the Server" on page 7.)

## After Installing the ESSO-PG Server

Now you need to create a new App Pool and move your ESSO-PG Console and ESSO-PG Service into it.

1. Go to **Programs** > **Administrative Tools** > **IIS**. From the IIS Manager, select **2008SRV-STD** > **Application Pools**.
2. Right-click **Application Pools** and select **Add Application Pool...** from the drop-down menu.
3. For the name of the new app pool, enter **Classic .Net App Pool**. From the Managed Pipeline Mode field drop-down menu, select **Classic**.



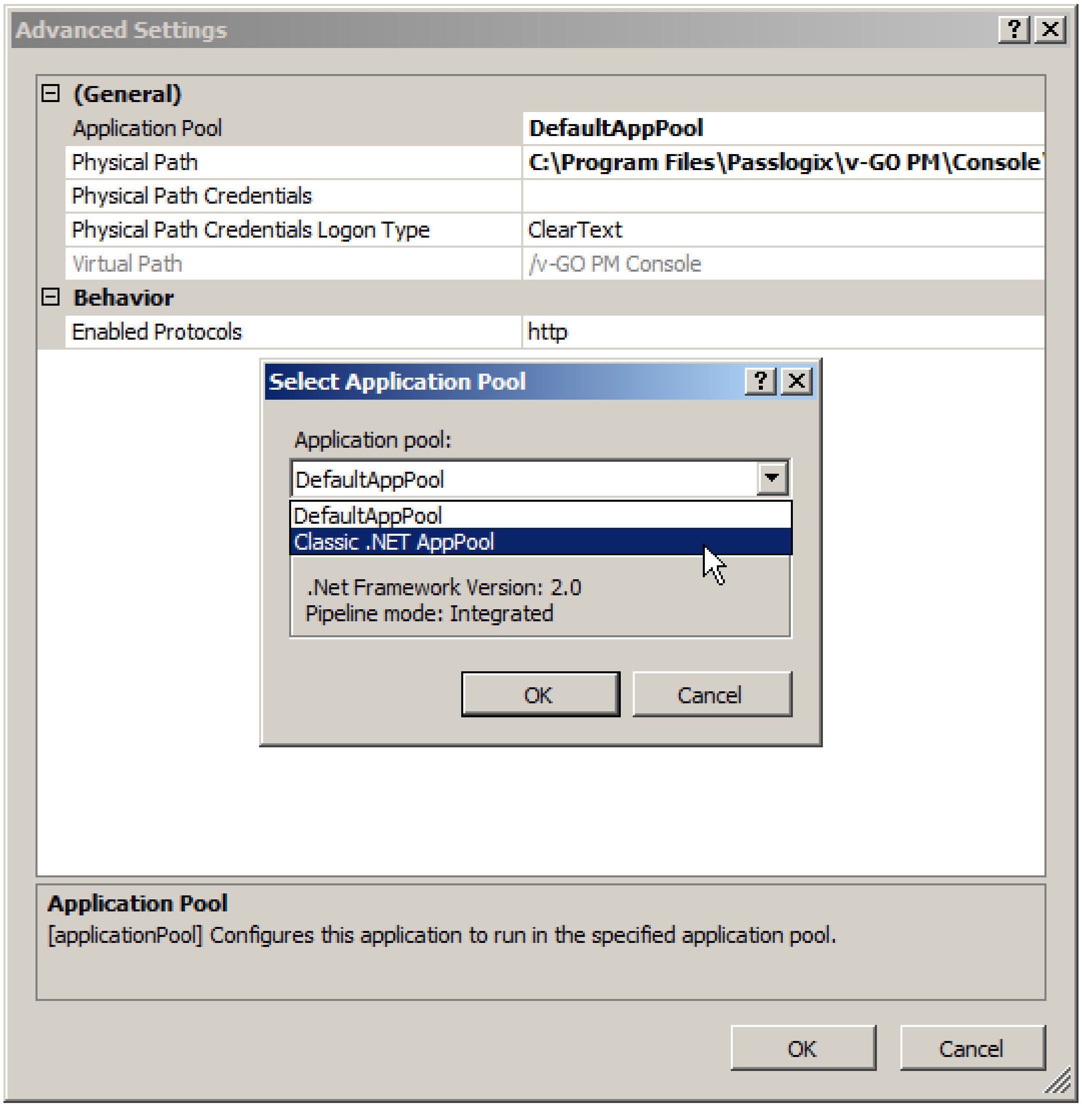
Name: Classic .NET AppPool

.NET Framework version: .NET Framework v2.0.50727

Managed pipeline mode: Classic

☑ Start application pool immediately

4. Return to **2008SRV-STD** >**Sites**>**Default Web Site** and right-click **ESSO-PGConsole**.
5. Select **Manage Application** >**Advanced Settings**. In the Advanced Settings window, select **Application Pool**. In the Select Application Pool window, select **Classic .NET AppPool**.



| | |
|---|---|
| **(General)** | |
| Application Pool | **DefaultAppPool** |
| Physical Path | **C:\Program Files\Passlogix\v-GO PM\Console** |
| Physical Path Credentials | |
| Physical Path Credentials Logon Type | ClearText |
| Virtual Path | /v-GO PM Console |
| **Behavior** | |
| Enabled Protocols | http |

Application pool:

DefaultAppPool

DefaultAppPool<br>
Classic .NET AppPool

.Net Framework Version: 2.0<br>
Pipeline mode: Integrated

**Application Pool**

[applicationPool] Configures this application to run in the specified application pool.

6. Click **OK**.
7. Follow the same steps to move the ESSO-PG Service into the Classic .NET App Pool.

> For all Web Services using .NET and IIS, where .NET is installed before IIS is configured, you must run the command "aspnet_regiis –i from the command prompt after you have completed all of the other steps. (The aspnet_regiis tool is located in "%WINDIR%\Microsoft.NET\Framework\v2.0.50727.)

## Configuring a 64-bit OS to Run ESSO-PG Server

On a 64-bit Windows 2003 Server, you need to enable IIS 6.0 to run 32-bit applications. To do so:

1. Open a command prompt and navigate to the %systemdrive%\Inetpub\AdminScripts directory.
2. Type the following command:

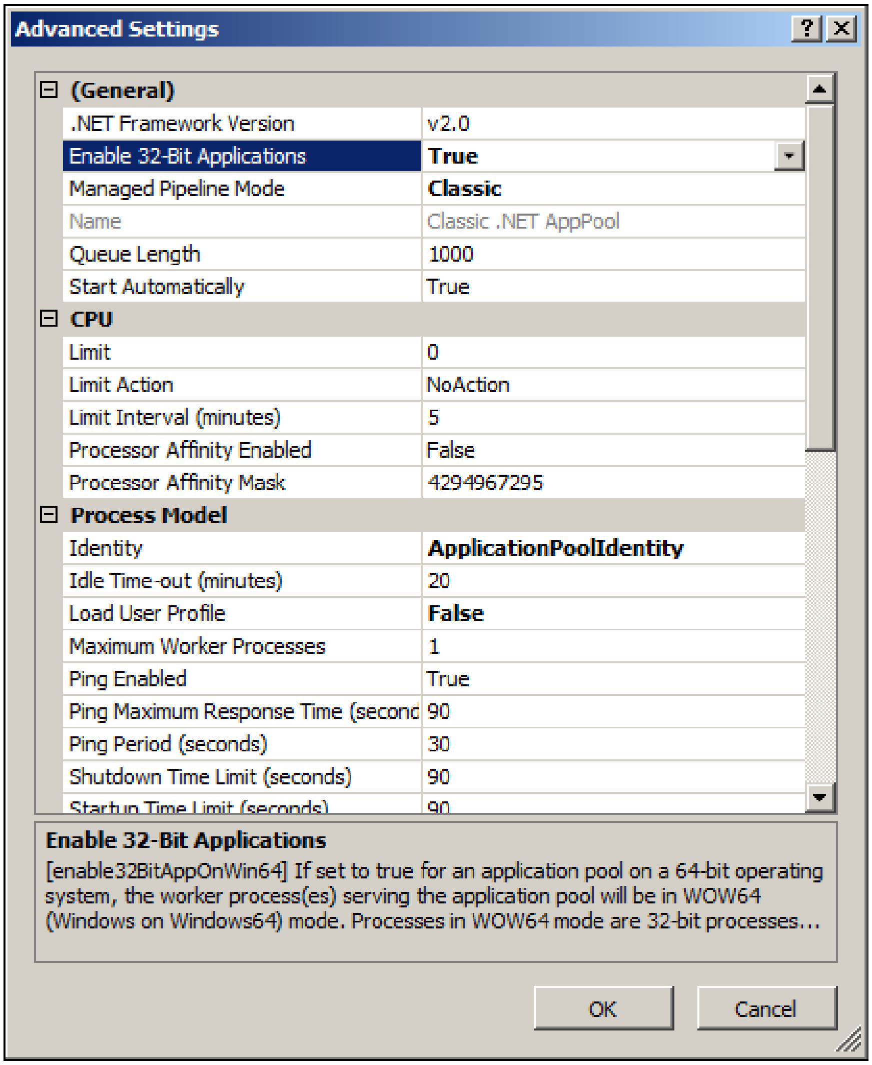
```
cscript.exe adsutil.vbs set W3SVC/AppPools/Enable32BitAppOnWin64 "true"
```

3. Press ENTER.
4. Restart IIS.

These steps should be done after installing the ESSO-PG Server.

On a 64-bit Windows 2008 Server, you need to enable running 32-bit applications for the Classic .NET Application Pool:

1. Open Internet Information Services (IIS) Manager.
2. Click **Application Pools**.
3. Right-click **Classic .NET AppPool** and select **Advanced Settings...**
4. Change "Enable 32-bit Applications" settings to **True**.
5. Click OK.



Advanced Settings

| | |
|---|---|
| ⊟ **(General)** | |
| .NET Framework Version | v2.0 |
| Enable 32-Bit Applications | **True** |
| Managed Pipeline Mode | **Classic** |
| Name | Classic .NET AppPool |
| Queue Length | 1000 |
| Start Automatically | True |
| ⊟ **CPU** | |
| Limit | 0 |
| Limit Action | NoAction |
| Limit Interval (minutes) | 5 |
| Processor Affinity Enabled | False |
| Processor Affinity Mask | 4294967295 |
| ⊟ **Process Model** | |
| Identity | **ApplicationPoolIdentity** |
| Idle Time-out (minutes) | 20 |
| Load User Profile | **False** |
| Maximum Worker Processes | 1 |
| Ping Enabled | True |
| Ping Maximum Response Time (seconc | 90 |
| Ping Period (seconds) | 30 |
| Shutdown Time Limit (seconds) | 90 |
| Startup Time Limit (seconds) | 90 |

**Enable 32-Bit Applications**

[enable32BitAppOnWin64] If set to true for an application pool on a 64-bit operating system, the worker process(es) serving the application pool will be in WOW64 (Windows on Windows64) mode. Processes in WOW64 mode are 32-bit processes...

6. Restart IIS.

# Creating or Identifying a User Account for Anonymous Logon

You must create or identify a dedicated Anonymous User account through which ESSO-PG users and administrators access ESSO-PG Web Services. This Anonymous User account should be a member of the Administrators group.

> Because the default Anonymous User account in IIS, IUSR_MACHINE_NAME, is not a member of the Administrator group, you must create or choose a domain user account that is an Administrator; this will allow the account to perform the following tasks:
>
> - Change which Web service account to use from the management console
> - Read from and write to the directory service (if AD or ADAM)
> - Write to the local-machine registry IHKLM).
>
> To create a new user account or assign Administrator rights to an existing account, use the Active Directory Users and Computers console (for an Active Directory domain) or the Computer Management console (for non-AD domains)

The user account you create or choose is specified as the Anonymous User dialog of the Services tool during this step.

### If you are using Windows 2008:

1. Launch the Microsoft IIS Manager.
2. In the left-hand tree, drill down to ***<Server>*** > ***Sites*** > ***Default Web Site*** and select the ESSO-PG Console site node.
3. In the IIS section of the center pane, double-click **Authentication**.
4. In the Authentication pane, right-click **Anonymous Authentication** and select **Edit**.
5. In the dialog box that appears, select **Specific User** and click **Set**.
6. In the dialog box that appears, enter the name of the anonymous access user account in the <DOMAIN>\<user> form, and the appropriate password, then click **OK**.
7. Click **OK** in the Edit Anonymous Access… dialog to dismiss it.
8. Repeat steps 2-7 for the ESSO-PG Service site.
9. When you have finished, restart Microsoft IIS to apply your changes.

### If you are using Windows 2003:

1. Launch the Microsoft IIS Manager.
2. Locate the ESSO-PG Console node in the tree, right-click on it, and click **Properties**.
3. Click the **Directory Security** tab and click the **Edit** button next to **Anonymous Access**
4. Mark the **Anonymous Access** checkbox and enter the username and password of the anonymous user. The anonymous user must have local administrative access.

> By default, the ESSO-PG Management Console is not restricted. Any user with a credential in the backend storage can log in. If you want to restrict access to a particular group, please see the Additional Security Settings in the ESSO-PG Administrator Guide.

## Give the IIS Anonymous Account Access to ADAM

> This step only applies to ADAM users. Use the account chosen in Step 4 above.

1. Click **Start**, point to **Program Files**, point to **ADAM**, and then click **ADAM Tools Command Prompt**.
2. Enter:

   ```
   dsacls [\\SERVER:PORT\DISTINGUISHED_NAME] /g [USER]:ga /i:t"
   ```

   For example:

   ```
   dsacls \\localhost:50000\ou=pm,dc=passlogix,dc=com /g PLX\PMWeb:ga
   /i:t
   ```

3. To verify that the account was given access, type:

   ```
   dsacls \\SERVER:PORT\DISTINGUISHED_NAME
   ```

   The output shows the security information for the directory object. The Anonymous Account should appear in the list with full access.

## Give the ASPNET Account Additional Privileges

> The following step is for Windows 2000 users only.

You must give ASPNET the "Act as part of the operating system" privilege:

1. Open the MMC console by clicking **Start** > **Run**. Type `mmc` and then click **OK**. The Microsoft Management Console opens.
2. On the File menu, click **Add/Remove Snap-in**.
3. On the Standalone tab, click **Add**.
4. In the Add Standalone Snap-in dialog, highlight **Group Policy** and click **Add**.
5. On the Group Policy dialog, select **Local Compute**r and click **Finish**. Click **OK**.

> If you are installing the ESSO-PG Console on a workstation that is a domain controller, instead of selecting Local Computer, click Browse and search for Default Domain Controller Policy. When you complete the next step in the procedure, Default Domain Controller Policy will be displayed in the MMC instead of Local Computer Policy.

6. In the MMC, click the + sign to expand **Local Computer Policy** and continue expanding **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies**. Double-click on **User Rights Assignment**.
7. Double-click **Act** as part of the operating system and click the **Add User or Group** button.
8. Select the ASPNET account and click **OK**. Click **OK** again.

# 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 the *ESSO-PG Minimum Permissions Guide*. Add to this group the names of any users you want to enable to view provisioning activity using the ESSO-PG 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*.

# Enabling SSL

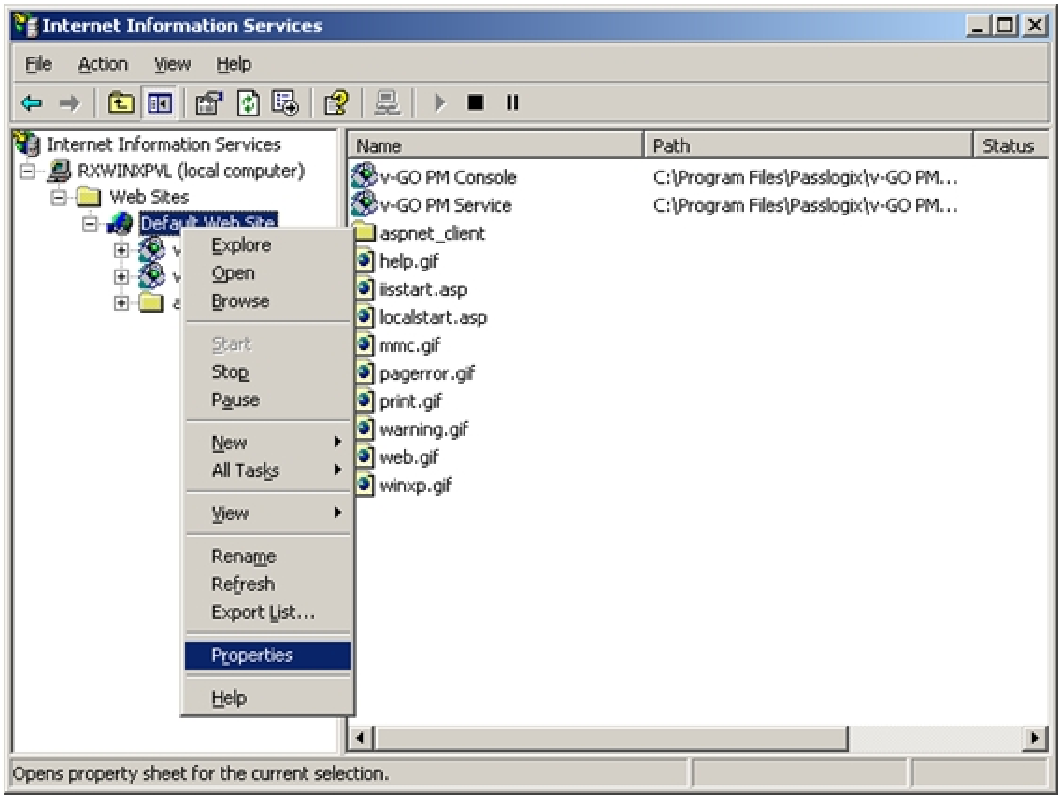
An X.509 Certificate for SSL must be obtained from a trusted certificate authority. This trusted CA must be installed in the list of trusted Root CAs.

The certificate must be valid for the current date and must contain the name of the Web site (machine name).

The following instructions assume that these certificates are available at known locations.

> The following articles from the Microsoft Web site can be referred to for information on installing certificates and setting up SSL:
>
> "How to: Obtain an X.509 Certificate” http://msdn2.microsoft.com/en-us/library/ms819929.aspx
>
> “How to: Set Up SSL on a Web Server” http://msdn2.microsoft.com/en-us/library/aa302411.aspx
>
> If you use Microsoft Certificate Services to obtain the X.509 certificate, choose a Server Authentication Certificate. Also, enable the **Mark keys as exportable** and **Use local machine store** options under the **Key Options** section.

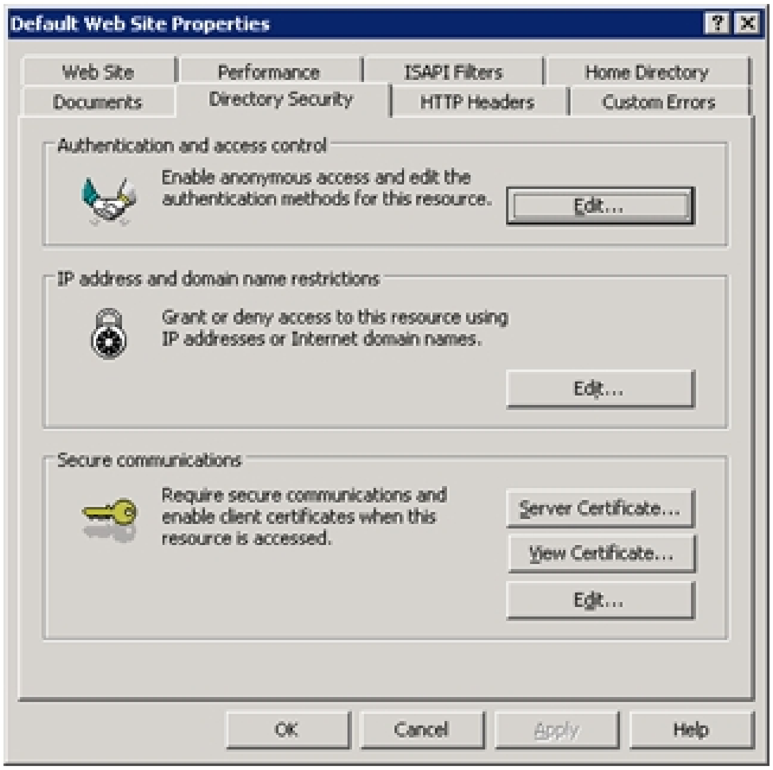
1. Go to **Control Panel** > **Internet Information Services**. Right-click **Default Web Site**. Select **Properties**.



| Name | Path | Status |
|---|---|---|
| v-GO PM Console | C:\Program Files\Passlogix\v-GO PM... | |
| v-GO PM Service | C:\Program Files\Passlogix\v-GO PM... | |
| aspnet_client | | |
| help.gif | | |
| iisstart.asp | | |
| localstart.asp | | |
| mmc.gif | | |
| pagerror.gif | | |
| print.gif | | |
| warning.gif | | |
| web.gif | | |
| winxp.gif | | |

Opens property sheet for the current selection.

2. Click the **Directory Security** tab and under **Secure Communications**, click **Server Certificate**.



Authentication and access control

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

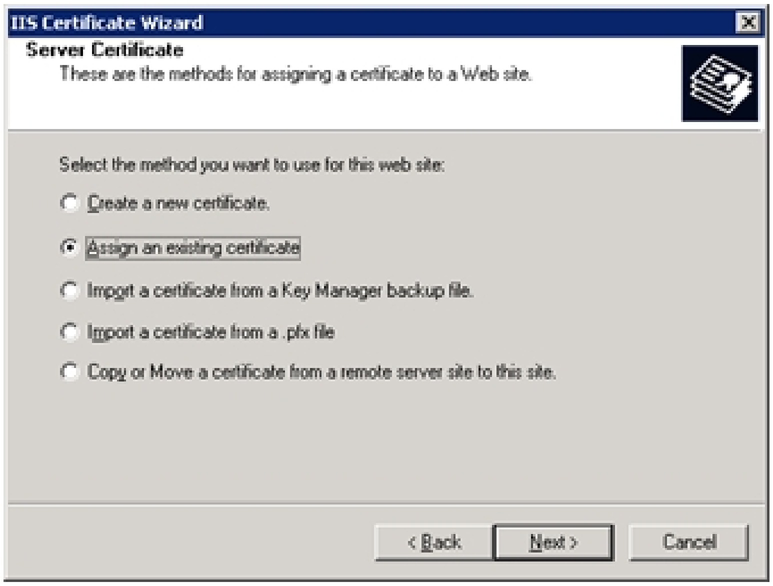
IP address and domain name restrictions

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.

3. The Web Server Certificate Wizard opens. This is where you generate a request for a certificate. Click **Next**.
4. Select **Assign an existing certificate** and click **Next**.



Server Certificate

These are the methods for assigning a certificate to a Web site.

Select the method you want to use for this web site:

○ Create a new certificate.

● Assign an existing certificate

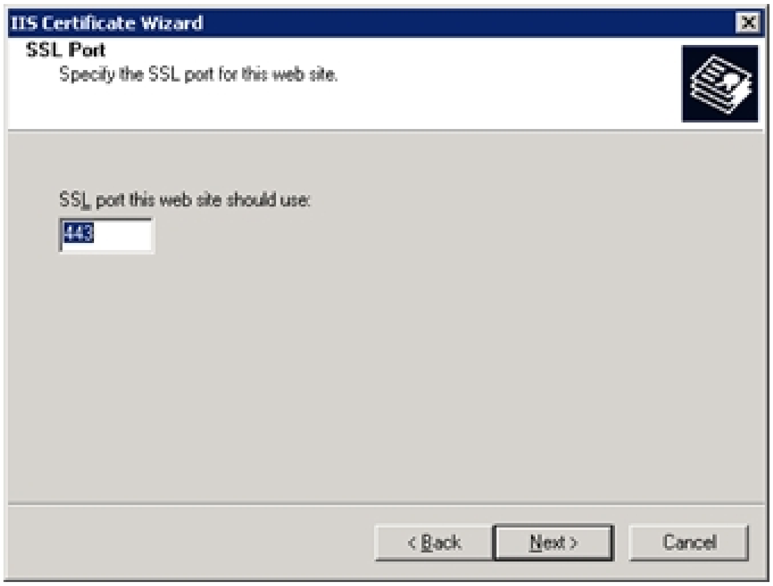
○ Import a certificate from a Key Manager backup file.

○ Import a certificate from a .pfx file

○ Copy or Move a certificate from a remote server site to this site.

5. Highlight the certificate to assign and click **Next**.

6. The default SSL port is 443. Accept the default and click **Next**.



IIS Certificate Wizard

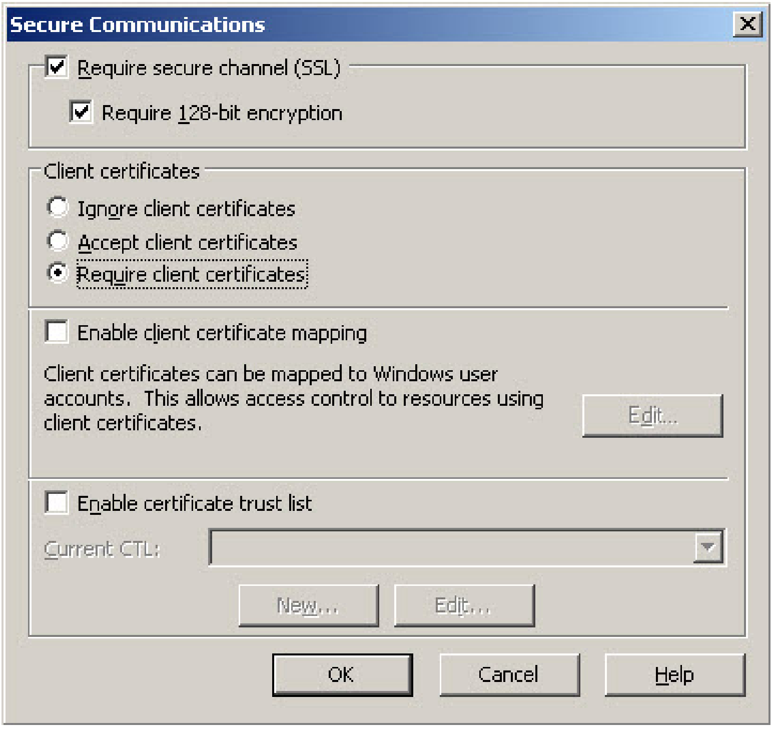
SSL Port

Specify the SSL port for this web site.

SSL port this web site should use:

443

7. Review the summary of your request. Click **Next**.
8. Click **Finish**.
9. The Directory Security tab will still be open. Under **Secure Communications**, click **Edit**.
10. In the Secure Communications dialog box, check **Require secure channel (SSL)** and **Require 128-bit encryption**. Click **OK** to close the dialog.



Secure Communications

☑ Require secure channel (SSL)

☑ Require 128-bit encryption

Client certificates

○ Ignore client certificates

○ Accept client certificates

● Require client certificates

☐ Enable client certificate mapping

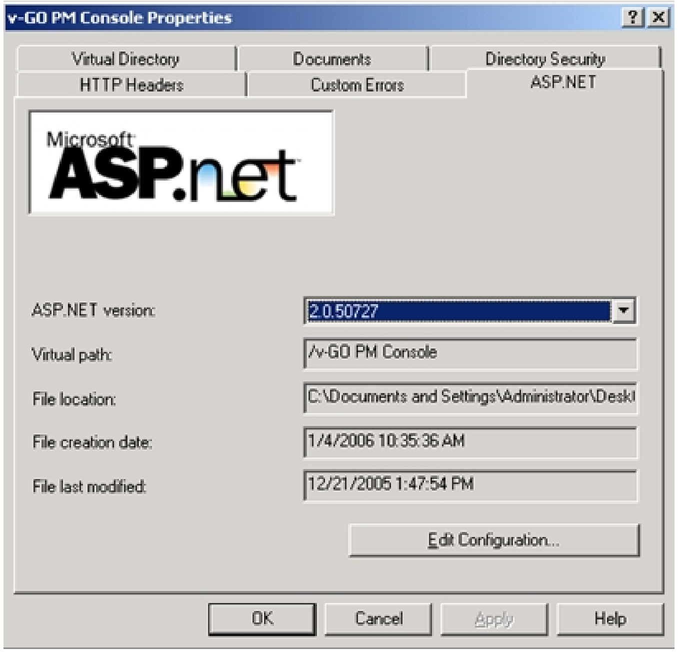
Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

☐ Enable certificate trust list

Current CTL:

11. On the Internet Information Services Tree (see screen following step 1), select ESSO-PG Console. Right-click and select **Properties**. To enable SSL for the Console, repeat steps 2 through 10. The next two steps ensure that the Console can communicate with the Web service.

12. Select the ASP.NET tab (on the ESSO-PG Console Properties dialog box). Verify that the ASP.NET version is set to 2.0.x. (If it is not set to 2.0, change the setting, then click **Apply**). Click **Edit Configuration**.



ASP.NET version: 2.0.50727

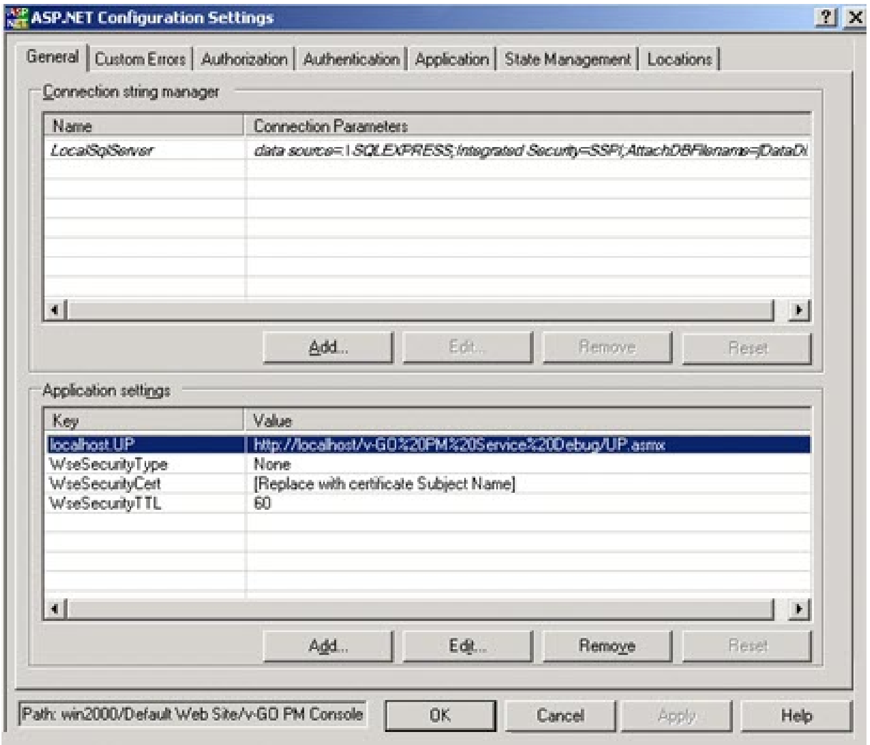
Virtual path: /v-GO PM Console

File location: C:\Documents and Settings\Administrator\Deskt

File creation date: 1/4/2006 10:35:36 AM

File last modified: 12/21/2005 1:47:54 PM

13. Under Application Settings, select **localhost.UP** and click **Edit**.



| Name | Connection Parameters |
|---|---|
| *LocalSqlServer* | *data source=.\SQLEXPRESS;Integrated Security=SSPI;AttachDBFilename=\|DataDi* |

| Key | Value |
|---|---|
| localhost.UP | http://localhost/v-GO%20PM%20Service%20Debug/UP.asmx |
| WseSecurityType | None |
| WseSecurityCert | [Replace with certificate Subject Name] |
| WseSecurityTTL | 60 |

Path: win2000/Default Web Site/v-GO PM Console

14. In the **Value** field, change the prefix of the URL to **https**. The console will now communicate over SSL with the Web service.

# Configuring Syslog

After ESSO-PG installation is complete, you must configure Syslog:

1. Click on the **Settings** option, then click on the **Event Log**.
2. From the **Database Type** drop-down list, select **Syslog Daemon**.
3. Click **Save Changes**.

Complete the following Registry changes:

1. Open regedit and navigate to the following location:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\Extensions\EventManager\Syslog
   ```

2. Enter the IP address of your Syslog server in the RemoteAddress key.

> If you are using a non-standard Syslog port, enter the correct port number of your Syslog server in the RemotePort key.

# Installing the Client CLI

> This installation procedure is optional. The ESSO-PG Client CLI SDK is supplied as an integration component for Provisioning Solutions.

The ESSO-PG Server provides a Web service that allows integration with other third-party provisioning systems. The ESSO-PG CLI is used to communicate with this Web service. You can use it as a traditional scripting tool or, if you prefer, you can use the SDK library to develop more complex integration solutions and connectors for the ESSO-PG Server.

Complete the following procedure to install and configure the ESSO-PG CLI. For more information on the CLI syntax and usage, refer to the *ESSO-PG CLI Guide*.

1. Close all programs.
2. Insert the installation CD in your CD-ROM drive (or start the installation from a shared network drive).
3. In the \ClientCLI folder, double-click the Client CLI file. Wait while the installer loads.
4. On the Welcome Panel, click **Next**.
5. On the Customer Agreement panel, enter your user name, organization name, and select who to **Install this application for: All Users** or **Only for you**. Click **Next**.
6. The Setup Type panel appears. Select **Complete** or **Custom**. **Complete** installs all program files; **Custom** allows you to choose what program files are installed and the location. Custom installations are only recommended for advanced users. To install the Java CLI, you must choose the custom panel. Installation choices for the Java CLI are for JDK 1.4 or 1.5.

8. Select the proper setup options and click **Next**.
9. ESSO-PG is ready to be installed. Click **Install**.
10. When the installation is complete, click **Finish**.

# Installing Support for the Agent

To install and configure the ESSO-PG support for the ESSO-LM Agent:

1. Close all programs.
2. Insert the installation CD in your CD-ROM drive (or start the installation from a shared network drive).
3. In the \Client folder, double-click the Client file. Wait while the installer loads.
4. On the Welcome panel, click **Next**.
5. ESSO-PG is ready to be installed. Click **Install**.
6. When the installation is complete, click **Finish**.

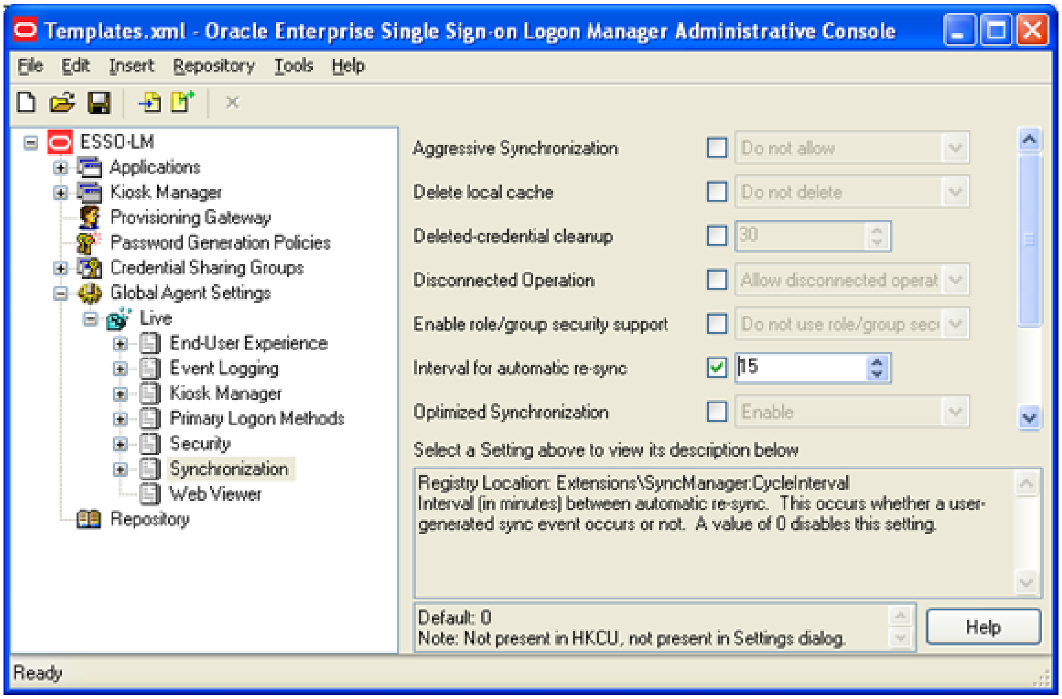
## Setting the CycleInterval Registry Key

In order for ESSO-PG to function properly, the ESSO-PG Agent must synchronize to retrieve the provisioning instructions from the directory.

When you deploy ESSO-PG, you must decide on the synchronization interval. The `CycleInterval` registry key is used to force synchronization to occur on a regular interval. If this is not set to a non-zero value, synchronization only occurs upon some user action. This is not the desired behavior with ESSO-PG. Oraclerecommends that this key be set to a value, for example, 15 minutes. This setting would guarantee that the provisioning instructions are pulled down from the directory within 15 minutes (or whatever interval is set) of when they are put there by the ESSO-PG Server.

The `CycleInterval` registry key can be set through the ESSO-LM Administrative Console:

1. Open the ESSO-LM Administrative Console by clicking **Start**>**Programs** > **Oracle** > **Oracle Administrative Console**.
2. Expand **ESSO-LM**, **Global Agent Settings**, expand **Live**, and click **Synchronization**.
3. Set the Interval for automatic re-sync setting to the desired value.
4. Click **Tools** > **Write Global Agent Settings to HKLM**.
5. The Apply Settings dialog opens. Click **Yes**.



Aggressive Synchronization □ Do not allow

Delete local cache □ Do not delete

Deleted-credential cleanup □ 30

Disconnected Operation □ Allow disconnected operat

Enable role/group security support □ Do not use role/group secu

Interval for automatic re-sync ☑ 15

Optimized Synchronization □ Enable

Select a Setting above to view its description below

Registry Location: Extensions\SyncManager:CycleInterval
Interval (in minutes) between automatic re-sync. This occurs whether a user-generated sync event occurs or not. A value of 0 disables this setting.

Default: 0
Note: Not present in HKCU, not present in Settings dialog.

This procedure applies only to running ESSO-LM agents. If a user does not have ESSO-LM running, the provisioning instructions are not processed until the user starts ESSO-LM.

Processing the provisioning instructions requires that the user be authenticated to ESSO-PG. If the user is not authenticated to ESSO-PG (for example, the timeout expired) then an authentication UI is presented and the synchronization process is blocked until the user authenticates.

# Upgrade Notes

If you are upgrading from an earlier version of ESSO-PG, perform the following procedures.

## ESSO-PG Server

Follow the instructions in Installing the Server. After running the installer, you must reset IIS and verify that the anonymous accounts are still set.

## ESSO-PG Agent

Before installing, shut down the ESSO-LM Agent. Follow the instructions in Installing Support for the Agent. After running the installer, restart the ESSO-LM Agent.

# Uninstalling ESSO-PG

Use the following procedure to uninstall ESSO-PG.

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Open **Add/Remove Programs**.
3. Select **Oracle Enterprise Single Sign-on Provisioning Gateway Server** and click **Remove**.
4. Follow the prompts to uninstall ESSO-PG.
5. Repeat Steps 3 and 4 for Oracle Enterprise Single Sign-on Provisioning Gateway **Agent for SSO** and **Oracle Enterprise Single Sign-on Provisioning Gateway Client CLI**.

# Reference and Troubleshooting

## Customization Notes

### Creating Default Access Pages

You can create HTML pages to provide end users with easy Web access to the ESSO-PG Management Console. Here is an example of the HTML markup for an end-user access page:

You can then create and distribute desktop shortcuts or Internet Explorer favorites to access this page.

You can also make your access page the default (home) page for the host Web server (YOURHOST, in the example URLs above). To do this, follow these steps:

1. Open IIS Manager.
2. Right-click the Default Web Site, and then choose **Properties** from the shortcut menu.
3. Click the **Documents** tab.
4. Make sure that the **Enable default content page** option is checked (note the name of the first-listed default page), then click **OK**.
5. Place your access page in the root folder of the default Web site and rename it as the default content page. Note that the link URL can now be relative to the root (for example, href="ESSO-PG Console").

Use these URLs in an access page or shortcut to access Management Console functions; again, substitute your host server name for *YOURHOST*:

```
<a href="http://YOURHOST/ESSO-PG Console/overview.aspx">Overview</a>
<a href="http://YOURHOST/ESSO-PG Console/storage.aspx">Storage
Settings</a>
<a href="http://YOURHOST/ESSO-PG Console/users.aspx">Users</a>
<a href="http://YOURHOST/ESSO-PG Console/eventLog.aspx">Event Log</a>
<a href="http://YOURHOST/ESSO-PG Console/report.aspx"/Report</a>
```

## Installation and Configuration Notes

Review the following installation and configuration notes:

- ESSO-PG Does Not Support File Synchronization
- Multiple Locators Require an Entlist at Each Locator Site
- Using AD or ADAM and IIS Web Services on Different Servers
- Windows Installer Error 1720
- Internet Security Settings (Windows 2003 Users)
- Internet Security settings (Windows Domain and Citrix MetaFrame users)
- Deploying ESSO-PG With Multiple Oracle Internet Directory (OID) Servers

### ESSO-PG Does Not Support File Synchronization

ESSO-PG will not function correctly if it is deployed with the file synchronizer.

The Agent is configured to store its user data as a flat file on a network drive, FTP server, NFS share, or local disk drive. ESSO-PG will not function in this scenario because it requires a directory in order to distinguish and provision individual user accounts.

Multiple Locators Require an Entlist at Each Locator Site

If two users are stored in different containers, a matching application configuration list (entlist) must exist in each locator site in order for provisioning to work down to the client. The matching entlists must exist under both containers that store the user credentials.

## Using AD or ADAM and IIS Web Services on Different Servers

If IIS and Active Directory (or the ADAM-instance) are on different computers, then you must provide the IIS Web services with a user account that is in the same domain as (or a trusted domain of) AD or ADAM, and that is provided with read/write access to the directory.

## Windows Installer Error 1720

Error 1720 occurs during ESSO-PG Client software installation when the logged-on user does not have sufficient rights to install software on the workstation. You must log on to the workstation as a user with administrator rights or contact support personnel for assistance.

## Internet Security Settings (Windows 2003 Users)

The default settings for Windows 2003 Internet Security are more stringent than those for Windows 2000 and XP. If Internet Explorer Enhanced Security Configuration is enabled (on by default in Windows 2003), you must add the ESSO-PG Web Console URL to the workstation's Trusted Sites Internet Zone or the Local Intranet Zone in order to use ESSO-PG without issues.

## Internet Security Settings (Windows Domain and Citrix MetaFrame® Users)

In order for Windows domain users and Citrix MetaFrame users to access ESSO-PG, you must add the ESSO-PG Web service to the workstation's Local Intranet zone.

## Deploying ESSO-PG With Multiple Oracle Internet Directory (OID) Servers

When ESSO-PG is deployed with multiple Oracle Internet Directory (OID) servers load-balanced in an active-active (all servers active) topology, ESSO-PG cannot resolve the client-server session state due to multiple servers being involved in the session. This will cause ESSO-PG to behave erratically. To avoid this issue, do one of the following:

- For simple failover support, load-balance your deployment using an active-standby topology. In this configuration, only one OID server is handling connections from ESSO-PG clients at any given moment. Backup servers, synchronized with the active server via replication, are ready to take over if the active server fails. You must configure your network to automatically re-route the connections from the failed server to one of the backup servers when a failure occurs.
- (Recommended) Use the Oracle Real Application Cluster (RAC) technology to create an OID server cluster. A cluster will appear as a single server to ESSO-PG clients, while providing the performance and high availability of a fully load-balanced deployment. In case of server failure, operation continues uninterrupted, and servers can be replaced on the fly. Servers can also be added at any time, providing quick and easy scalability.