

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

Installation and Setup Guide

Release 10.1.4.1.0

E12614-01

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 ESSO-PG	4
Audience.....	4
Installation Overview.....	5
System Requirements and Supported Applications	6
Minimum System Requirements	6
Software Requirements	6
Installing ESSO-PG.....	9
Installing the ESSO-PG Server	9
Creating or Identifying a User Account for Anonymous Logon	9
Enabling SSL	12
Configuring Syslog	17
Installing the ESSO-PG Client CLI	18
Installing ESSO-PG Support for ESSO-LM Agent.....	19
Upgrade Notes.....	21
ESSO-PG Server:	21
ESSO-PG Agent:	21
Uninstalling ESSO-PG	22
Reference and Troubleshooting	23
Customization Notes.....	23
Installation and Configuration Notes	24

About ESSO-PG

Oracle Enterprise Single Sign-On (ESSO-PG) enables an administrator to automatically provision in 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 ESSO-PG functionality and provides instructions for installation and configuration.

Audience

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.

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

Installation Overview

ESSO-PG is installed as an add-on component to ESSO Logon Manager (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 . Each procedure is explained in detail in the [Installing ESSO-PG](#) section. If you are upgrading from an earlier version of ESSO-PG, refer to the [Upgrade Notes](#).

- [Installing ESSO PG Server](#)
 - [Installing the Server](#)
 - [Creating or identifying a User Account for Anonymous Logon](#)
 - [Enabling SSL](#)
- [Installing ESSO-PG Client CLI](#) (*optional*)
- [Installing ESSO-PG Support for ESSO-LM Agent](#)
 - [Set CycleInterval Registry Key](#)

System Requirements and Supported Applications

The information in this section applies to the ESSO-PG Server, unless otherwise indicated.

Minimum System Requirements

In order for you to install ESSO-PG and have it function properly, your system must meet the following minimum requirements:

- Process: Pentium III class processor running at 900 MHZ
- Memory: 512 MB RAM
- Disk Space: a complete installation requires at least 3 MB. ESSO-PG support for the SSO Agent requires at least 1 MB of additional disk space.

Software Requirements

In order for you to install ESSO-PG and have it function properly, your system must have the following applications installed:

- Internet Explorer 6.0 or higher with 128-bit encryption or Mozilla Firefox 1.0+
- Microsoft® .NET Framework 2.0 (installed as part of the ESSO-PG setup)
- Microsoft Web Services Enhancements 3.0 (WSE 3.0) (installed as part of the ESSO-PG setup)

ESSO-PG Support for SSO Agent

In order for the ESSO-PG support for the ESSO-LM Agent to function properly, ESSO-LM must be installed.

ESSO-PG Server

In order for ESSO-PG Server to function properly, your system must have the following applications installed:


- Microsoft Windows® 2000 Server or Windows Server 2003
- Microsoft Internet Information Server version 5.0 or later (6.x recommended)
- Microsoft Active Directory®, Microsoft ADAM, Sun Directory Server, or IBM LDAP Directory, Oracle Internet Directory, Novell eDirectory Server.
- Microsoft SQL Server 2000, Microsoft SQL Server 2000 Desktop Engine (MSDE 2000), Microsoft SQL Server 2005 Express Edition, or Microsoft SQL Server 2005 (only required if you are using event logging)

OR

- Oracle database

Microsoft IIS Requirements:

Microsoft Internet Information Server (IIS), version 5.0 or later, is required. ESSO-PG uses the IIS Web server to provide a browser-based interface for user enrollment, general setup, and administrative tasks.

	<p>If Active Directory or ADAM is used, the anonymous account used in IIS must have administrative privileges and the server must be joined to the domain.</p> <p>If you are running Windows 2000 SP4, verify that the ASPNET account (or IWAM_Machine if ASPNET does not exist) has the privilege to impersonate a client after authentication. Refer to http://support.microsoft.com/kb/821546 for more information.</p>
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

ESSO-PG Repository Requirements:

ESSO-PG can use any of the following as the repository:

- Oracle Internet Directory
- Microsoft Active Directory or Active Directory Application Mode (ADAM). The Active Directory server or ADAM instance (that is, Active Directory running as a user service) can be on any server and in the same domain.
- Sun Directory Server
- IBM LDAP Directory
- Novell eDirectory

Installer Requirements

To install ESSO-PG, you must have Administrative privileges for the ESSO-PG and IIS server. You must provide the following information to configure a directory server:

host	Name of the server hosting the directory server instance.
port	Port number of directory server instance.
<i>name1[,name2,name3]</i>	Distinguished name of the directory server domain root.

Certificate Requirements

An X.509 Certificate for SSL must be obtained from a certificate authority (CA).

A trusted root CA certificate should also be downloaded from your certificate authority into the list of trusted root CA certificates on the local computer.

For more information, see [Enabling SSL](#).

ESSO-PG Installation and Setup Guide

A certificate setup guide is provided with the ESSO-PG documentation suite. If you do not have a certificate authority in place and want to use Microsoft Certificate Services to obtain certificates, refer to the *ESSO-PG Certificate Setup Guide*, which explains how to obtain the necessary certificates using Microsoft Certificate Services.

Installing 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:

- Install the ESSO-PG Server
 - [Install the Server](#)
 - [Create or identify a User Account for Anonymous Logon](#)
 - [Enable SSL](#)
- [Install the ESSO-PG Client CLI](#)
- [Install ESSO-PG support for the ESSO-LM Agent](#)


Installing the ESSO-PG Server

To install and configure the ESSO-PG Server:

1. Close all programs.
2. Double-click the **ESSO-PG Server.exe** or **ESSO-PG Server.msi** file to begin the installation.
3. On the Welcome Panel, click **Next**.
4. The License Agreement panel opens. Read the license agreement carefully. Click the **I accept the terms in the license agreement** button and 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**.

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.

	<p>Because the default Anonymous User account in IIS, <code>IUSR_MACHINE_NAME</code>, 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:</p>
-------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


<ul style="list-style-type: none">• 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 (HKLM). <p>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).</p>

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

1. Click **Start > Program Files > Administrative Tools > Internet Information Services**.
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.

 <p>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 <i>ESSO-PG Administrator Guide</i>.</p>

Give the IIS Anonymous Account Access to ADAM

 <p>This step only applies to ADAM users. Use the account chosen in Step 2b.</p>

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

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

For example:

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

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

```
dsacl s \\SERVER:PORT\DISTINGUISHED_NAME
```


The output shows the security information for the directory object. The v-GO PM 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 Computer** 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.

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.

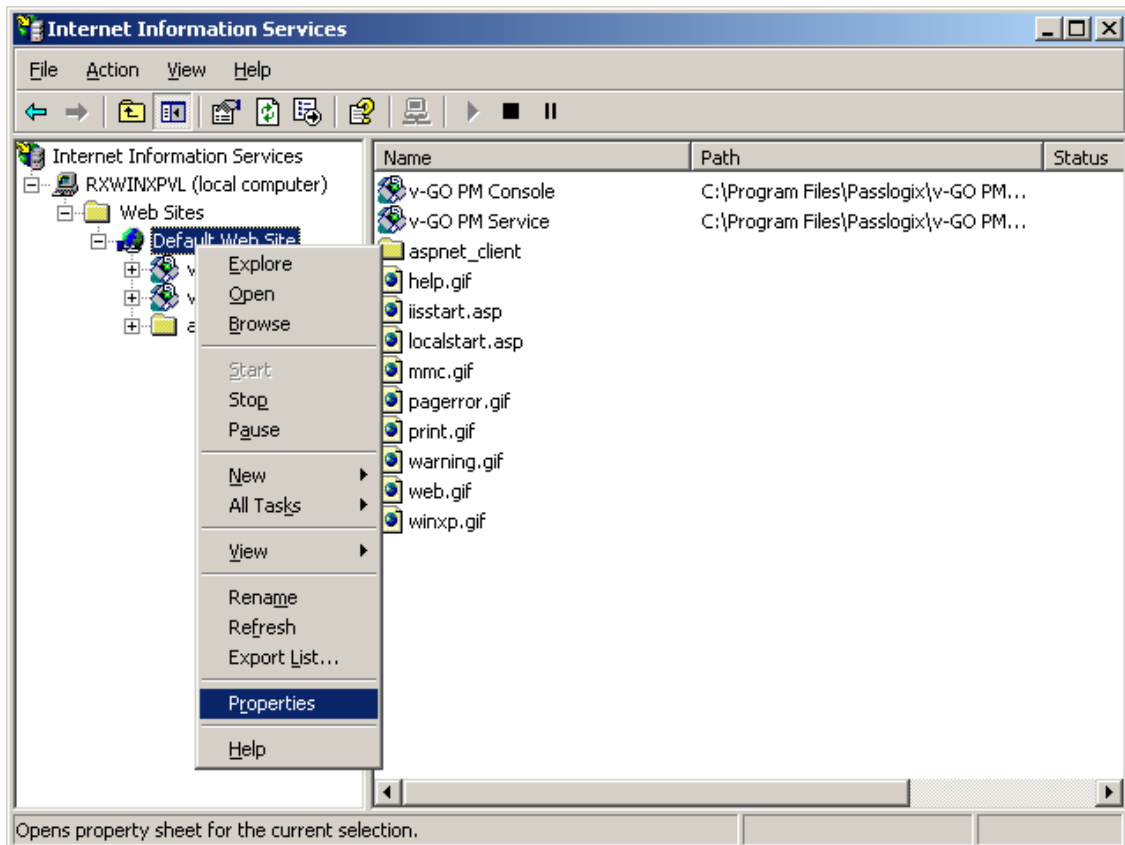


The following articles from the Microsoft Web site can be referred to for information on installing certificates and setting up SSL:

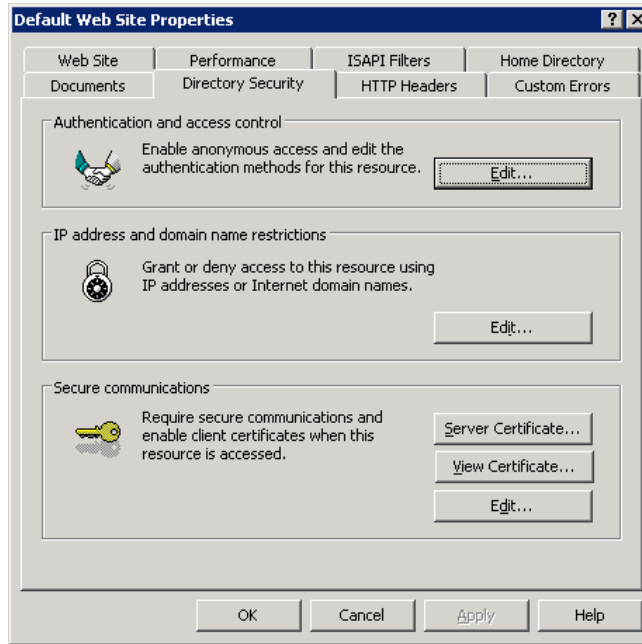
- “How to: Obtain an X.509 Certificate”
<http://msdn2.microsoft.com/en-us/library/ms819929.aspx>
- “How to: Set Up SSL on a Web Server”
<http://msdn2.microsoft.com/en-us/library/aa302411.aspx>

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.

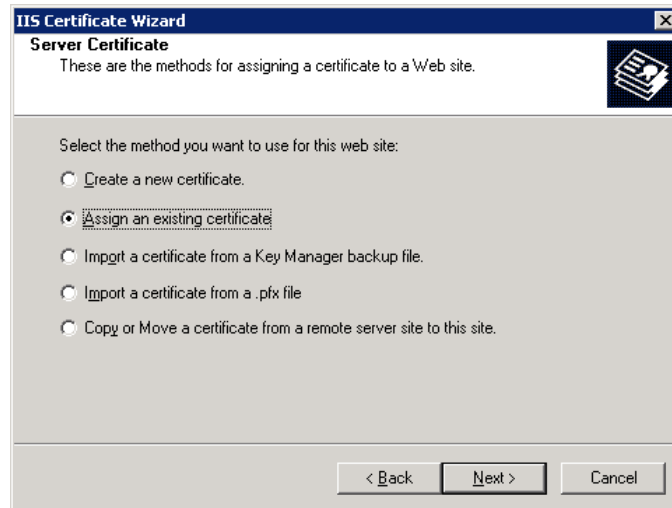
1. Go to **Control Panel** → **Internet Information Services**. Right-click Default Web Site web site. Select **Properties**.



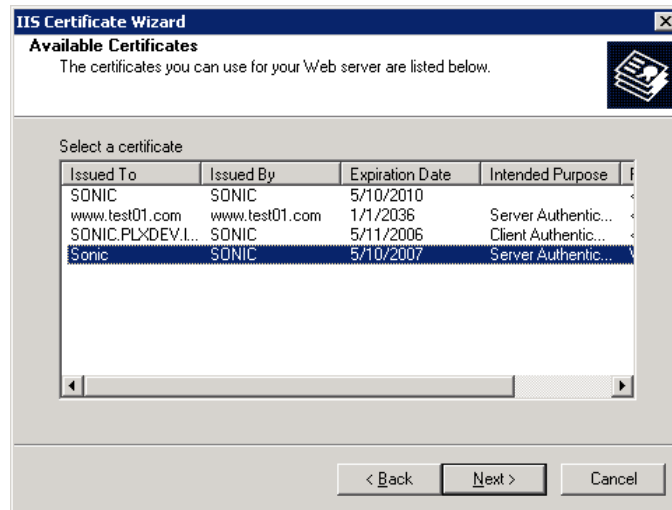
- Click the **Directory Security** tab and under **Secure Communications**, click **Server Certificate**.



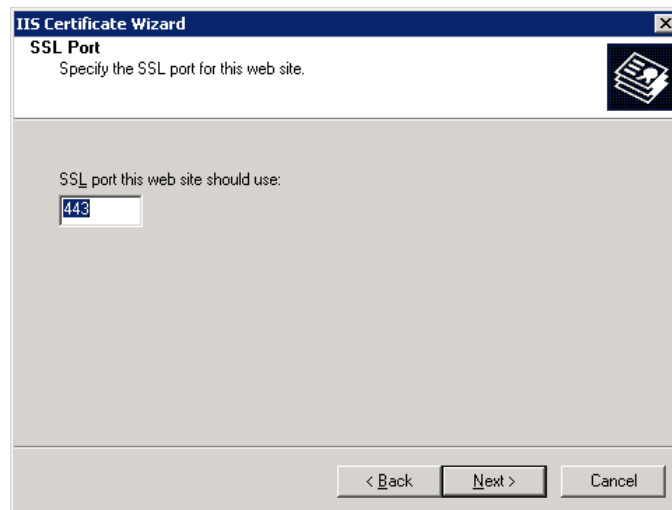
- The Web Server Certificate Wizard opens. This is where you generate a request for a certificate. Click **Next**.
- Select **Assign an existing certificate** and click **Next**.



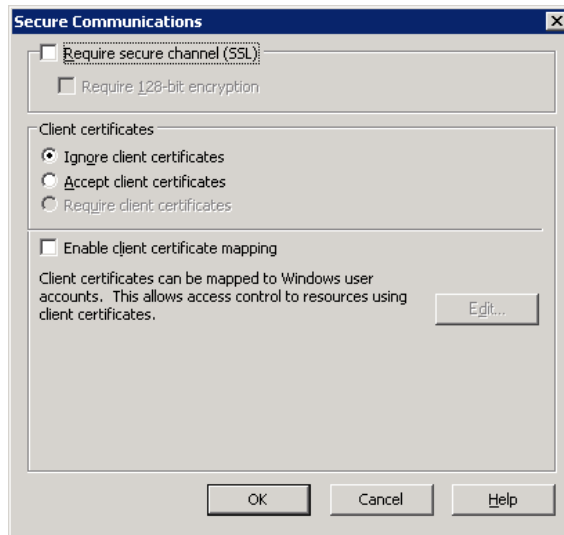
5. Highlight the certificate to assign and click **Next**.



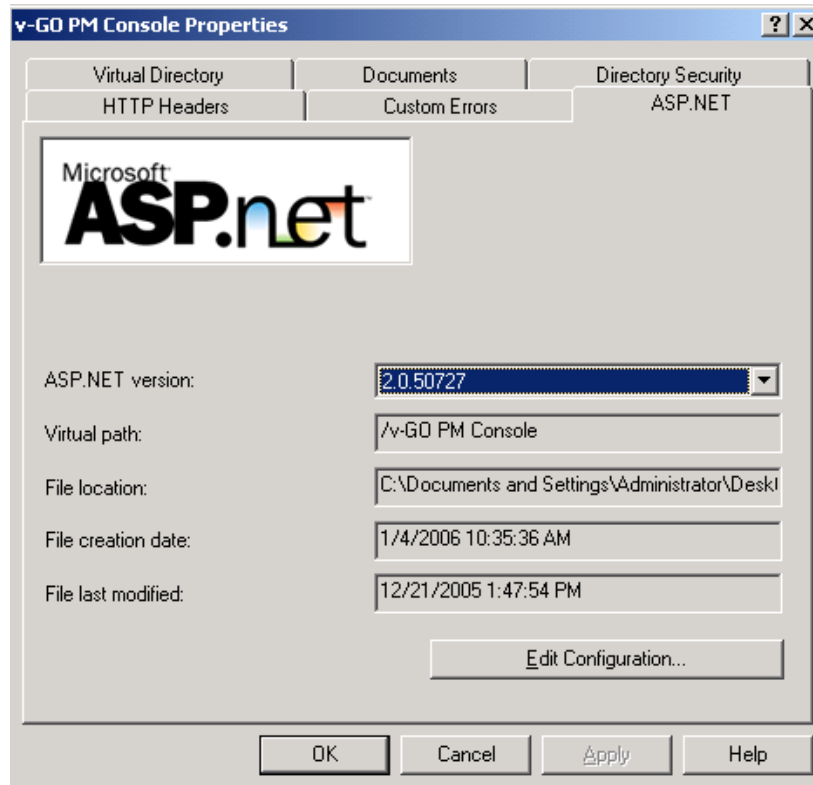
6. The default SSL port is 443. Accept the default and click **Next**.



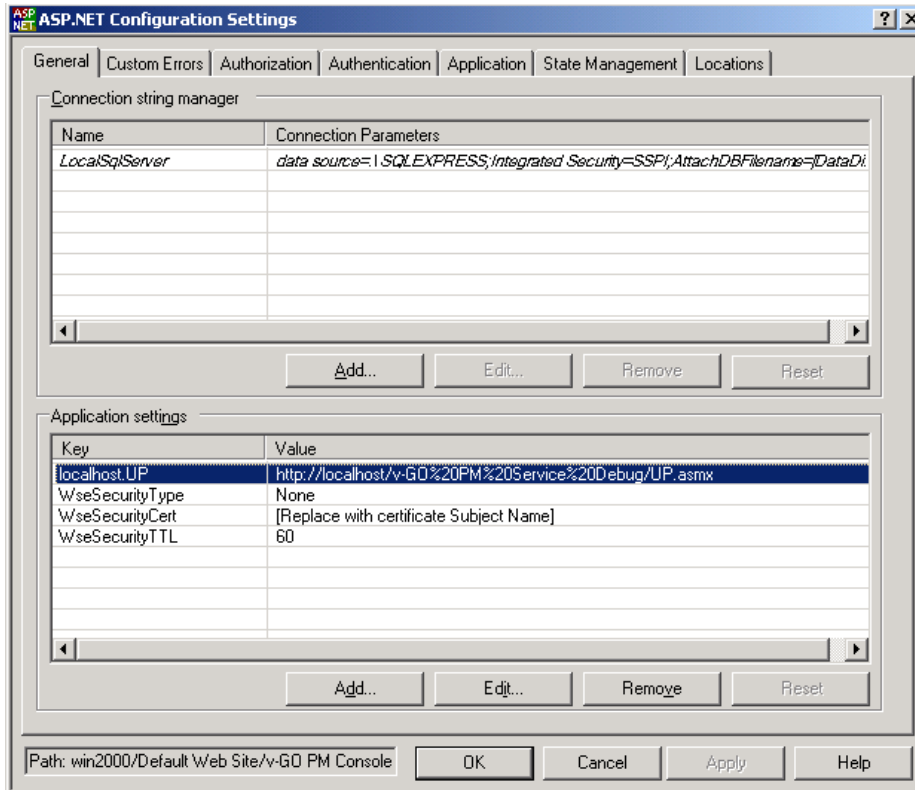
7. Review the summary of your request. Click **Next**.
8. Click **Finish**.
9. The **Directory Security** tab will still be open. Under **Secure Communications**, click **Edit**.
10. In the Secure Communications dialog box, check **Require secure channel (SSL)** and **Require 128-bit encryption**. Click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



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**.



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



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 ESSO-PG 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. Double-click the **ESSO-PG Client CLI.exe** or **ESSO-PG Client CLI.msi** file to begin the installation.
3. On the Welcome Panel, click **Next**.
4. The License Agreement panel appears. Read the license agreement carefully. Click the **I accept the terms in the license agreement** button and click **Next** to continue.
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.
7. Select the proper setup options and click **Next**.
8. ESSO-PG is ready to be installed. Click **Install**.
9. When the installation is complete, click **Finish**.

Installing ESSO-PG Support for ESSO-LM Agent

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

1. Close all programs.
2. Double-click the **ESSO-PG Client.exe** or **ESSO-PG Client.msi** file to begin the installation.
3. On the Welcome panel, click **Next**.
4. The License Agreement panel opens. Read the license agreement carefully. Click the **I accept the terms in the license agreement** button and click **Next** to continue.
5. ESSO-PG is ready to be installed. Click **Install**.
6. When the installation is complete, click **Finish**.

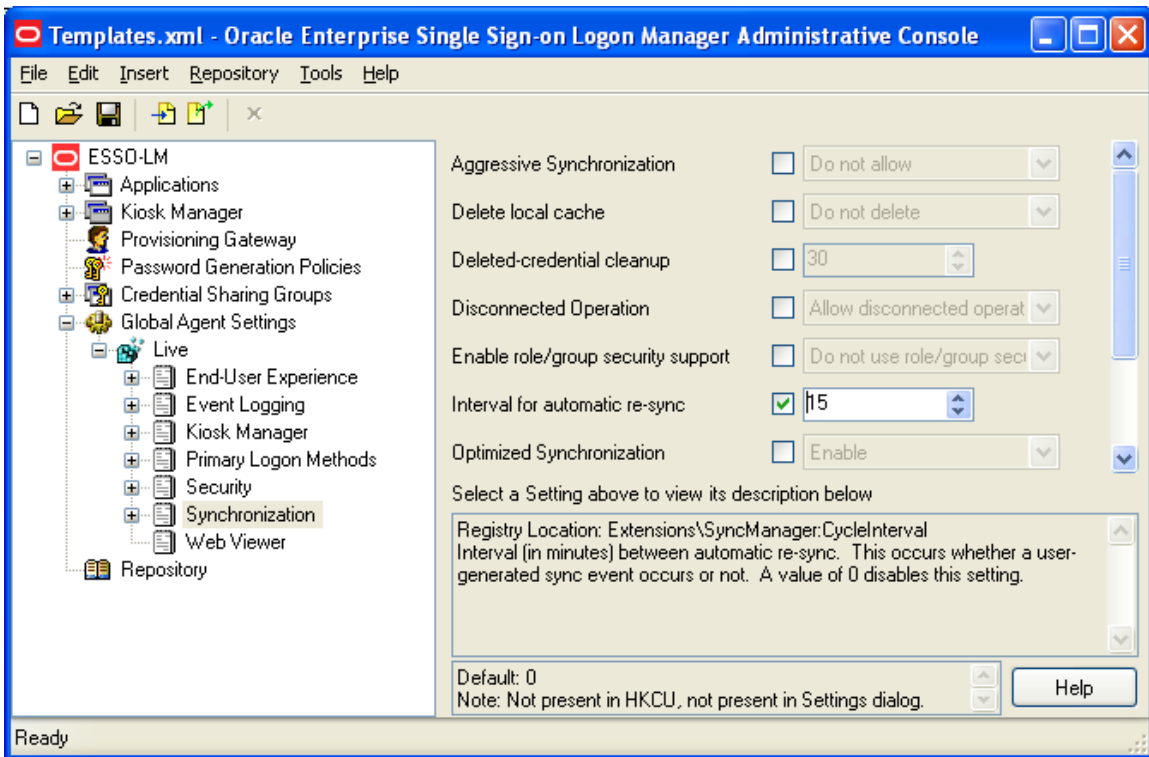
Setting the `CycleInterval` Registry Key


In order for ESSO-PG to function properly, the ESSO-LM 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. Oracle recommends 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 Console:

1. Open the ESSO-LM Administrative Console by clicking **Start**, point to **Programs > Oracle > ESSO-PG**, and click **ESSO-LM 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**.



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

Processing the provisioning instructions requires that the user be authenticated to ESSO-LM. If the user is not authenticated to ESSO-LM (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 these steps:

ESSO-PG Server:

Follow the instructions in the [Installing the v-GO PM Server](#) section. 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 the [Installing v-GO PM Client \(Support for v-GO SSO Agent\)](#) section. After running the installer, restart the Agent.

Uninstalling ESSO-PG

Follow these steps to uninstall ESSO-PG.

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Open **Add/Remove Programs**.
3. Select **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 **ESSO-PG Agent for ESSO-LM** and **ESSO-PG 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 Administrative Console.

Here is an example of the HTML markup for an end-user access page:

```
<html>
<head>
  <title>v-GO PM Console</title>
  <style>
    body
    {
      font-family:Verdana;
      font-size:12px;
      text-align:center
    }
    h1
    {
      font-size: 18px
    }
  </style>
</head>
<body>
  <h1>v-GO Provisioning Manager</h1>
  <!--substitute the host computer name for YOURHOST.
  If over SSL, use HTTPS instead of HTTP.
  -->
  <p>
    <a href="http://YOURHOST/v-GO PM Console/overview.aspx">
      v-GO PM Administrative Console
    </a>
  </p>
</body>
</html>
```

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="v-GO PM Console").
1. Use these URLs in an access page or shortcut to access Administrative Console functions; again, substitute your host server name for *YOURHOST*:

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

Installation and Configuration Notes

Review the following installation and configuration notes:

- ESSO-PG does not support File Sync
- [Multiple Locators Require an Entlist at Each Locator Site](#)
- [Using AD/ADAM and IIS Web Services on Different Servers](#)
- [Windows Installer Error 1720](#)
- [Internet Security Settings \(Windows 2003 Users\)](#)
- [Internet Security settings \(Windows Domain and Citrix MetaFrame users\)](#)

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.