Oracle ESSO Provisioning Gateway with Luna HSM

Integration Guide

SafeNet
THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-012388-001 (Rev A)
Release Date	November 2013

Trademarks

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimer

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Email	support@safenet-inc.com	

Contents

CHAPTER 1
Introduction

This document is intended to guide administrators through the steps for Oracle ESSO-PG and Luna HSM integration, and also covers the necessary information to install, configure and integrate Oracle ESSO-PG with SafeNet Luna Hardware Security Modules (HSMs).

The Luna HSMs integrates with the Oracle ESSO-PG to provide significant performance improvements by off-loading cryptographic operations from the Server to the Luna HSMs. In addition, the Luna HSMs provides extra security by protecting the private keys within a FIPS 140-2 certified hardware security module.

Understanding the ORACLE 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.

Scope

This guide provides instructions for setting up a small test lab with Oracle ESSO-PG running with Luna HSM for securing the SSL private keys. It explains how to install and configure the software that is required for setting up a SSL on Oracle ESSO-PG while storing private key on Luna HSM.

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.

3rd Party Application Details

- Oracle ESSO Provisioning Gateway 11.1.2.1.0

You can download the ESSO-PG Software's from Oracle Support site:

Supported Platforms

The following platforms are supported for Luna HSM:

Operating System	SafeNet Luna HSM	Oracle ESSO-PG
Windows Server 2008 R2	Luna SA v4.4.3	11.1.2.1.0

HSM and Firmware Support

We did this integration with the following:

Luna SA f/w 4.8.1 with Luna Client s/w v4.4.1 (64 bit)

Prerequisites

Luna SA Setup

Please refer to the **Luna SA** documentation for installation steps and details regarding configuring and setting up the box on Windows operating systems. Before you get started ensure the following:

- Luna SA appliance and a secure admin password
- Luna SA, and a hostname, suitable for your network
- Luna SA network parameters are set to work with your network
- Initialized the HSM on the Luna SA appliance.
- Created and exchanged certificates between the Luna SA and your Client system.
- Created a partition on the HSM, remember the partition password that will be later used by Oracle ESSO-PG.
- Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from Luna SA. The general form of command is “C:\Program Files\LunaSA\vtl verify” for Windows.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Oracle ESSO-PG Setup

You should familiarize yourself with Oracle ESSO-PG. Refer to the Oracle documentation for more information to install and pre-installation requirements.

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.

This guide will use to setup small lab for testing purposes that uses the following:

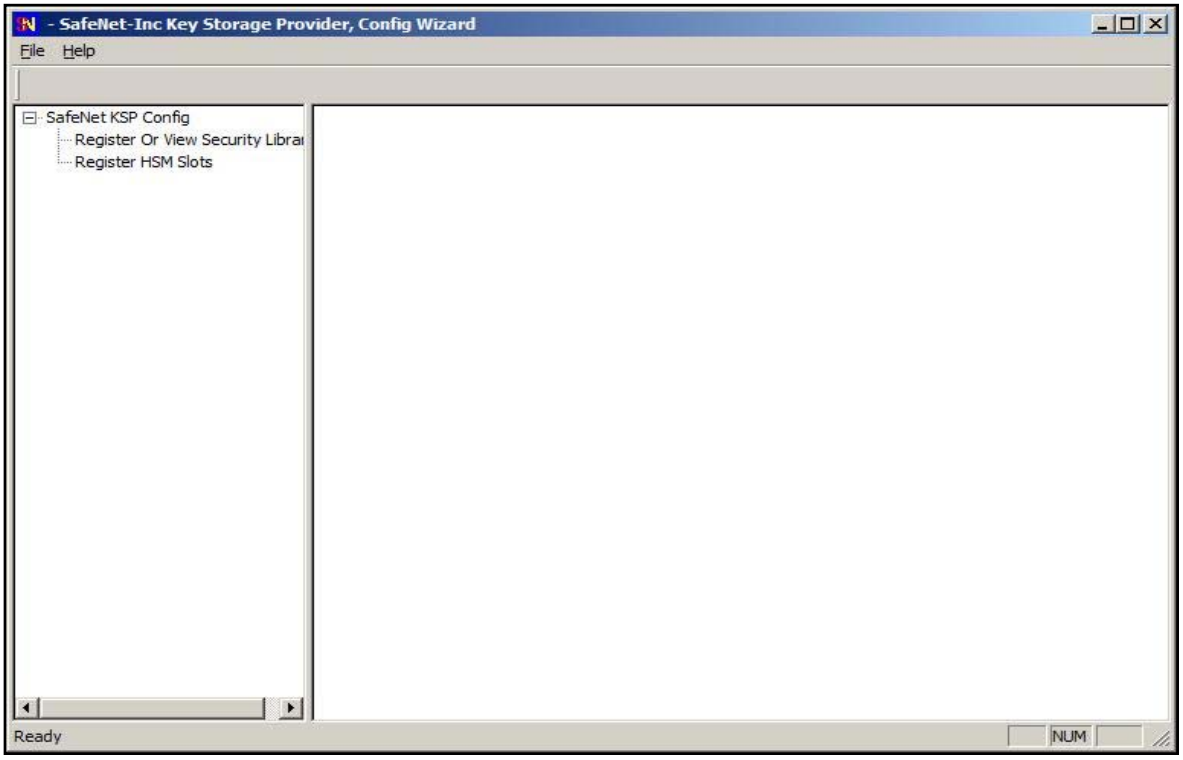
- Windows machine, which will become a Domain Controller and Certification Authority.

NOTE: We can install the domain controller and CA on different machines depends upon the requirement. For testing purpose we installed the Domain

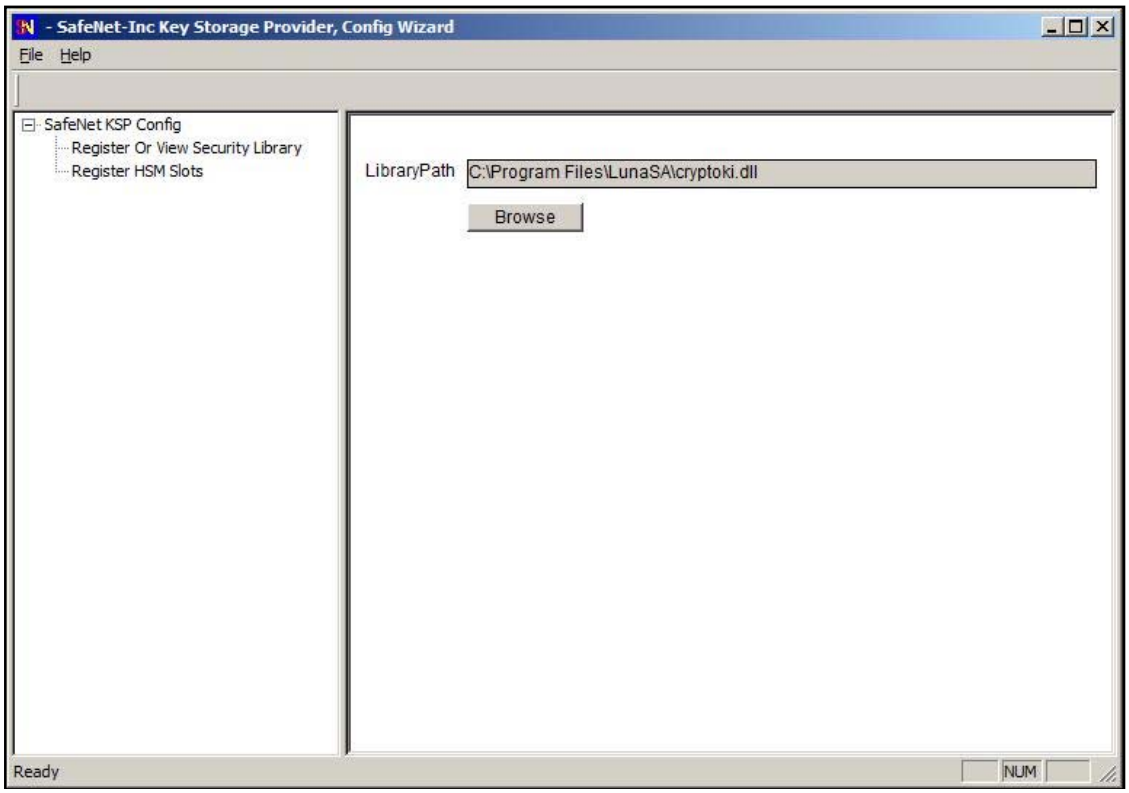
Controller and CA on same machine.

Before you install

- KSP must be installed in a separate step following completion of the main Luna SA Client software installation.
- Traverse to *C:\Program Files\SafeNet*
- Run the KspConfig.exe (KSP configuration wizard).



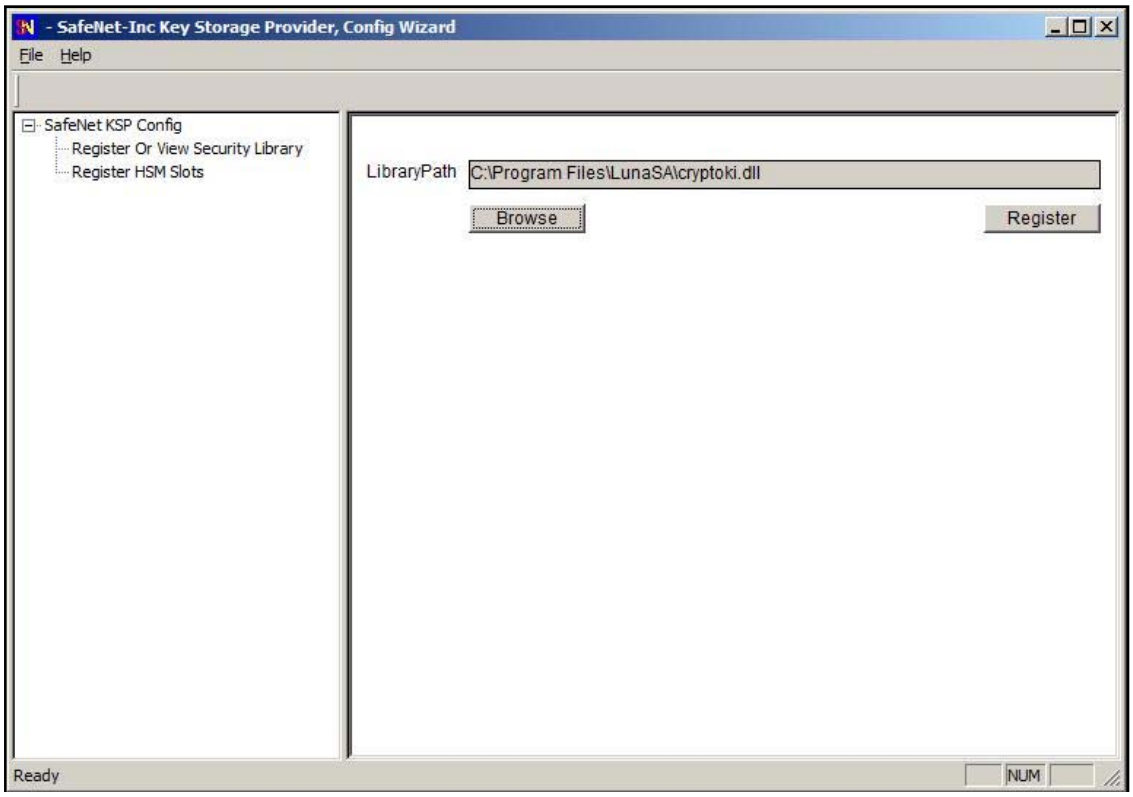
- Double click **Register or View Security Library** on the left side of the pane.



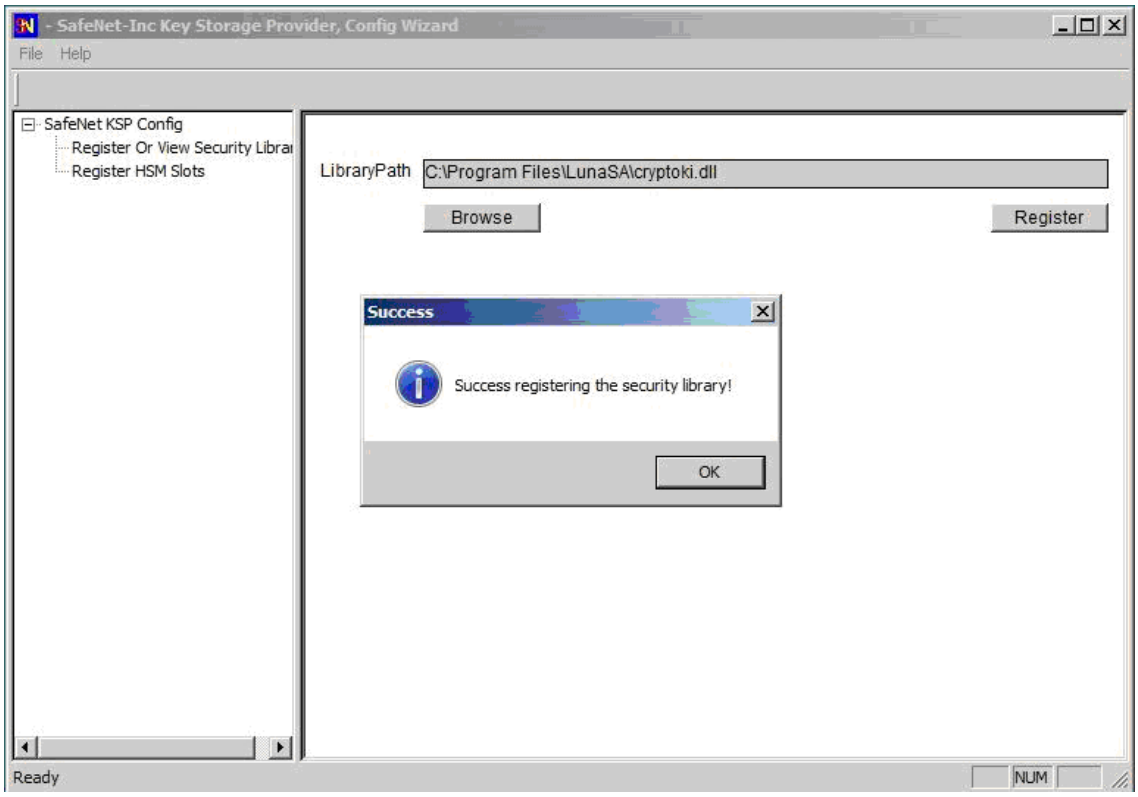
- Browse the library

  C:\Program Files\LunaSA\cryptoki.dll

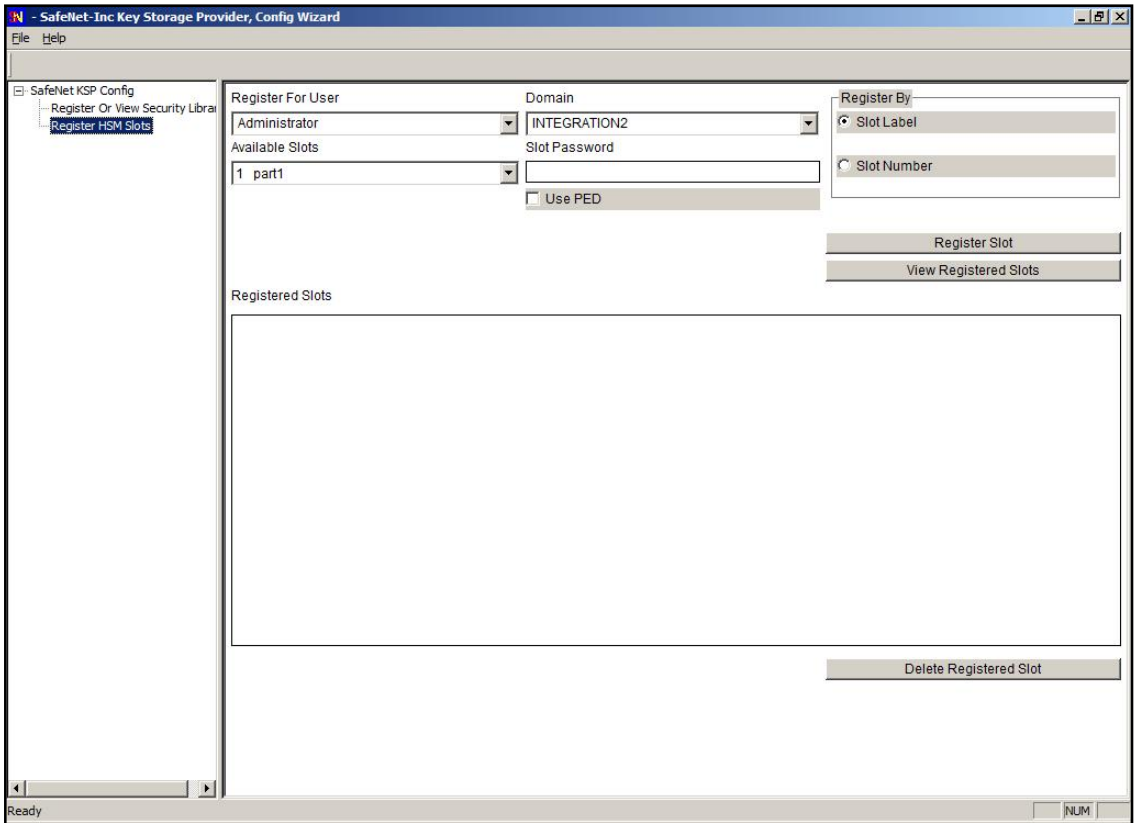
  Now click **Register**.



- On successful registration you will receive a message as **Success registering the security library**.

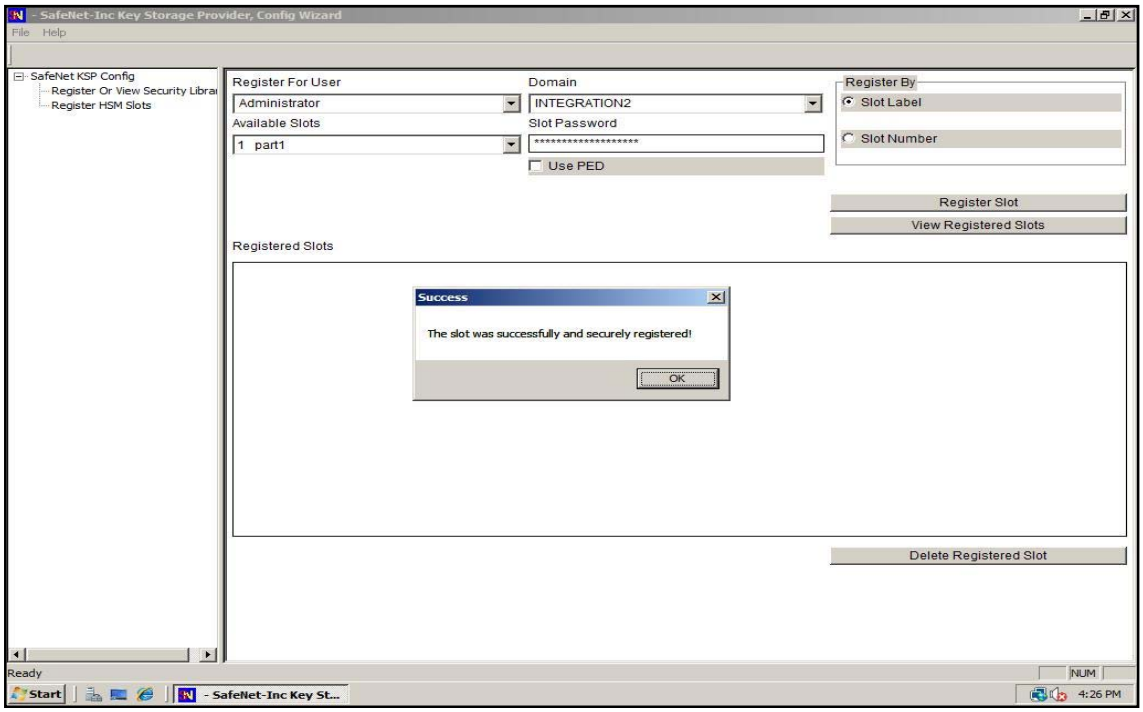


- Double click **Register HSM Slots** on the left side of the pane.

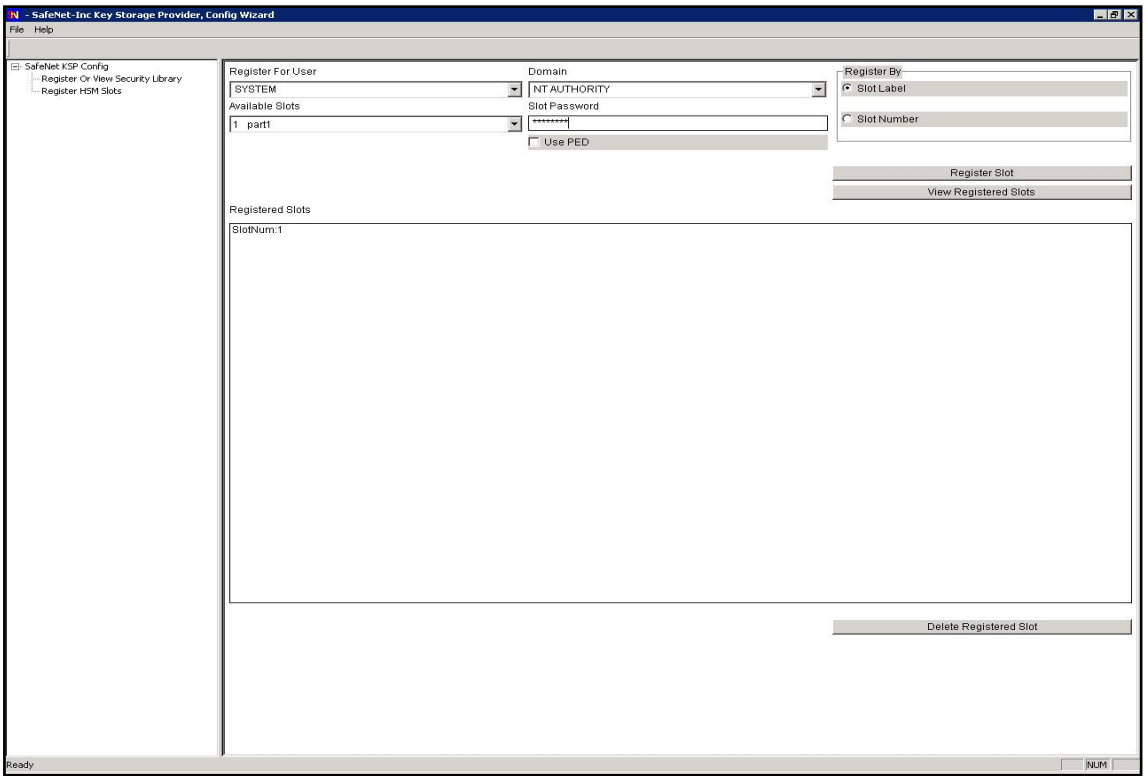


- Enter the Slot (Partition) password.

- Click on **Register Slot** to register the slot for Domain\User. On successful registration you will receive a message "**The slot was successfully and securely registered"**.



- You need to register the slot for NT_AUTHORITY\SYSTEM.


- SafeNet-Inc Key Storage Provider, Config Wizard
File
Help
SafeNet KSP Config
Register Or View Security Library
Register HSM Slots
Register For User
SYSTEM
Domain
NT AUTHORITY
Register By
Slot Label
Available Slots
1 part1
Slot Password
Slot Number
Use PED
Register Slot
View Registered Slots
Registered Slots
SlotNum:1
Delete Registered Slot
Ready
NUM

CHAPTER 2
Integrating Oracle ESSO-PG with Luna

Setting up Luna with Oracle ESSO-PG

To set up Luna HSM for Oracle ESSO-PG, kindly perform the following steps:

Setting up Luna SA for Active Directory Certificate Services

To set up Luna SA for Active Directory Certificate Services, kindly refer the Microsoft Active Directory Certificate Services Integration Guide with Luna SA.

1. Before Installing the ESSO-PG Server

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 R2 Server machine.

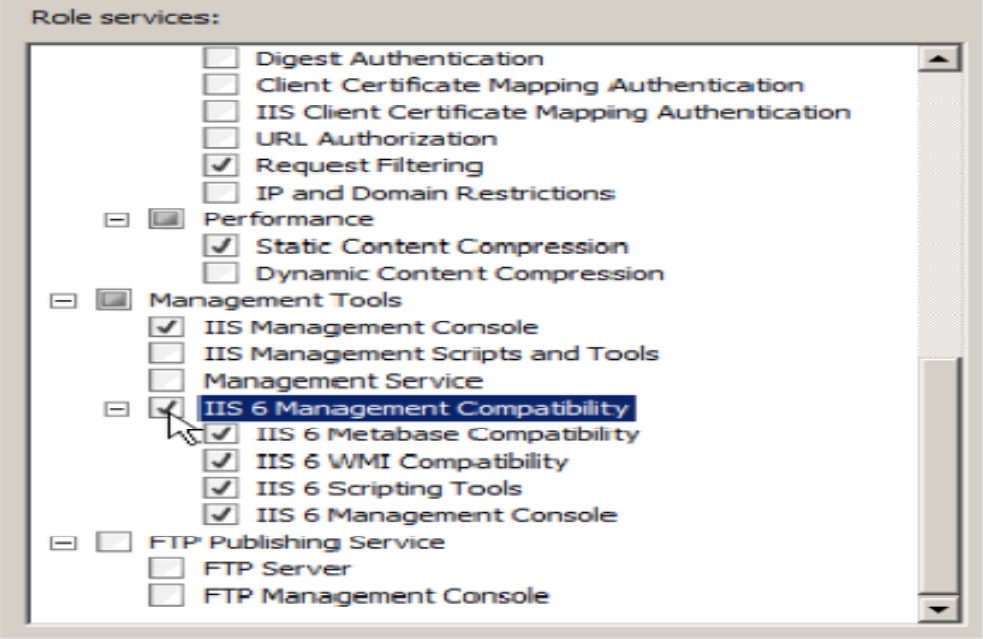
To add the IIS 6 Management Compatibility role service to IIS:

a) Click on Start -> Administrative Tools -> Server Manger.

b) Click on Roles -> Web Server (IIS).

c) Click on Add Role Services.

d) In the Role services window, scroll down and select IIS 6 Management Compatibility.



e) Click Next.

f) From the Confirmation screen of the Add Roles wizard, click Install.

g) After configuring IIS 6 Management Compatibility, install the ESSO-PG Server.

NOTE: 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.)

2. Installing the Server

To install and configure the ESSO-PG Server:

a) Close all programs.

b) Insert the installation CD in your CD-ROM drive (or start the installation from a shared network drive).

c) In the \Server folder, double-click the Server file. Wait while the installer loads.

d) On the Welcome Panel, click Next.

e) 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.

f) ESSO-PG is ready to be installed. Click Install. Wait for the installation to complete. When it is done, click Finish.

3. After installing the ESSO-PG Server

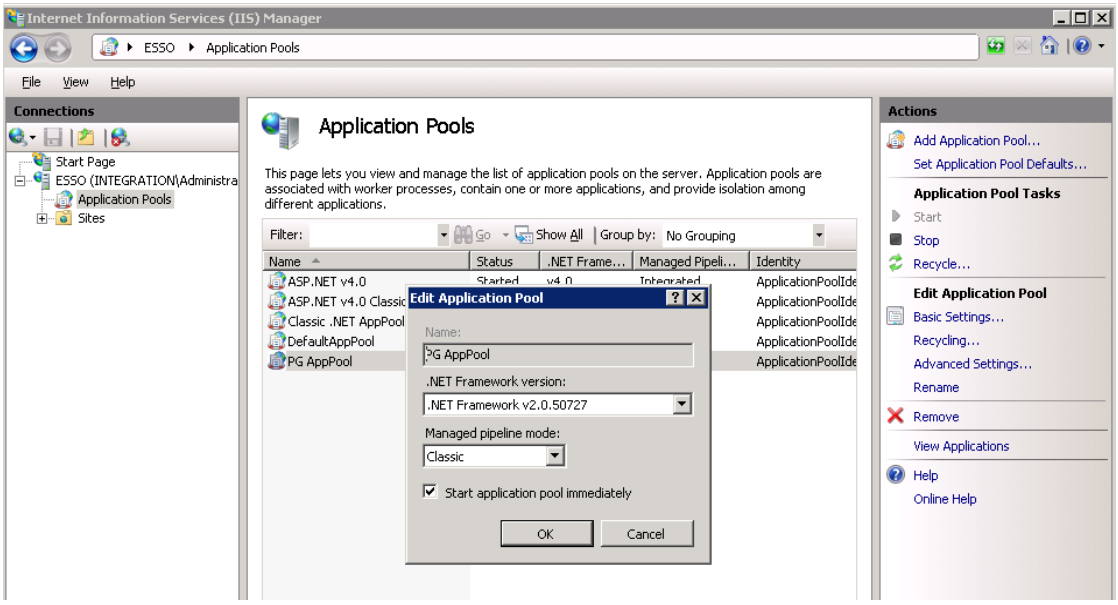
Now you need to create a new App Pool and move your ESSO-PG Console and ESSO-PG Service into it.

a) Click on Start -> Administrative Tools -> Internet Information Services (IIS) Manager.

b) Expand the Server tree in left hand pane click on Application Pools.

c) Click on Add Application Pool.

d) Enter the Name as PG AppPool, Select .NET Framework version as 2.0.x and Managed pipeline mode as Classic.

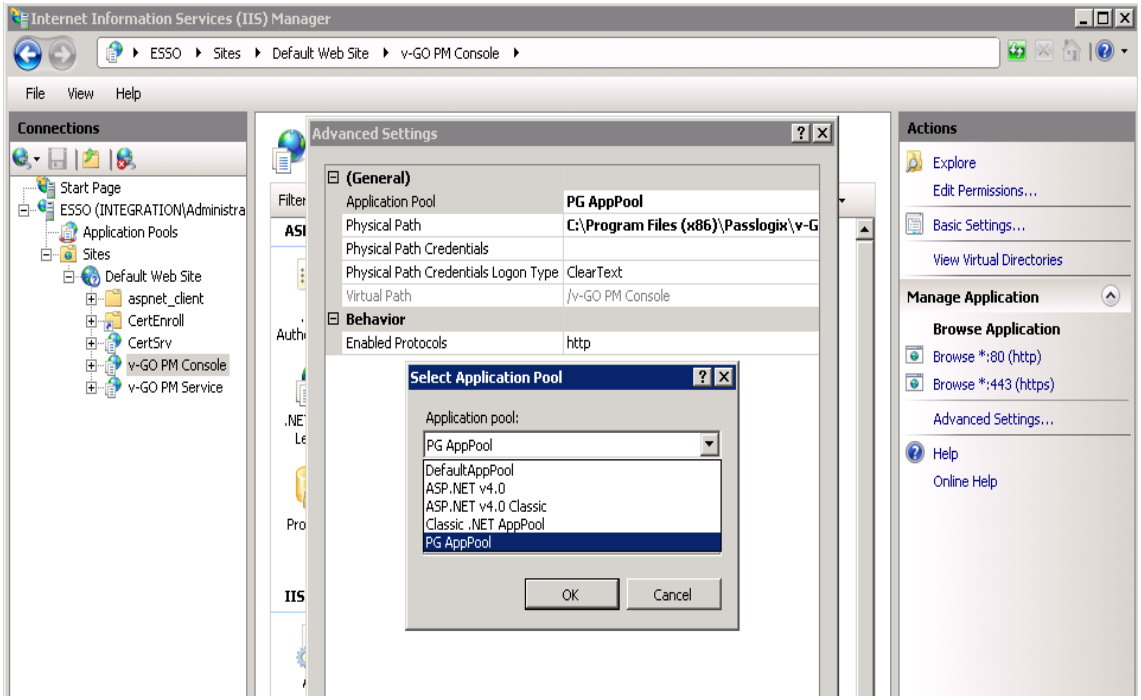


e) Click on OK button.

f) Click on Sites -> Default Web Site and right-click ESSO-PG Console.

g) Select Manage Application >Advanced Settings. In the Advanced Settings window, select Application Pool.

h) In the Select Application Pool window, select PG AppPool.



i) Click OK.

j) Follow the same steps to move the ESSO-PG Service into the PG AppPool.

4. Configuring a 64-bit OS to Run ESSO-PG Server

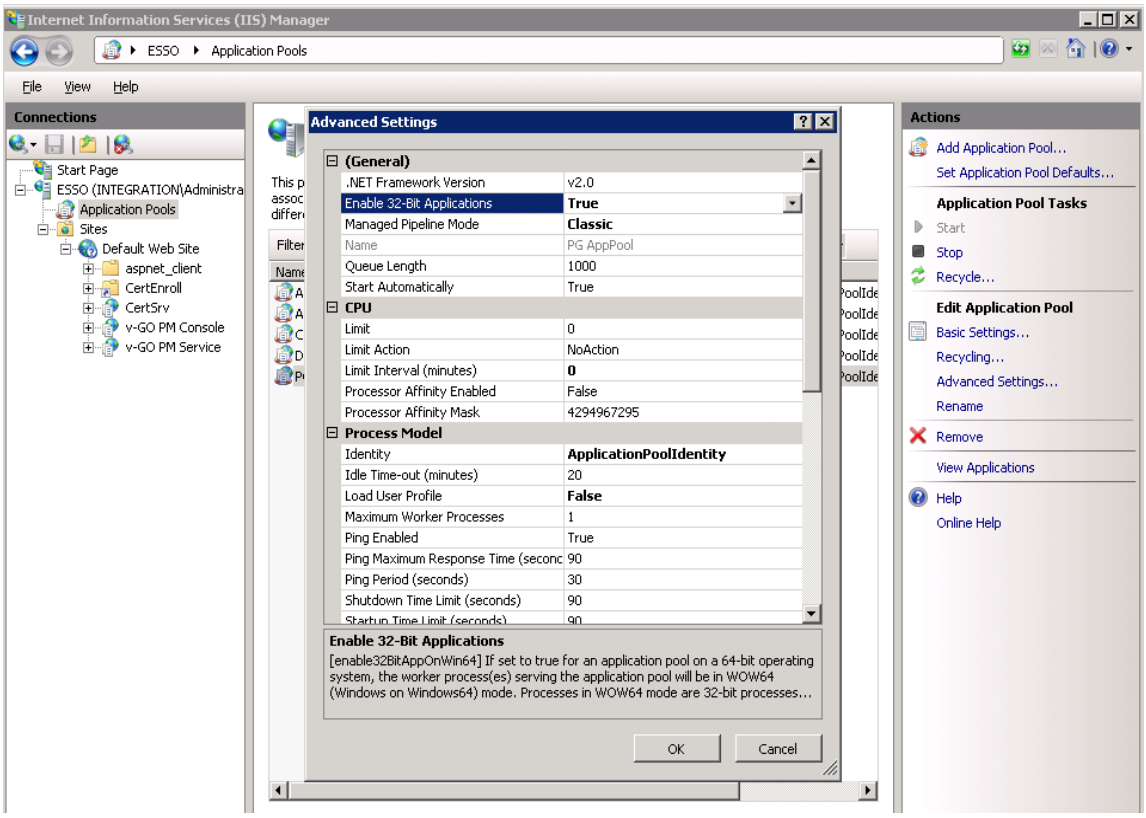
a) Open Internet Information Services (IIS) Manager.

b) Click Application Pools.

c) Right-click PG AppPool and select Advanced Settings...

d) Change "Enable 32-bit Applications" settings to True.

e) Click OK.



f) Restart IIS.

5. 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. 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).

a) Click on Start -> Administrative Tools -> Active Directory Users and Computers.

b) Right click on Users and select New -> User.

c) Enter the details and click Next.

d) Enter the Password and Confirm password.

e) Click Next and then Finish to create the user.

f) Right click to the user and click Add to group…

g) Type Administrators and click OK. Close the console.

h) Launch the Microsoft IIS Manager.

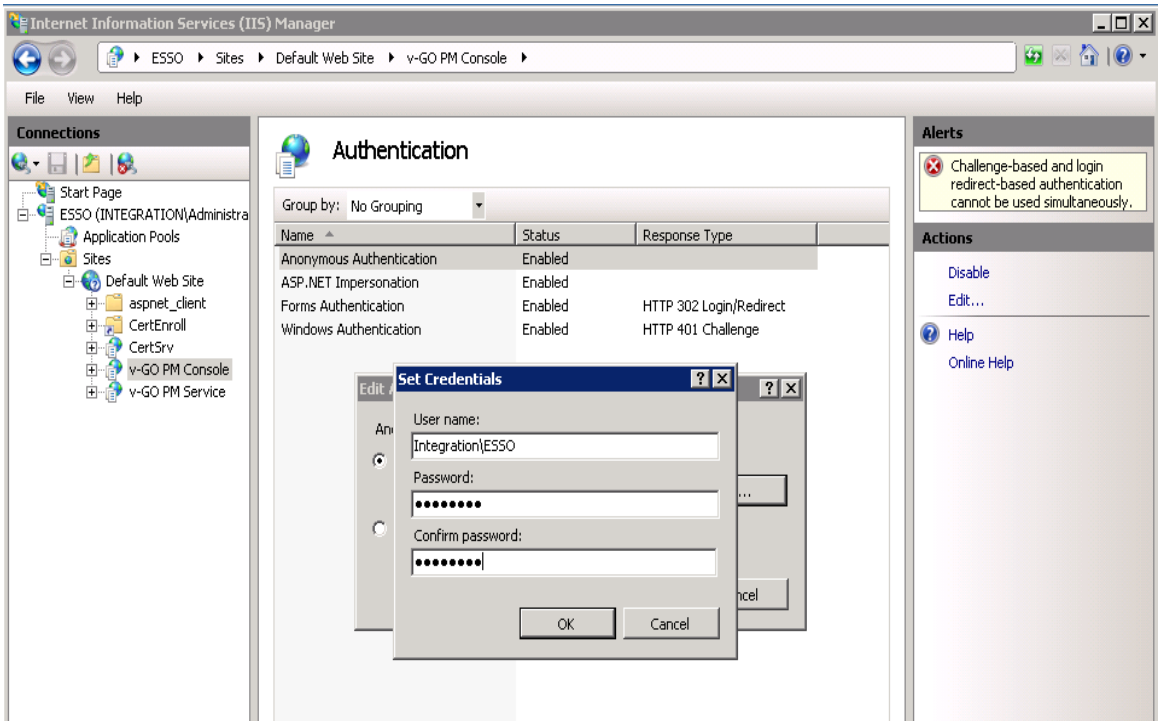
i) In the left-hand tree, drill down to <Server> -> Sites -> Default Web Site and select the ESSO-PG Console site node.

j) In the IIS section of the center pane, double-click Authentication.

k) In the Authentication pane, right-click Anonymous Authentication and select Edit.

l) In the dialog box that appears, select Specific User and click Set.

m) 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.



n) Click OK in the Edit Anonymous Access… dialog to dismiss it.

o) Repeat steps i-n for the ESSO-PG Service site.

p) When you have finished, restart Microsoft IIS to apply your changes.

6. Enabling SSL

Note: IIS Manager does not support the creation of certificates protected by CNG Keys and these need to be created using the Microsoft command line utilities.

Create a certificate request

To generate a request for an SSL certificate linked to a RSA key, create a file called request.inf with the following information:

```
[Version]
Signature= "$Windows NT$"
[NewRequest]
Subject = "C=IN,CN=ESSO.Integration.com,O=SafeNet,OU=TestET,L=GBNagar,S=UP"
HashAlgorithm = SHA1
KeyAlgorithm = RSA
KeyLength = 2048
```

ProviderName = "Safenet Key Storage Provider"
KeyUsage = 0xf0
MachineKeySet = True
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1

1. Specify the subject details of the Domain Controller which is issuing the certificate.
2. Specify the key algorithm and key length as required (e.g. RSA).
3. Specify the Provider name as "Safenet Key Storage Provider"
4. Save the above content in the file request.inf.

To create the certificate request for the Certification Authority, open the command prompt execute the command:

certreq.exe –new request.inf request.req

This creates a certificate request file request.req that can be sent to a Certificate Authority.

Install the Certificate

After creating the certificate request, you obtain the certificate by using the CA web interface. Submit the request to the Certificate Authority and obtain the signed certificate from CA.

To make the certificate available for use in IIS, execute the command

certreq.exe –accept somecert.cer

Where somecert.cer is the binary certificate exported from the CA.

Now Open the command prompt and type MMC and click Enter.

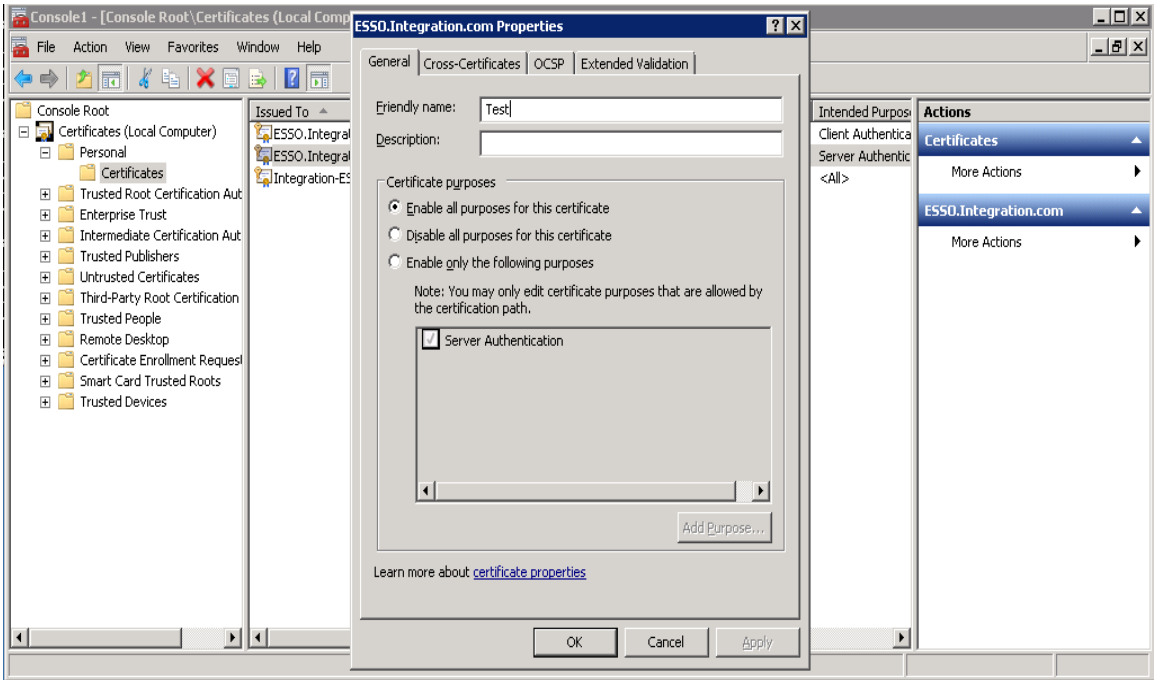
Click File -> Add Remove Snap-in…

Click Certificate -> Add -> Computer Account -> Next -> Local Computer -> Finish -> OK.

Click Certificates (Local Computer) -> Personal -> Certificates.

Right click on the certificate and click Properties.

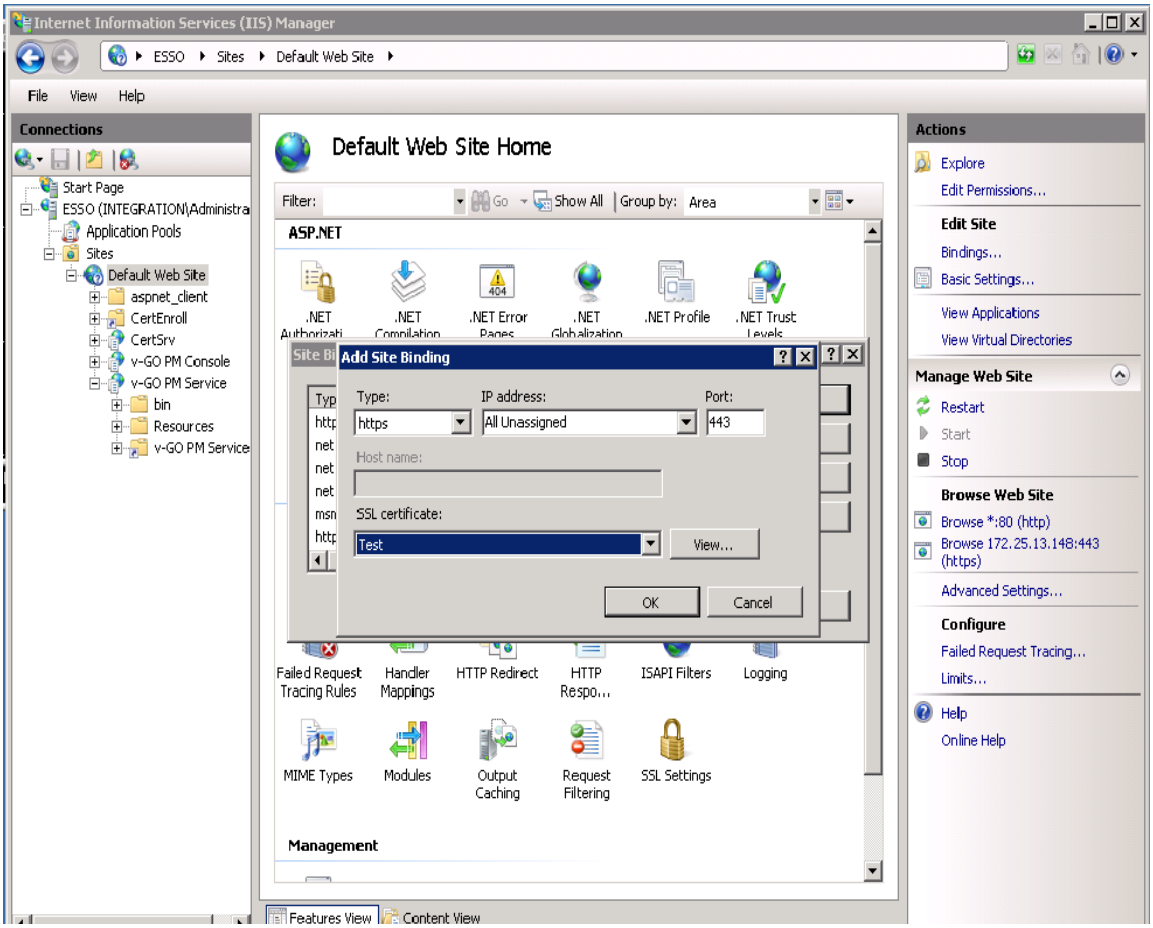
Select General tab, type Friendly name and click OK.



Binding the certificate with IIS Web Server

To bind the certificate with IIS Web Server:

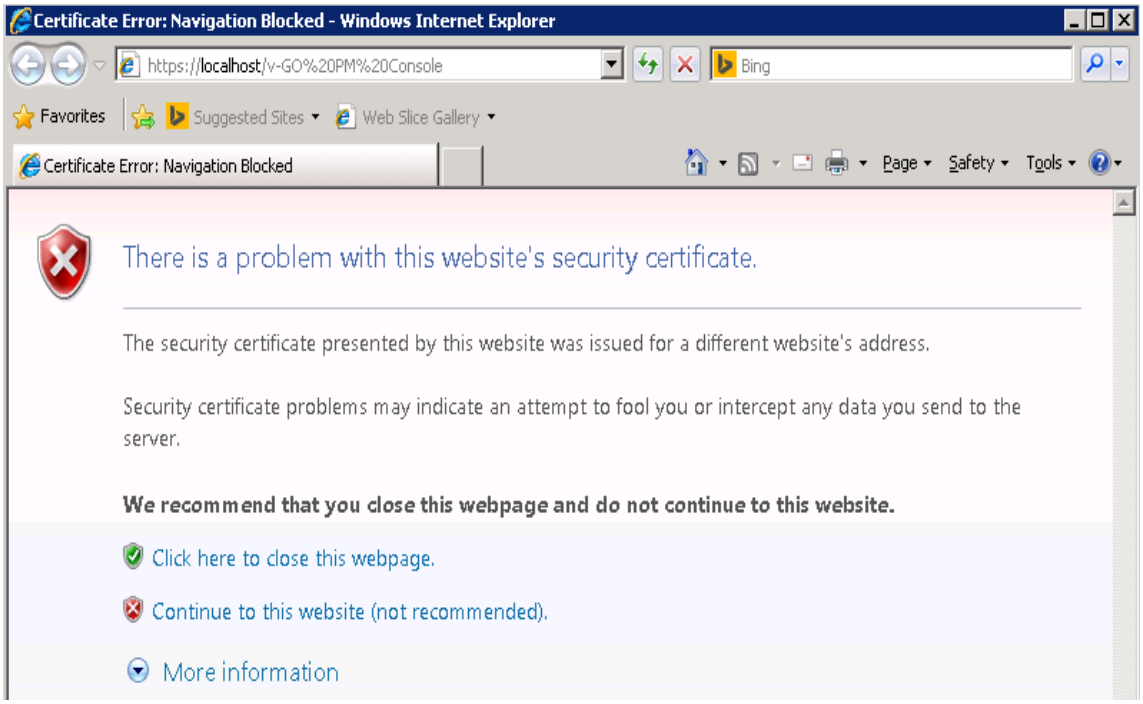
1. Open the IIS Manager from Start > Administrative Tools > Internet Information Services (IIS) Manager.
2. Under Sites on the left hand side of the IIS Manager Window, select the Default Web Site.
3. On the right hand side of the IIS Manager, click the Bindings link.
4. In the Site Bindings window, click Add.
5. Select the protocol as https.
6. Select IP address of machine running IIS from the IP Address dropdown list and port as 443.
7. Select the certificate from the drop-down list.
8. To complete the certificate binding for SSL connection, click OK.



9. Click Close to site Bindings window.
10. Click on the ESSO-PG Console site node.
11. In the console double click on the Application Settings.
12. Right click on the localhost.UP and click Edit and change the prefix of the URL to https i.e.

    https://localhost/v-GO%20PM%20Service/UP.asmx
13. Open the browser and type the https://<server-name>/v-GO PM Console i.e.

    https://localhost/v-GO PM Console
14. If the certificate navigation error occurred then click Continue to this website.



15. Oracle ESSO Provisioning Gateway admin console will display.