Oracle® Enterprise Single Sign-on Provisioning Gateway

Certificate Setup Guide Release 10.1.4.1.0 **E12609-01**

November 2008

ORACLE

Oracle Enterprise Single Sign-on Provisioning Gateway Certificate Setup Guide, Release 10.1.4.1.0

E12609-01

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 Certificate Setup	. 4
Audience	. 4
Using ESSO-PG Certificate Setup	. 5
Installing the Microsoft Certificate Authority	. 6
Enabling SSL for Your Web Site	. 9
Submitting a Certificate Request to a CA Manually	15

About ESSO-PG Certificate Setup

This guide describes how to obtain certificates through Microsoft[®] Certificate Services and how to install a standalone certificate authority (CA), which can be used to issue certificates to anyone, even non-Windows[®] entities.

Audience

This guide is intended for experienced administrators responsible for obtaining certificates and for installing and managing a standalone certificate authority. Persons completing the procedures 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

Using ESSO-PG Certificate Setup

In order to use ESSO-PG, you must obtain an X.509 Certificate for SSL and Certificate Chain from a trusted certificate authority.

Certificates can be obtained from any trusted certificate authority. This purpose of this guide is to demonstrate how certificates can be obtained through Microsoft Certificate Services.

These instructions will guide you through installation of a standalone CA, which can be used to issue certificates to anyone, even non-Windows entities.

Certificates can be installed on Windows 2000 and Windows 2003. The instructions and screen shots in this guide are primarily for Windows 2000. The instructions in this guide can easily be followed using either operating system.



The following pages contain the procedures involved in certificate setup:

- Installing the Microsoft Certificate Authority
- Enabling SSL for Your Web Site
- Submitting a Certificate Request to a CA Manually

Installing the Microsoft Certificate Authority

- 1. Click Start > Settings > Control Panel > Add/Remove Programs.
- 2. Click Add/Remove Windows Components.

🖬 Add/Remov	re Programs		<u> </u>
12	Currently installed programs:	Sort by: Name	•
Change or Remove Programs Add New Programs Add/Remove Windows Components	 Microsoft Data Access Components KB870669 Click here for support information. To change this program or remove it from your computer, click Change/Remove. Microsoft VGX Q833989 Outlook Express Q823353 Windows 2000 Hotfix - KB823182 Windows 2000 Hotfix - KB823559 Windows 2000 Hotfix - KB824105 Windows 2000 Hotfix - KB824141 Windows 2000 Hotfix - KB824195 Windows 2000 Hotfix - KB826232 Windows 2000 Hotfix - KB828028 	⊆hange/Remove	
		Clo	se

3. Check Certificate Services and click Next.

Windows Components Wizard	×
Windows Components You can add or remove components of Windows 2000.	3
To add or remove a component, click the checkbox. A shaded part of the component will be installed. To see what's included i Details.	box means that only n a component, click
Components:	
🗹 📻 Accessories and Utilities	12.1 MB 🔺
Certificate Services	1.4 MB
🗹 🦻 Indexing Service	0.0 MB
🗹 💐 Internet Information Services (IIS)	21.6 MB
🗆 🚔 Management and Monitoring Tools	5.2 MB 🔟
Description: Installs a certification authority (CA) to issue certific public key security applications.	ates for use with
Total disk space required: 1.9 MB	Details
Space available on disk: 522.0 MB	
< <u>B</u> ack	Next > Cancel

4. When you are asked if you want to continue, click Yes.



5. Select Stand-alone root CA.

Certification Authority Type There are four types of certification author	ties.
Certification Authority types:	Description:
C Enterprise root CA	The most trusted CA in a CA
C Enterprise subordinate CA.	Active Directory.
Stand-alone root CA	
O Stand-alone subordinate CA	_
To install an Enterprise CA, the Active Dire member of the Domain Administrator group deselect Certificate Services.	ctory must be accessible and you must be a Please go back to the previous screen and
Auvanceu options	

6. Enter CA Identifying Information. Enter the length of time that this certificate should be valid. Click **Next**.

Windows Components Wizard	×
CA Identifying Information Enter information to identify	n this CA
C <u>A</u> name:	Certificate for PM
Organization:	Company X
Organizational <u>u</u> nit:	
City:	
State or province:	Country/region: US
<u>E</u> -mail:	
CA <u>d</u> escription:	
<u>V</u> alid for:	2 Years Expires: 4/4/2007 2:48 PM
	< Back Next > Cancel

7. Specify the storage location for the configuration data. Click **Next**.

Windows Components Wizard	×
Data Storage Location Specify the storage location for the configuration data, database and log	, 🌆
Certificate database:	
C:\WINNT\system32\CertLog	Br <u>o</u> wse
Certificate database log:	
C:\WINNT\system32\CertLog	Bro <u>w</u> se
Store configuration information in a shared folder Shared folder: C:\CAConfig	Biowse
Preserve existing certificate database	
< <u>B</u> ack <u>N</u> ext >	Cancel

8. You might be prompted to stop IIS. If so, click OK.

Microsoft	t Certificate Services
⚠	Internet Information Services is running on this computer. You must stop this service before proceeding. Do you want to stop the service now?
	Cancel

9. You might be prompted to insert the Windows CD. If so, insert it and click OK.



10. At this point, you might be prompted to enable ASP pages. You must select **Yes**.11. Click **Finish**.

Enabling SSL for Your Web Site

- 1. Open Microsoft IIS and expand the Default Web Site. You will perform the following steps for each ESSO-PG Web site.
- 2. Right-click the Web site (for example, Default Web Site). Click Properties.



3. Select the **Directory Security** tab. Under **Secure communications**, click **Server Certificate**.

Default Web Site Properties	<u>?</u> ×			
Web Site Operators Performance ISAPI Filters Directory Security HTTP Headers Custom I	Home Directory Documents Errors Server Extensions			
Anonymous access and authentication control Enable anonymous access and edit the authentication methods for this resource.	Edit			
IP address and domain name restrictions Grant or deny access to this resource using IP addresses or internet domain names.				
	Edit			
Secure communications				
Require secure communications and enable client certificates when this resource is accessed.	<u>S</u> erver Certificate ⊻iew Certificate E <u>d</u> it			
OK Cancel	Apply Help			

4. The Web Server Certificate Wizard appears. You will use the wizard to generate a request for a certificate. Click **Next**.



5. Select Create a new certificate and click Next.

i Certificate Wizard	2
Server Certificate There are three methods for assigning a certificate to a Web site.	
Select the method you want to use for this web site:	
<u>Create a new certificate</u>	
C Assign an existing certificate	
Import a certificate from a Key Manager backup file.	
< Back Next >	Cancel

6. Select Prepare the request now, but send it later and click Next. If you have an Enterprise-level CA and the machine is part of the domain, a request can be directly prepared. The Send the request immediately to an online certification authority will be available. If you select this option, you do not need to follow the steps in Submitting a Certificate Request to a CA Manually.

Certificate Wizard Delayed or Immediate Requ You can prepare a request immediately.	i est o be sent later, o	r you can send (one	
Do you want to prepare a c immediately to an online cer	rtificate request I ification authority	to be sent later, i?	or do you want to	send it
Prepare the request now	, but send it later			
C Send the request immed	ately to an online	e certification au	thority	
				

7. Enter a name for the new certificate. Ensure that the name is easy to refer to and to remember. Choose the bit length. The higher the bit length, the stronger the encryption, but the slower the performance. Choose a bit length that will balance strength and performance for your needs. For a root CA, you should use a key length of at least 2048 bits. This option is not available if you use existing keys. Click **Next**.

IIS Certificate Wizard	x
Name and Security Settings Your new certificate must have a name and a specific bit length.	Þ
Type a name for the new certificate. The name should be easy for you to refer to and remember.	
Na <u>m</u> e:	
Default Web Site	
The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.	
Bit length:	
Server Gated Cryptography (SGC) certificate (for export versions only)	
< <u>B</u> ack <u>N</u> ext > Cancel	

- 8. Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department. Click **Next**.
- 9. Enter your site's common name. *This name must match the machine name or site URL*. Click Next.



10. Enter your geographical information and click **Next**.

IS Certificate Wizard			×
Geographical Information The certification authority requires the followin	g geographical infor	mation.	
Country/Region: US (United States) ▼			
<u>S</u> tate/province:			
			•
City/jocality:			
			•
State/province and City/locality must be comp abbreviations.	olete, official names	and may not con	tain
	< <u>B</u> ack	<u>N</u> ext >	Cancel

11. Enter a file name for the certificate request. Click **Browse** to locate it. Remember the location of this file as you will open it after completing the request.

ertificate Request File Name			
Your certificate request is saved as a text file wit specify.	h the file name you		
Enter a file name for the certificate request.			
<u>F</u> ile name:			
c:\certreq.txt		Browse	
	Z Dank J	Louis L	Canool

12. Review the summary of your request. Click Next.

IIS Certificate Wizard				×
Request File Summary You have chosen to genera	te a request file.			
To generate the following re	quest, click Next.			
File name: c:\certreq.txt				
Your request contains the fo	llowing information:			
Issued To Friendly Name Country / Region State / Province City Organization Organizational Unit	pqa4iis pqa4iis US New York New York Company X Company X			
		< <u>B</u> ack	<u>N</u> ext >	Cancel

13. Click Finish.

IIS Certificate Wizard		×
	Completing the Web Server Certificate Wizard	
	You have successfully completed the Web Server Certificate wizard. A certificate request was created and saved to the file:	
	c:\certreq.txt	
	Send or e-mail this file to your certification authority, who will send you a response file containing your new certificate. Restart this wizard to attach the new certificate to your server.	
	<u>Click here</u>	
	for a list of certification authorities who offer services for Microsoft products.	
	To close this wizard, click Finish.	
	< Back Finish Cancel	

Submitting a Certificate Request to a CA Manually

1. Locate the certificate request document *(refer to Step 11 for the location)*. Open the text file and copy all of the contents to a clipboard. You will paste the contents into a request in Step 5.



 Open Microsoft Certificate Services. The URL is <u>http://yourmachinename/certsrv/</u>. Select Request a Certificate and click Next.



3. Select Advanced Request and click Next.



4. Select Submit a certificate request using a base64 encoded... file and click Next.



5. In the **Saved Request** text box, paste the contents of the certificate request file copied in Step 1 (or you can browse to locate the file and insert it). Click **Submit**.





6. Your certificate request has been received and is pending.



7. Open the Certificate Authority tool by clicking **Start** > **Programs** > **Administrative Tools** > **Certificate Authority**. Expand the certificate authority.

📴 Certification Authority			
ActionYiew ← → mm _] 🖸 🖫 😫 ▶ ■		
Tree	Name	Description	
Certification Authority (Local)	Certificate for PM	Certification Authority	
, 	,		

8. Click on the **Pending Requests** folder. Click the certificate request in the right pane, and click **All Tasks** > **Issue**.



The Pending Requests folder is now empty.



The certificate moves to the Issued Certificates folder.



9. Open Microsoft Certificate Services. The URL is http://yourmachinename/certsrv/. Select Check on a pending certificate and click Next.



10. Select the certificate that was just created and click **Next**.

Microsoft Certificate Services - Microsoft Internet Explorer	
<u>File Edit Vi</u> ew Favorites <u>I</u> ools <u>H</u> elp	
🗢 Back 🔹 🤿 🗸 🙆 🚰 🧟 Search 😨 Favorites 🛞 Media 🍏 🖏 🖓 🚽 📰 🔹	
Address le http://pqa4iis/certsrv/certckpn.asp	▼ 🔗 Go Links »
	<u>_</u>
Microsoft Certificate Services Certificate for PM	Home
Check On A Pending Certificate Request	
Please select the certificate request you want to check:	
Saved-Request Certificate (Monday April 04 2005 3:07:37 PM)	
	Next >
	*
Done	E Local intranet

11. Click **Download CA certificate.** You can select either DER or Base 64 encoded.

Microsoft Certificate Services - Microsoft Internet Evolorer			
File Edit View Favorites Tools Help			
(⇒ Back • ⇒ • (2) (2) (2) (2) Search (Sal Favorites (2) Media (2) (2) •			
	-	િજેલ્ગા	inke »
		1 (, 30 1	1110
Microsoft Certificate Services Certificate for PM		Home	
Certificate Issued			_
The certificate you requested was issued to you.			
Download CA certificate Download CA certification path			
			-
			-
E Done	📑 🔤 Local i	ntranet	/

12. Save the file to a location on your computer. Download the certificate.



13. Locate the certificate that was just downloaded and double-click it to open it.

Certifica	te Information	
This certificate	is intended to:	
 Ensures th 	e identity of a remote comput	er
Issued to:	pqa4iis	
	C 10 1 C DU	
Issued by:	Certificate for PM	
Valid from	4/4/2005 to 4/4/2006	
		_
	Įnstall Certificate.	Issuer Statement

14. This certificate must now be installed into IIS. Open IIS and locate the Web site where ESSO-PG is installed. Right-click the Web site and click **Properties**.

📲 Internet Information Services				
Action ⊻iew] 🗳 🗟 🗟 😫 🛛 💂 🕨			
Tree	Description	State	Host Header Name	e IP Address
Internet Information Services	🧔 Default Web Site	Running		* All Unas:
🚊 🖳 📕 * pqa4iis	le Administration Web Site	Running		* All Unas:
 ⊕ Ø Default Web Site ⊕ Ø Administration Web Site ⊕ Ø Default SMTP Virtual Server 	Serault SMTP virtual Server	Running		* All Unas
	۱			Þ

15. Select the **Directory Security** tab and click **Server Certificate**.

Default Web Site Properties	? ×
Web Site Operators Performance ISAPI Filters Home Directory Docume Directory Security HTTP Headers Custom Errors Server Extension	ents ns
Anonymous access and authentication 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. Edjt	
Secure communications Require secure communications and enable client certificates when this resource is accessed. Server Certificate View Certificate Egit	
OK Cancel Apply Help)

16. On the Web Server Certificate Wizard panel, click Next.



17. Click Process the pending request and install the certificate. Click Next.

ending Certificate Request		ß
A pending certificate request is a request to authority has not yet responded.	which the certification	
A certificate request is pending. What would	you like to do?	
 Process the pending request and install t 	he certificate	
\bigcirc <u>D</u> elete the pending request		

18. Browse to the location of the saved certificate file. Click Next.

IIS Certificate Wizard		x
Process a Pending Request Process a pending certificate request by retrieving the file that contains the certification authority's response.		
Enter the path and file name of the file containing the certification author	rity's response.	
Path and file name:		
C:\Documents and Settings\Administrator\Desktop\certnew.cer	Browse	
< <u>B</u> ack	t> Can	icel

19. The Wizard asks for the SSL port to use with this Web site. The default SSL Port is 443. Click **Next**.

IIS Certificate Wizard	X
SSL Port Specify the SSL port for this web site.	
SSL port this web site should use:	
	< <u>B</u> ack <u>N</u> ext > Cancel

20. Review the summary of your request. If there are any problems, you might have to issue a new certificate. If everything is correct, click **Next** to install the certificate.

IS Certificate Wizard X Certificate Summary You have chosen to install a certificate from a response file.	
To install the followin	g certificate, click Next.
Certificate details: Issued To Issued By Expiration Date Intended Purpose Friendly Name Country / Region State / Province City Organization Organization	pqa4iis Certificate for PM 4/4/2006 Server Authentication pqa4iis US New York New York New York Company X Company X
	< Back Next > Cancel

21. When the IIS Certificate Wizard is done, click Finish.