Oracle® Enterprise Single Sign-on Password Reset How-To: Configuring SSL Support for the ESSO-PR Web Interface Release 11.1.1.2.0 **20418-01** 



Oracle Enterprise Single Sign-on Password Reset How-To: Configuring SSL Support for the ESSO-PR Web Interface

Release 11.1.1.2.0

20418-01

Copyright © 2010, 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

Table of Contents
Introduction4
About This Guide4
Prerequisites4
Terms and Abbreviations4
Accessing ESSO-PR Documentation4
Part 1: Creating and Installing an SSL Certificate5
Overview5
Step 1: Installing Microsoft Certificate Services6
Step 2: Generating a Certificate Request for the IIS Site Serving the ESSO-PR Web Interface11
Step 3: Submitting the Certificate Request to the Certificate Authority
Step 4: Issuing the Certificate24
Step 5: Installing the Certificate26
Part 2: Configuring the ESSO-PR Web Interface for SSL Connections
Overview
Step 1: Modifying the ESSO-PR Server Configuration Files32
Step 2: Granting ESSO-PR Server Access to the WebServices Directory
Step 3: Restricting Web Interface Connections to SSL Only
Part 3: Testing the New Configuration

## Introduction

## **About This Guide**

This document describes how to create and install an X.509 SSL certificate using Microsoft Certificate Services (MCS) to enable SSL security for ESSO-PR. The instructions in this guide apply to Windows 2000 and Windows Server 2003 families of operating systems. The guide also describes how to configure Microsoft Internet Information Services (IIS) to enable SSL (and disallow non-SSL) connections to the ESSO-PR Web interface.

### **Prerequisites**

Readers of this guide should be familiar with the administration and maintenance of the Windows family of operating systems, and particularly, configuring Microsoft Internet Information Services (IIS). Readers should also understand cryptography concepts such as certificates, certificate authorities, and the Secure Sockets Layer (SSL) technology.

#### **Terms and Abbreviations**

Term or Acronym	Description	
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset	
CA	Certificate Authority	
MCS	Microsoft Certificate Services	
Server	ESSO-PR Server	
Client	ESSO-PR client-side software	
Console	ESSO-PR Administrative Console	

The following table describes the terms and abbreviations used throughout this guide:

#### **Accessing ESSO-PR Documentation**

We continually strive to keep ESSO-PR documentation accurate and up to date. For the latest version of this and other ESSO-PR documents, visit <u>http://download.oracle.com/docs/cd/E15624\_01/index.htm</u>.



## Part 1: Creating and Installing an SSL Certificate

### **Overview**

To enable SSL support for ESSO-PR, you must create and install an X.509 SSL certificate for the IIS Web site serving the ESSO-PR Web interface. The certificate is issued by a Certificate Authority (CA), which can be a commercial entity or a software application on the target local machine. This guide describes how to create a certificate through the latter option using Microsoft Certificate Services (MCS), a component of the Windows 2000 and 2003 families of operating systems.

The steps are:

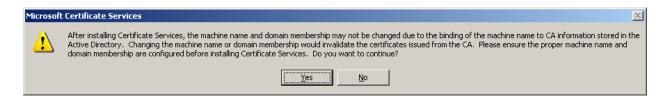
- 1. Installing Microsoft Certificate Services
- 2. Generating a certificate request for the ESSO-PR Web interface IIS site
- 3. <u>Submitting the request to the CA for processing</u>
- 4. Issuing the certificate
- 5. Installing the certificate for the ESSO-PR Web interface IIS site

### **Step 1: Installing Microsoft Certificate Services**

- 1. Open the "Add/Remove Programs" applet:
  - a. Click Start → Settings → Control Panel.
  - b. In the Control Panel, double-click the Add/Remove Programs icon.
- 2. In the "Add/Remove Programs" applet, click Add/Remove Windows Components.
- 3. In the **Components** list, select **Certificate Services**.

Windows Components Wizard	×
Windows Components You can add or remove components of Windows.	<b>E</b>
To add or remove a component, click the checkbox. A shade part of the component will be installed. To see what's included Details.	
Components:	
🗹 📻 Accessories and Utilities	4.9 MB 🔺
Active Directory Services	16.7 MB 🚽
Application Server	33.4 MB
🗹 🙀 Certificate Services	1.4 MB
🗆 🖗 Distributed File System	7.7 MB
Description: Installs a certification authority (CA) to issue certif public key security programs.	icates for use with
Total disk space required: 3.1 MB	Details
Space available on disk: 2967.1 MB	
< <u>B</u> ack <u>N</u> ext >	Cancel Help

4. When the following warning appears, read it carefully, then click **Yes** to proceed.



5. Click Next.

6. In the "CA Type" dialog, select **Stand-alone root CA** and click **Next**.

Windows Components Wizard	×
CA Type Select the type of CA you want to set up.	S.
<ul> <li>Enterprise root CA</li> <li>Enterprise subordinate CA</li> <li>Stand-alone root CA</li> <li>Stand-alone subordinate CA</li> <li>Description of CA type The most trusted CA in a CA hierarchy.</li> </ul>	
< <u>B</u> ack <u>N</u> ext > Cancel Help	



7. In the "CA Identifying Information" dialog, fill in the appropriate fields and click **Next**.

Windows Components Wizard				×
CA Identifying Information Enter information to identify				đ
Common name for this CA:				
ssocert				
Distinguished name suffix:				
DC=ssolab,DC=com				
Preview of distinguished name	:			
CN=ssocert,DC=ssolab,DC=c	om			
Validity period: 5 Years ▼		Expiration date 10/29/2013 9:		
	< <u>B</u> ack	<u>N</u> ext >	Cancel	Help

8. Wait for the cryptographic key to be generated, then proceed to the next step.

9. In the "Certificate Database Settings" dialog, enter the desired paths. If unsure, leave the fields at their default values. When you're finished, click **Next**.

Windows Components Wizard	×
<b>Certificate Database Settings</b> Enter locations for the certificate database, database log, and configura information.	ation
<u>C</u> ertificate database:	
C:\WINDOWS\system32\CertLog	Browse
, Certificate <u>d</u> atabase log:	
C:\WINDOWS\system32\CertLog	Bro <u>w</u> se
Store configuration information in a shared folder	
S <u>h</u> ared folder:	
C:\CAConfig	Browse
Preserve existing certificate database	
< <u>B</u> ack <u>N</u> ext > Cance	I Help

10. When prompted to temporarily stop IIS, click Yes.

Microsof	t Certificate Services
1	To complete the installation, Certificate Services must temporarily stop the Internet Information Services. Do you want to stop the service now?
	<u>∑Yes</u> <u>N</u> o



11. Wait for the installation to complete. If you are prompted for your Windows CD-ROM, insert it, and follow the displayed instructions.

Windows Components Wizard
Configuring Components Setup is making the configuration changes you requested.
Please wait while Setup configures the components. This may take several minutes, depending on the components selected.
Status: Examining installed files
< Back Next > Cancel Help

12. When prompted to enable Active Server Pages, click **Yes**.

Microso	ft Certificate Services
1	Active Server Pages (ASPs) must be enabled in Internet Information Services (IIS) in order to allow Certificate Services to provide web enrollment services. Enabling ASPs is a potential security risk and must be carefully evaluated. You can enable ASPs later if you choose not to do it now. IIS must be manually reconfigured later to enable this functionality. Do you want to enable Active Server Pages now?
	<u>Yes</u> <u>N</u> o

13. When the "Windows Components Wizard" completes, click Finish.

Microsoft Certificate Services is now installed. Proceed to the next section to generate a certificate request.

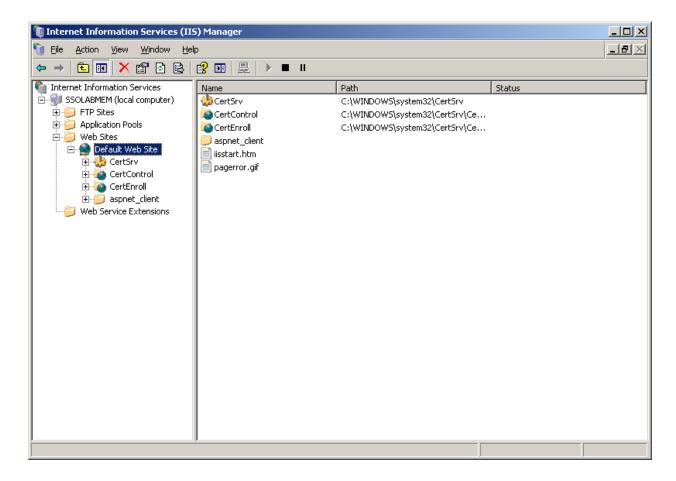


# Step 2: Generating a Certificate Request for the IIS Site Serving the ESSO-PR Web Interface

Once you have access to a trusted Certificate Authority, you must generate a certificate request for the IIS site serving the ESSO-PR Web interface. You will submit this request to the CA for processing as described later in this guide.

**Note:** You must perform this procedure for every ESSO-PR Web interface site served by IIS within the domain.

- Launch the IIS Manager. Click Start → Programs → Administrative Tools → Internet Information Services (IIS) Manager.
- In the tree in the left-hand pane, expand Web Sites and right-click the IIS site serving the SSPR Web interface. Typically, this will be Default Web Site. Select Properties from the context menu.



3. In the dialog that appears, select the **Directory Security** tab.



4. In the Secure communications section, click Server Certificate.

Default Web Site	Properties			? ×
Web Site Documents	Performance Directory Security	ISAPI Filters HTTP Head	- · ·	Directory
• , E	and access control inable anonymous access an uthentication methods for t		<u>E</u> dit	
	d domain name restrictions - irant or deny access to this P addresses or Internet don		Edįt	
e 🛁 e	nications equire secure communicatio nable client certificates whe esource is accessed.		( <u>S</u> erver Certific <u>V</u> iew Certifica E <u>d</u> it	
	ок	Cancel	Apply	Help

- 5. When the "Web Server Certificate Wizard" dialog appears, click **Next**.
- 6. In the "Server Certificate" dialog, select **Create a new certificate** and click **Next**.

IIS Certificate Wizard	×
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:	
< <u>B</u> ack <u>N</u> ext >	Cancel

- 7. In the "Delayed or Immediate Request" dialog, select **Prepare the request now, but send it later** and click **Next**.
  - Note: The Send the request immediately to an online certification authority option is not available unless an Enterprise-level CA exists on the domain of the target machine. In such cases you may select the option to generate and submit the certificate request immediately. If you do so, skip the steps in the next section and continue directly to <u>Step 4</u>: <u>Issuing the Certificate</u> once you complete this procedure.

IIS Certificate Wizard 🛛 🕺
Delayed or Immediate Request You can prepare a request to be sent later, or you can send one immediately.
Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?
Prepare the request now, but send it later
C Send the request immediately to an online certification authority
< <u>B</u> ack <u>N</u> ext > Cancel

- 8. In the "Name and Security Settings" dialog, name your certificate and set its bit length. Keep the following in mind:
  - Choose a descriptive name that is easy to refer to and to remember.
  - For a root CA, we recommend a bit length of at least 2048 bits.
  - The longer the bit length, the stronger the encryption; however, stronger encryption requires more server resources. In the end, the bit length you choose will depend on the needs of your organization.
  - If you are using existing keys, the certificate's bit length cannot be changed.

IIS Certificate Wizard	×
Name and Security Settings Your new certificate must have a name and a specific bit length.	>
Type a name for the new certificate. The name should be easy for you to refer to and remember. Name:	
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: 1024	
Select cryptographic service provider (CSP) for this certificate	
< <u>B</u> ack ( <u>Next</u> >) Cancel	

#### ORACLE<sup>®</sup>

9. In the "Organization Information" dialog, select or enter the desired values, then click **Next**.

IIS Certificate Wizard
Organization Information Your certificate must include information about your organization that distinguishes it from other organizations.
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. For further information, consult certification authority's Web site. Organization:
ssolab
Organizational <u>u</u> nit:
ssolab
< <u>B</u> ack Cancel

10. Enter the *exact* name of the target machine, or the *exact* URL of the IIS site serving the ESSO-PR Web interface, whichever applies to your configuration. Click **Next**.

IIS Certificate Wizard	×
Your Site's Common Name Your Web site's common name is its fully qualified domain name.	
Type the common name for your site. If the server is on the Internet, use a valid D name. If the server is on the intranet, you may prefer to use the computer's NetBIC name.	NS )S
If the common name changes, you will need to obtain a new certificate.	
Common name:	
ssolabmem	
< <u>B</u> ack	Cancel



11. In the "Geographical Information" dialog, fill in the fields as appropriate, then click **Next**.

IIS Certificate Wizard	×
Geographical Information The certification authority requires the fol	lowing geographical information.
<u>C</u> ountry/Region: US (United States) <b>▼</b>	
<u>S</u> tate/province:	
NY	•
City/locality:	
New York	•
State/province and City/locality must be abbreviations.	complete, official names and may not contain
	< Back Next > Cancel

12. In the "Certificate Request File Name" dialog, enter the name of the file to which your request will be saved, then click **Next**.

IIS Certificate Wizard	×
Certificate Request File Name Your certificate request is saved as a text file with the file name you specify.	
Enter a file name for the certificate request.	
<u>F</u> ile name:	
T:\certreq.txt	Browse
,	
< Back	Cancel



#### ORACLE<sup>®</sup>

13. In the summary dialog, review your choices and click **Back** if you need to make changes. If all the information is correct, click **Next**.

IIS Certificate Wizard		×
Request File Summary You have chosen to generate a	a request file.	
To generate the following requ	est, click Next.	
File name: c:\certreq.txt		
Your request contains the follow	ving information:	
Issued To Friendly Name Country/Region State / Province City Organization Organizational Unit	ssolabmem Default Web Site US NY New York ssolab ssolab	
	< <u>B</u> ack <u>N</u> ext>	Cancel

14. When the wizard completes, click **Finish**.

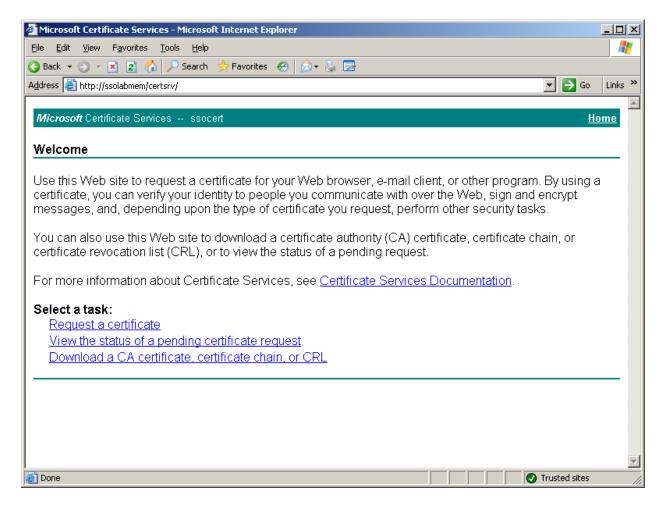
Your certificate request has been saved to a file and, if applicable, submitted to your enterprise CA. Your next step is one of the following:

- If you chose to submit the request manually, proceed to <u>Step 3: Submitting</u> the Certificate Request to the Certificate Authority.
- If you chose to submit the request automatically, proceed to <u>Step 4: Issuing the</u> <u>Certificate</u>.



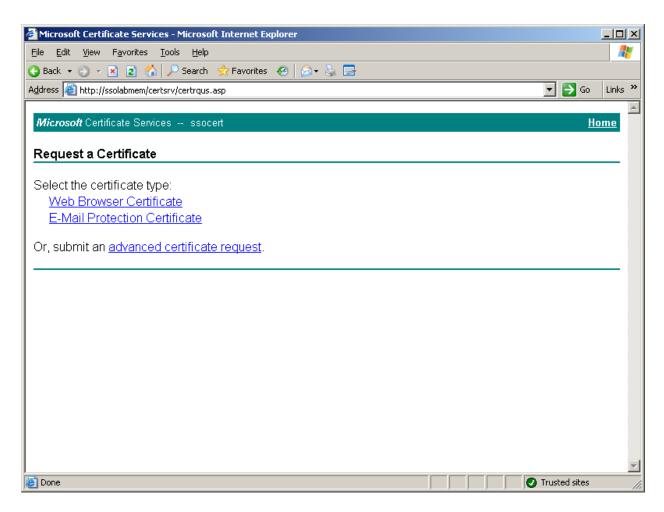
## **Step 3: Submitting the Certificate Request to the Certificate Authority**

 Go to <u>http://<machine\_name>/certsrv/</u> to access the Microsoft Certificate Services Web interface.



2. Click Request a certificate.

3. On the next page, click **advanced certificate request**.



4. On the next page, click **Submit a certificate request by using a [...] file**.

Microsoft Certificate Services - Microsoft Internet Explorer			<u>- 0 ×</u>
File Edit View Favorites Tools Help			
G Back ▼ (2) ▼ N 2 (2) /> Search ☆ Favorites ④ (2) ▼ 3 2			
Address 🕘 http://ssolabmem/certsrv/certrqad.asp	•	ightarrow Go	Links »
		_	<b>A</b>
<i>Microsoft</i> Certificate Services ssocert		Ho	me
Advanced Certificate Reguest			
Advanced Certificate Request			—
The policy of the CA determines the types of certificates you can request. Click one c	of the following	options	to:
Create and submit a request to this CA.			
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file.	or submit a re	newal	
request by using a base-64-encoded PKCS #7 file.			
			_
http://ssolabmem/certsrv	🕖 Trust	ed sites	

- 5. Submit the certificate as follows:
  - a. Locate the certificate request file you generated earlier in this guide and open it in a text editor.
  - b. Copy the entire contents of the file and paste them into the **Saved Request** field on the page that appears.
  - c. Click Submit.

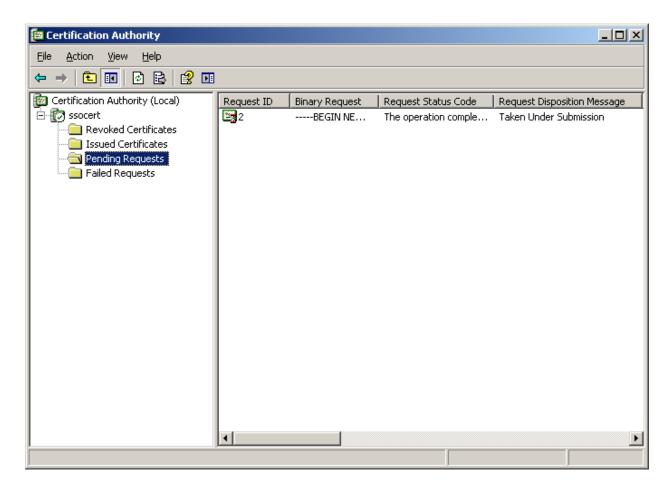
Misseeft Castifies	ate Services - Microsoft Internet Explorer	_ 🗆 ×
File Edit View F		
	labmem/certsrv/certrqxt.asp	Links »
Microsoft Certific	ate Services ssocert	lome
Submit a Certi	ficate Request or Renewal Request	
	red request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request on val request generated by an external source (such as a Web server) in the Saved Reques	
Saved Request:		
certificate request (CMC or PKCS #10 or PKCS #7):	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
Additional Attribu	ites:	
Attributes:		
	Submit >	•
ē)	Trusted sites	

Your certificate request is now pending approval. Proceed to the next section to approve it and issue the certificate.

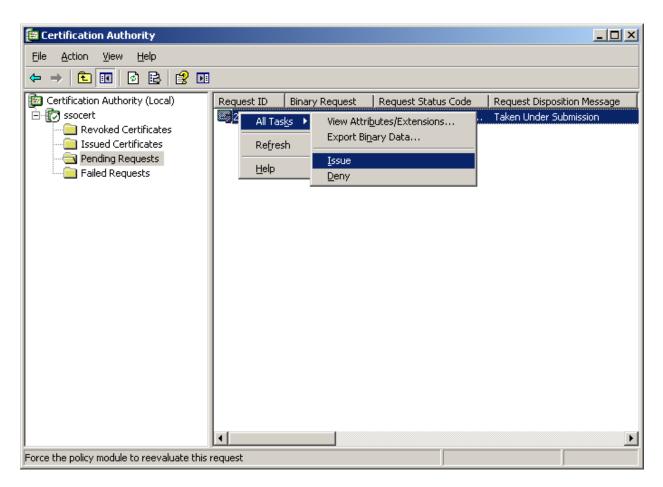
## **Step 4: Issuing the Certificate**

Issue the certificate as follows:

- Launch the Certification Authority tool. Click Start → Programs → Administrative Tools → Certification Authority.
- 2. In the left-hand pane, expand the root tree node and click **Pending Requests**. The request you submitted earlier is listed in the list of pending requests.



 Right-click the pending request and select All Tasks → Issue from the context menu. The certificate is issued and the request disappears from the list.

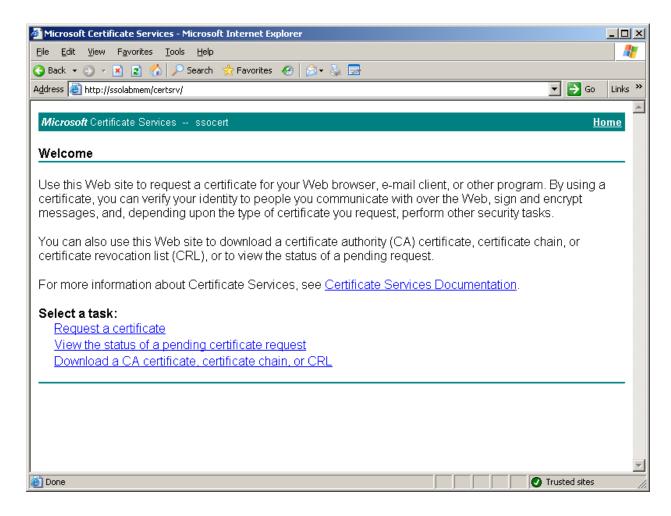


4. Verify that the certificate has been successfully issued. Click **Issued Certificates** in the left-hand pane and verify that your certificate appears in the list.

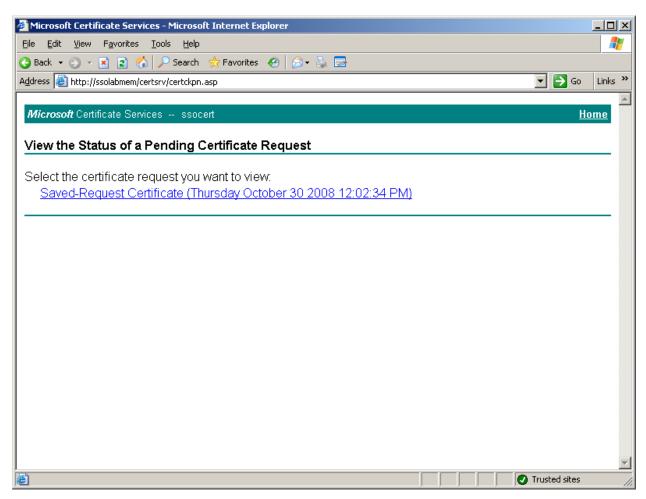
## **Step 5: Installing the Certificate**

Once the certificate has been issued, it must be installed for the ESSO-PR Web interface IIS site. This procedure assumes that the ESSO-PR Web interface is served by the default web site in IIS.

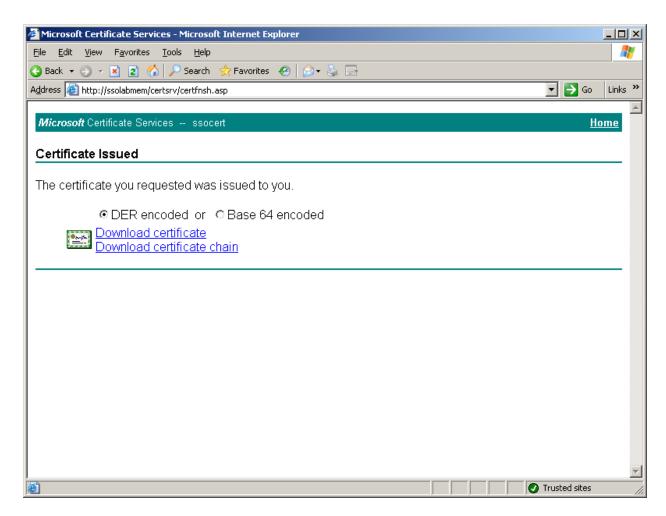
- 1. Return to the Microsoft Certificate Services Web interface and click **Home** in the upper right corner.
- 2. On the MCS home page, click View the status of a pending certificate request.



3. On the next page, click the certificate request you created earlier in this section.



4. On the next page, click **Download certificate**.



- 5. When prompted whether to open or save the certificate file, click **Save**.
- 6. In the dialog that appears, navigate to the target location for the file and click **Save**.
- 7. Install the certificate:
  - a. If it is not already running, launch the IIS Manager.
  - b. In the left-hand pane, expand the root node, then expand **Web Sites**.
  - c. Right-click **Default Web Site** and select **Properties** from the context menu.
  - d. In the dialog that appears, select the **Directory Security** tab.
  - e. In the "Secure communications" field, click Server Certificate.
  - f. In the wizard that appears, click **Next**.
  - g. In the "Pending Certificate Request" dialog, select **Process the pending request and install the certificate**, then click **Next**.

IIS Certificate Wizard	×
Pending Certificate Request A pending certificate request is a request to which the certification authority has not yet responded.	
A certificate request is pending. What would you like to do?	
Process the pending request and install the certificate	
C <u>D</u> elete the pending request	
< <u>B</u> ack <u>Next</u> >	Cancel

h. Enter the absolute path or navigate to the certificate file, then 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 <u>P</u> ath and file name:	ity's response.
c:\*.cer	B <u>r</u> owse
< <u>B</u> ack <u>N</u> ext >	Cancel

i. Specify the SSL port for the ESSO-PR Web interface site and click **Next**. The default value is 443.

IIS Certificate Wizard	×
SSL Port Specify the SSL port for this web site.	
SS <u>L</u> port this web site should use:	
	< <u>B</u> ack <u>Next</u> > Cancel



j. Review the information displayed in the summary dialog. If the information is correct, click **Next**.

IIS Certificate Wizard	2	<
Certificate Summary You have chosen to i	nstall a certificate from a response file.	
To install the following	g certificate, click Next.	
File name:	C:\Documents and Settings\Administrator.SSOL\certnew.cer	
Certificate details: Issued To Issued By Expiration Date Intended Purpose Friendly Name Country/Region State / Province City Organization Organizational Unit	ssolabmem ssocert 10/30/2009 Server Authentication Default Web Site US NY New York ssolab ssolab	
	< <u>B</u> ack Next > Cancel	

- k. In the dialog that appears, take note of the Issued To value (ssolabmem in our example). You will use this value to modify the ESSO-PR Server configuration files later in this document.
- I. Click **Finish** to exit the wizard.

The certificate is now installed. Proceed to the next section to configure the ESSO-PR Web interface to accept SSL-only connections.



## Part 2: Configuring the ESSO-PR Web Interface for SSL Connections

This part describes the steps necessary to configure ESSO-PR to accept SSL-encrypted connections to its Web interface.

**Note:** If you have not already done so, install an SSL certificate by completing the steps earlier in this document.

#### **Overview**

The steps required to enforce SSL-only connections to the ESSO-PR Web Interface are as follows:

- 1. Modifying the ESSO-PR Server Configuration Files
- 2. Granting ESSO-PR Server Access to the WebServices Directory
- 3. Restricting Web Interface Connections to SSL Only

### Step 1: Modifying the ESSO-PR Server Configuration Files

You must update the following configuration files to use the HTTP-over-SSL (HTTPS) protocol when calling the ESSO-PR Server Web interface pages:

- C:\Program Files\Passlogix\v-GO SSPR\EnrollmentClient\web.config
- C:\Program Files\Passlogix\v-GO SSPR\ManagementClient\web.config
- C:\Program Files\Passlogix\v-GO SSPR\ResetClient\web.config

- 1. Modify the \EnrollmentClient\web.config file as follows:
  - a. Locate the <appSettings> section.
  - b. Modify the EnrollSvc.enrollment key value as follows:
    - i. Change http to https.
    - ii. Replace localhost with the Issued To value from your SSL certificate.You recorded this value in step 7k on page 31.
    - iii. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon.

For example: http://sssolabmem.ssolab.com:1880

c. Save and close the file.

📴 Web.config - Notepad File Edit Format View Help	
"Passport" and "None"	
>	_
<authentication mode="windows"></authentication> <identity impersonate="true"></identity>	
APPLICATION-LEVEL TRACE LOGGING</td <td></td>	
Application-level tracing enables trace log output for every page within an	
application.' Set trace enabled="true" to enable application trace logging. If	
pageOutput="true", the	
trace information will be displayed at the bottom of each page. Otherwise, y	/ou
can view the	ion
root.	. 1011
> /tease packled "false" permant imit "10" personant "false"	
<pre><trace enabled="false" localonly="true" pageoutput="false" requestlimit="10" tracemode="SortByTime"></trace></pre>	
SESSION STATE SETTINGS</p	
By default ASP .NET uses cookies to identify which requests belong to a particular session.	
If cookies are not available, a session can be tracked by adding a session	
identifier to the URL.	
To disable cookies, set sessionState cookieless="true". >	
	24 "
<pre><sessionstate <="" cookieless="false" data="" id='sa;password="' mode="InProc" pre="" source="127.0.0.1;user" stateconnectionstring="tcpip=127.0.0.1:4242 sqlConnectionString="></sessionstate></pre>	
timeout="20"/> GLOBALIZATION</td <td></td>	
This section sets the globalization settings of the application.	
>	
<pre><globalization requestencoding="utf-8" responseencoding="utf-8"></globalization> </pre>	
<appsettings></appsettings>	
<pre><add key="EnrollSvc.enrollment" value="https://ssolabmem/vgoselfservicereset/webservices/enrollment.asmx"></add></pre>	
<pre></pre>	

- 2. Modify the \ManagementClient\web.config file as follows:
  - a. Locate the <appSettings> section.
  - b. Modify the AdminSvc.Administration key value as follows:
    - i. Change http to https.
    - ii. Replace localhost with the Issued To value from your SSL certificate.You recorded this value in step 7k on page 31.
    - iii. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon.

For example: http://sssolabmem.ssolab.com:1880

c. Save and close the file.

	- 🗆 >
jie <u>E</u> dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp	
"Passport" and "None" >	-
<pre><authentication mode="Windows"></authentication> <identity impersonate="true"></identity> <!-- APPLICATION-LEVEL TRACE LOGGING Application-level tracing enables trace log output for every page within an</pre--></pre>	
application.	
Set trace enabled="true" to enable application trace logging. If	
pageOutput="true", the trace information will be displayed at the bottom of each page. Otherwise, yo	u
an view the application trace log by browsing the "trace.axd" page from your web applicati root.	on
> <trace <br="" enabled="false" pageoutput="false" requestlimit="10">raceMode="SortByTime" localonly="true"/&gt; <!-- SESSION STATE SETTINGS<br-->By default ASP .NET uses cookies to identify which requests belong to a</trace>	
particular session. If cookies are not available, a session can be tracked by adding a session	
identifier to the URL. To disable cookies, set sessionState cookieless="true".	
> <sessionstate <br="" cookieless="false" data="" id='sa;password="' mode="InProc" source="127.0.0.1;user" stateconnectionstring="tcpip=127.0.0.1:42424&lt;br&gt;sqlConnectionString=">imeout="20"/&gt;</sessionstate>	"
GLOBALIZATION<br This section sets the globalization settings of the application.	
> <globalization requestencoding="utf-8" responseencoding="utf-8"></globalization>	
<pre> <appsettings> <add alue="https://ssolabmem/VgoSelfServiceReset/WebServices/Administration.asmx" key="AdminSvc.Administration"></add> </appsettings></pre>	

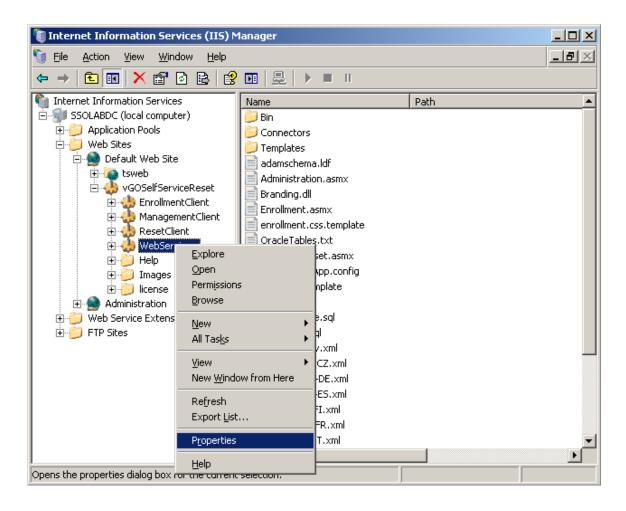
- 3. Modify the \ResetClient\web.config file as follows:
  - a. Locate the <appSettings> section.
  - b. Modify the ResetSvc.PasswordReset key value as follows:
    - i. Change http to https.
    - ii. Replace localhost with the Issued To value from your SSL certificate.You recorded this value in step 7k on page 31.
    - iii. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon.
       For example: http://sssolabmem.ssolab.com:1880
  - c. Modify the AdminSvc.Administration key value as follows:
    - iv. Change http to https.
    - v. Replace localhost with the Issued To value from your SSL certificate. You recorded this value in step 7k on page 31.
    - vi. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon. For example: http://sssolabmem.ssolab.com:1880
  - d. Save and close the file.

🕞 Web.config - Notepad	
<u>File Edit Format View Help</u>	
<pre>&gt;</pre>	n
<pre> <appsettings> <add <add="" key="AdminSvc.administration" value="https://ssolabmem/vgoselfservicereset/webservices/administration.asmx"></add> <add key="Resetsvc.PasswordReset" value="https://ssolabmem/vgoSelfServiceReset/webServices/PasswordReset.asmx"></add> </appsettings></pre>	Ŧ

## Step 2: Granting ESSO-PR Server Access to the WebServices Directory

Complete the following steps to grant the ESSO-PR Server access to the **WebServices** virtual directory:

- 1. Launch the Internet Information Services (IIS) Manager console.
- 2. In the tree in the left-hand pane, navigate to and expand the **vGoSelfServiceReset** site node.
- Right-click the WebServices node, located under the vGOSelfServicePasswordReset, and select Properties from the context menu that appears.



- 4. In the dialog that appears, select the **Directory Security** tab.
- 5. In the **Directory Security** tab, click **Edit** in the **IP address and domain name restrictions** section.

WebServices Propertie	5	<u>? ×</u>			
HTTP Headers Virtual Directory	Custom Errors Documents	ASP.NET Directory Security			
Authentication and a Enable authent	ccess control anonymous access and edit the ication 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.					
enable 🛁	ns secure communications and lient certificates when this e is accessed.	Server Certificate View Certificate Edit			
	OK Cancel	Apply Help			

- 6. Grant the IP address of the ESSO-PR Server machine access to the **WebServices** directory:
  - a. In the dialog that appears, select **Denied Access**. The dialog displays a list of IP addresses explicitly excluded from the global deny rule.
  - b. Click Add.

IP Address and	Domain Name Res	strictions	×
	cess restrictions	A.C	
Except the fo	l computers will be: llowing:	♂ ○ Granted access	
Access	IP address (Subnet	mask)	
of Granted	🛄 127.0.0.1		<u>Ad</u> d
			Re <u>m</u> ove Edi <u>t</u> ,
	ОК	Cancel <u>H</u> elp	



c. In the dialog that appears, select **Single Computer**, enter the target IP address, and click **OK**.

Grant Access	×
Туре:	
Single computer	
O Group of computers	
O Domain name	
IP address:	
10 . 0 . 0 .124 D <u>N</u> S Lookup	
Cancel <u>H</u> elp	

## Step 3: Restricting Web Interface Connections to SSL Only

1. In the tree in the left hand pane in IIS Manager, right-click **vGOSelfServiceReset** and select **Properties** from the context menu.

🐚 Internet Informatio	on Services (IIS) M	1anager				
🧐 Eile <u>A</u> ction <u>V</u> iew	<u>W</u> indow <u>H</u> elp		<u>_8×</u>			
Internet Information : SSOLABDC (local Application Pol Web Sites Service Administ Web Service FTP Sites	Services computer) ols 'eb Site	Name  EnrollmentClient  ManagementClient  ManagementClient  WebServices  Help  ss  e ChangePasswordSvc.exe	Path           C:\Program Files\Passlogix\v-GO SSPR\En           C:\Program Files\Passlogix\v-GO SSPR\Ma           C:\Program Files\Passlogix\v-GO SSPR\Re           C:\Program Files\Passlogix\v-GO SSPR\Re           C:\Program Files\Passlogix\v-GO SSPR\Wa			
Opens the properties dialo	g box for the current	selection.				



- 2. In the dialog that appears, select the **Directory Security** tab.
- 3. In the **Directory Security** tab, click **Edit** in the **Secure communications** section.

WebServices Pro	operties					<u>? ×</u>
	HTTP Headers Virtual Directory		ustom Errors uments	Direct	ASP.NET tory Security	
	n and access o Enable anonym authentication	ious access	and edit the r this resource.	Edit		
IP address and domain name restrictions Grant or deny access to this resource using IP addresses or Internet domain names. Edit.						
<b>~</b> 0	unications Require secure enable client ce resource is acco	ertificates w		Server Cer View Cert	ificate	
		ок	Cancel	Apply	He	lp



- 4. In the dialog that appears, do the following:
  - a. Select the Require secure channel (SSL) check box.
  - b. (Optional) If your environment requires 128-bit encryption, select the **Require 128-bit encryption** check box.
  - c. Click OK.

Secure Communications	×					
Require secure channel (SSL)						
Require <u>1</u> 28-bit encryption						
Client certificates						
<ul> <li>Ignore client certificates</li> </ul>						
O Accept client certificates						
C 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. Edit	_					
OK Cancel <u>H</u> elp						

- 5. Click **OK** in the parent dialog to close it.
- 6. Restart Internet Information Services for the changes to take effect.

## Part 3: Testing the New Configuration

Using a Web browser, access each of the ESSO-PR Web interface services using the new SSL-enabled URLs (i.e., using the https protocol header in place of http). The URLs are as follows:

- EnrollmentClient: https://<new\_host\_name>:<new\_port>/vGOSelfServiceReset/ WebServices/Enrollment.asmx
- ManagementClient: https://<new\_host\_name>:<new\_port>/vGOSelfServiceReset/ WebServices/Administration.asmx
- ResetClient:

https://<new\_host\_name>:<new\_port>/vGOSelfServiceReset/
WebServices/PasswordReset.asmx

If any of the URLs fail to load, check your configuration, such as virtual directory permissions and certificate options, then try again.