



GUMU™ Sage ERP Integration (Pro) for Salesforce

SSL CERTIFICATE INSTALLATION GUIDE



Contents

Introduction.....	3
SSL Certificate Request.....	3
SSL Certificate Installation	7



INTRODUCTION

GUMU™ Sage ERP Integration (Pro) for Salesforce – SSL Certificate Installation Guide assists you to how configure required settings for SSL Certificate Installation.

The SSL Certificate is must be signed by public CA (Certificate Authorities) like VeriSign, DigiCert etc. in order to secure data communication between Salesforce and ERP. It will keep you data safe while both system communication.

Only following public CA certificate supported in Salesforce. Link as follows...

https://developer.salesforce.com/page/Outbound_Messaging_SSL_CA_Certificates

SSL CERTIFICATE REQUEST

If you have “Microsoft Server 2003 or 2008” and IIS 7 and above is installed on the server then it is pretty easy to request a certificate for the server with domain name.

The below steps needs to follow in order to request a certificate.

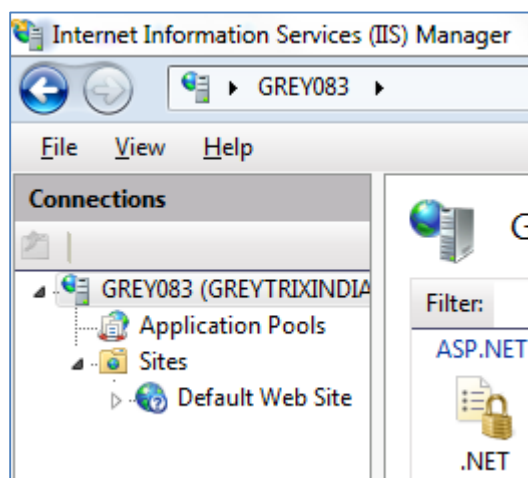
Step 1: Open IIS -

Go to Control Panel → Administrative Tools → Internet Information Services (IIS) Manager

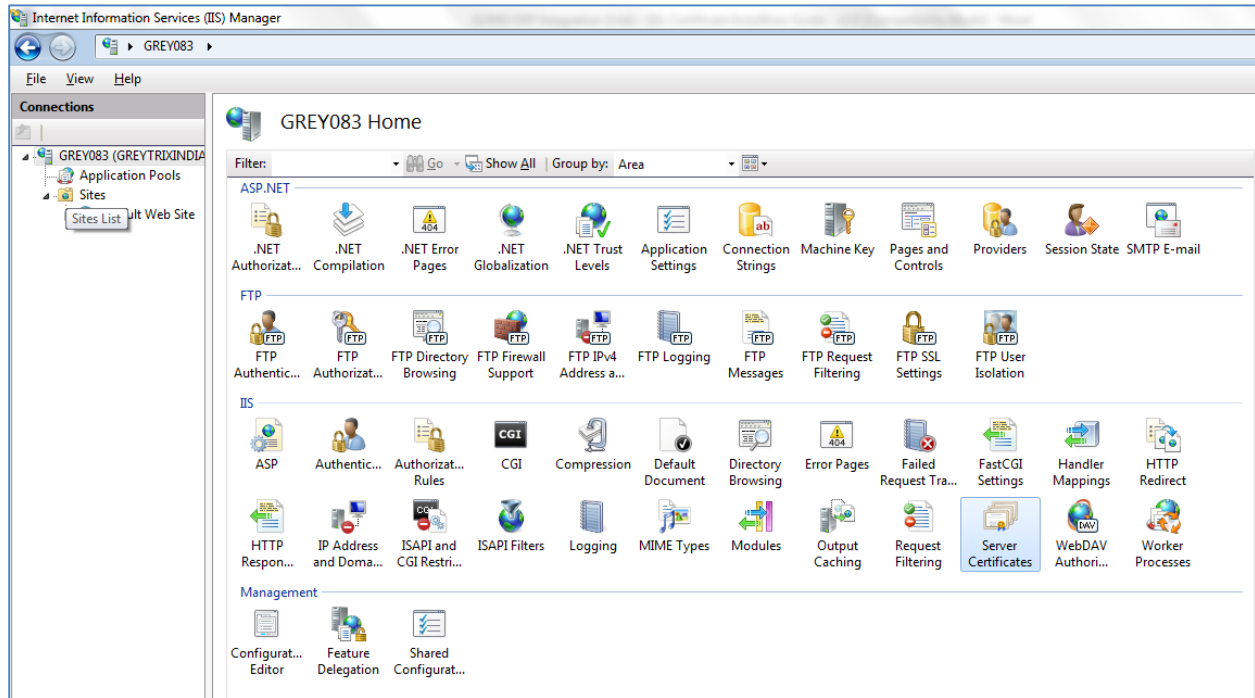
OR

Open “Run” window and type “inetmgr” command and select OK. It is a shortcut to open IIS.

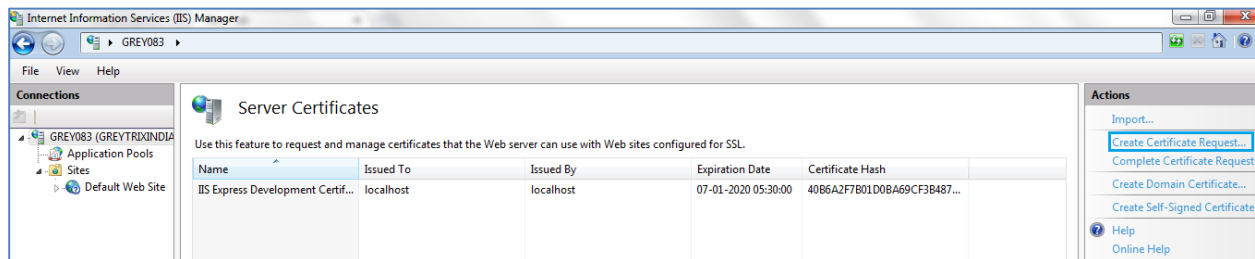
Step 2: Click on the main IIS Folder as highlighted in below screen shot from the left pane and an appropriate options will be populated in right section.



Step 3: Double Click on “Server Certificates” from right pane.



Step 4: The “Server Certificates” pane will be opened then need to click on “Create Certificate Request” from right most pane on the screen. See below screen shot.



Step 5: Then new window will be open... and you need to provide the appropriate information. See sample information filled in the below screen shot.

On the **Distinguished Name Properties** page of the **Request Certificate Wizard**, type the following information, and then click **Next**.

- In the **Common name** text box, type a name for the certificate.
- In the **Organization** text box, type the name of the organization in which the certificate will be used.



- In the **Organizational unit** text box, type the name of the organizational unit in the organization in which the certificate will be used.
- In the **City/locality** text box, type the unabbreviated name of the city or locality where your organization or organizational unit is located.
- In the **State/province** text box, type the unabbreviated name of the state or province where your organization or organizational unit is located.
- In the **Country/region** text box, type the name of the country or region where your organization or organizational unit is located.

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: integration.abc.com

Organization: ABC Ltd

Organizational unit: Dev

City/locality: California

State/province: CA

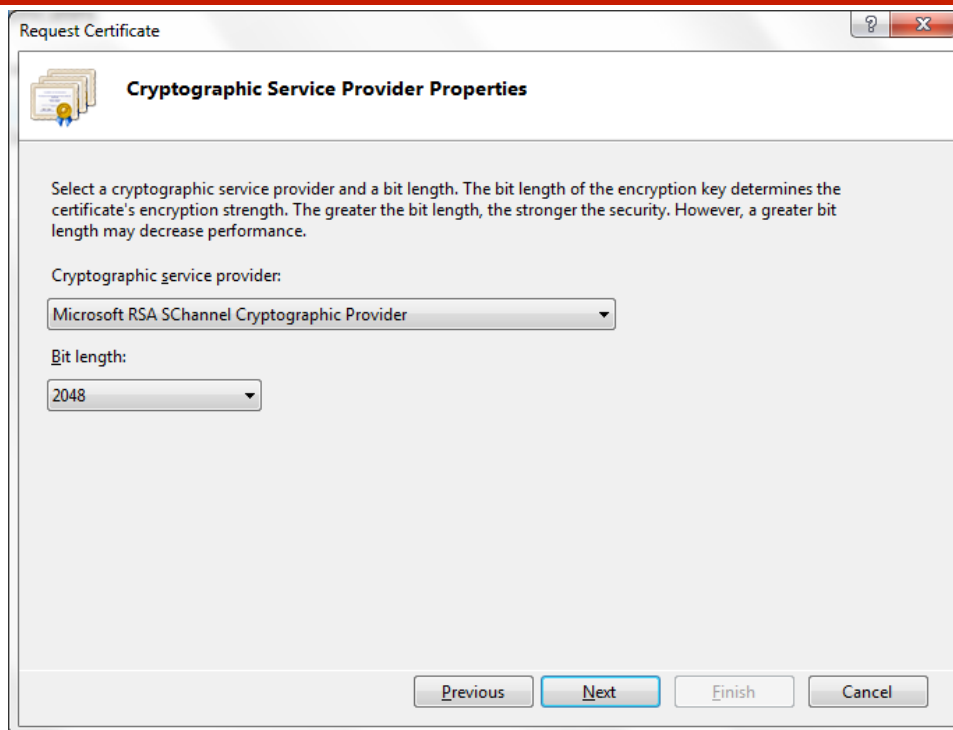
Country/region: US

Previous Next Finish Cancel

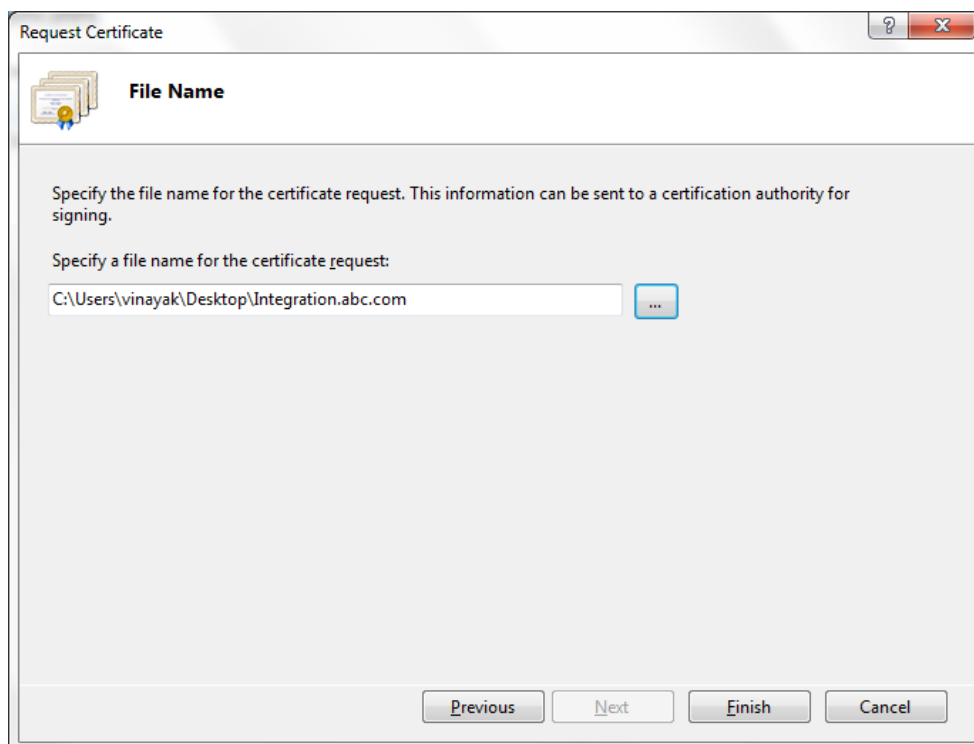
Step 6: On the **Cryptographic Service Provider Properties** page, select either **Microsoft RSA SChannel Cryptographic Provider** or **Microsoft DH SChannel Cryptographic Provider** from the **Cryptographic service provider** drop-down list. By default, IIS 7 uses the Microsoft RSA SChannel Cryptographic Provider.

In the **Bit length** drop-down list, select a bit length that can be used by the provider. By default, the RSA SChannel provider uses a bit length of 1024. The DH SChannel provider uses a bit length of 512. A longer bit length is more secure, but it can affect performance.

Click **Next**.



Step 7: On the **File Name** page, type a file name in the **Specify a file name for the certificate request** text box, or click the browse button (...) to locate a file, and then click **Finish**.





Step 8: Send saved certificate request file to a public CA.

SSL CERTIFICATE INSTALLATION

Install an Intermediate Certificate in Microsoft IIS 7

1. Click **Start**, and then click **Run...**
2. Type **mmc**, and then click **OK**. The Microsoft Management Console (Console) window opens.
3. In the **Console1** window, click the **File** menu, and then select **Add/Remove Snap-in**.
4. In the **Add or Remove Snap-in window**, select **Certificates**, and then click **Add**.
5. In the **Certificates snap-in window**, select **Computer Account**, and then click **Next**.
6. In the **Select Computer window**, select **Local Computer**, and then click **Finish**.
7. In the **Add or Remove Snap-in window**, click **OK**.
8. In the **Console1** window, click + to expand the folder.
9. Right-click **Intermediate Certification Authorities**, mouse-over **All Tasks**, and then click **Import**.
10. In the **Certificate Import Wizard** window, click **Next**.
11. Click **Browse** to find the intermediate certificate file.
12. In the **Open** window, change the file extension filter to **PKCS #7 Certificates (*.spc;*.p7b)**, select the ***_iis_intermediates.p7b** file, and then click **Open**.

NOTE: Do not install your Leaf Certificate in this area. Doing so removes your certificate from the list, and you must reinstall to correct the problem.

13. In the **Certificate Import Wizard** window, click **Next**.
14. Select **Place all certificates in the following store**, and then click **Browse**.
15. In the **Select Certificate Store** window, select **Intermediate Certification Authorities**, and then click **OK**.
16. In the **Certificate Import Wizard** window, click **Next**.
17. Click **Finish**.
18. Click **OK**.
19. Close the **Console 1** window, and then click **No** to remove the console settings.

To Install an SSL Certificate in Microsoft IIS 7

1. Click **Start**, mouse-over **Administrative Tools**, and then click **Internet Services Manager**.
2. In the **Internet Information Services (IIS) Manager** window, select your server.
3. Scroll to the bottom, and then double-click **Server Certificates**.
4. From the **Actions** panel on the right, click **Complete Certificate Request...**
5. To locate your certificate file, click
6. In the **Open** window, select *.* as your file name extension, select your certificate (it might be saved as a .txt, .cer, or .crt), and then click **Open**.
7. In the **Complete Certificate Request** window, enter a **Friendly name** for the certificate file, and then click **OK**.



NOTE: For Wildcard SSL certificates make sure your **Friendly Name** matches your Common Name (i.e. *.coolexample.com).

8. In the **Internet Information Services (IIS) Manager** window, select the name of the server where you installed the certificate.
9. Click + beside **Sites**, select the site to secure with the SSL certificate.
10. In the **Actions** panel on the right, click **Bindings...**
11. Click **Add...**
12. In the **Add Site Binding** window:
 - For **Type**, select **https**.
 - For **IP address**, select **All Unassigned**, or the IP address of the site.
 - For **Port**, type **443**.
 - For **SSL Certificate**, select the SSL certificate you just installed, and then click **OK**.
13. Close the **Site Bindings** window.
14. Close the **Internet Information Services (IIS) Manager** window. Your SSL certificate installation is complete.

Visit your website at **<https://www.coolexample.com>** (replacing *coolexample.com* with your domain name) to verify the installation.