Project Cost Mobile Configuration Guide

For:

Microsoft Dynamics ™ GP

Version

14.01

PROJECT COST BY OLYMPIC SYSTEMS, INC.

Project Cost Mobile Configuration Guide

3800 Aurora Ave North • Suite 360
Seattle, WA 98103
Phone 206.547.5777 • Fax 206.547.4933

Table of Contents

Prerequisite Software and Settings

Before you can install the Project Cost Mobile Connector software, you must complete the installation of the following:

1. Microsoft Dynamics GP
2. Internet Information Services (IIS)
3. ASP.NET.
4. Dexterity Shared Components
5. Project Cost Web Suite

Before you get started:

Submit Organization Key Request

Submit the URL of your Mobile Connector Web Service to MobileConnect@projectcost.net.

The URL should use the following scheme format:

Without SSL
http://SubDomain.Domain.TLD:89/ProjectCostService.svc

With SSL
https://SubDomain.Domain.TLD:443/ProjectCostService.svc

Terms:
Sub Domain – refers to an additional prefix added to a domain name and separated by a period.
Domain – refers to a name used in URL's to identify particular web page.
Top Level Domain (TLD) – is a suffix that points to the Top Level Domain a web site belongs to.
External Port Number – is the connection port designated in the web site bindings.

Example: http://time.projectcost.net:89/ProjectCostService.svc

Additionally, you must specify the Project Cost Employee UserID that shall administer the Mobile Connector portal site. This user can then grant or revoke access to the mobile app, as well as configure certain default settings and mail integration.

You will then be provided with an Organization Key

Project Cost Mobile Connector IIS Install Process

Copy Project Cost Mobile Connector components to the Inetpub Directory

1. These components are held in the folder **MobileConnector** that was included in the Download.
2. Use Windows Explorer to copy the **MobileConnector** directory to your **Inetpub**

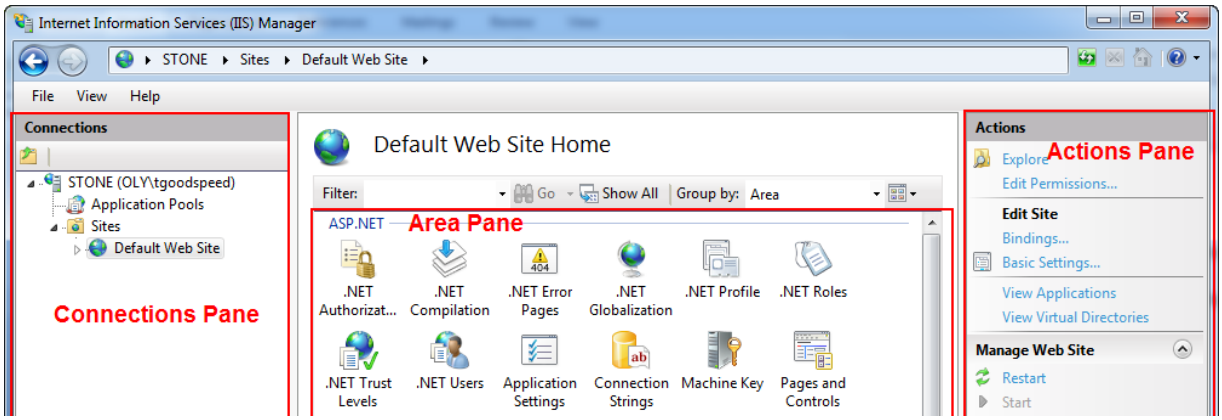
In this instruction we located this folder at **C:\Inetpub\MobileConnector**

Configuration of Internet Information Services on Windows 7

1. Navigate to the Control Panel.

   Note: Based on the operating system the commands may be different for this navigation.
   Using Windows 7 – go to **Control Panel>>System and Security>>Administrative Tools.**

2. Double click **"Internet Information Services (IIS) Manager".**
3. In the Internet Information Services window is divided into 3 primary areas or panes.
   a. The **Connections Pane** you should see the server's name, Application Pools and Sites.
   b. The **Area Pane** will list the features that may be configured and will look different based on the item selected in the **Connections Pane**.
   c. The **Actions Pane** again will look different based on the feature selected in the **Area Pane**.



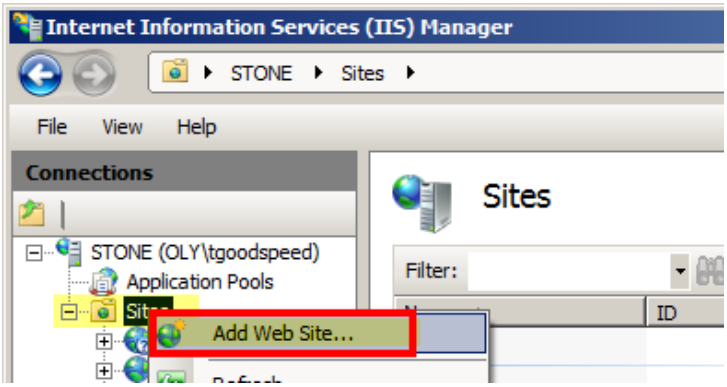
4. In the **Connections Pane** Click on the "►" to expand the **Server** view.

   This should expose folders for Application Pools and Sites.

Create New MobileConnector Web Site

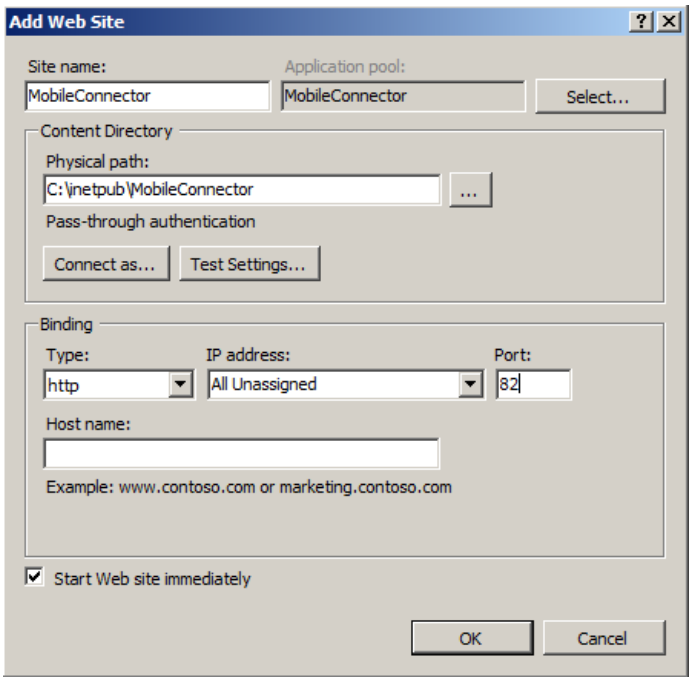
In the Connections Pane

1. Click on the "►" to expand the **Site** view.
2. Right Click on **Sites**
3. Select **Add Web Site**



In the Add Web Site window

1. Enter the Site Name: in our example we use **MobileConnector**.
2. Enter the Physical path:
   This is the location of the mobile connector components.
   In our example we use c:\Inetpub\MobileConnector
3. Enter the port number in the Binding area. We use 82 to avoid common conflicts with other IIS tools.
4. Click OK

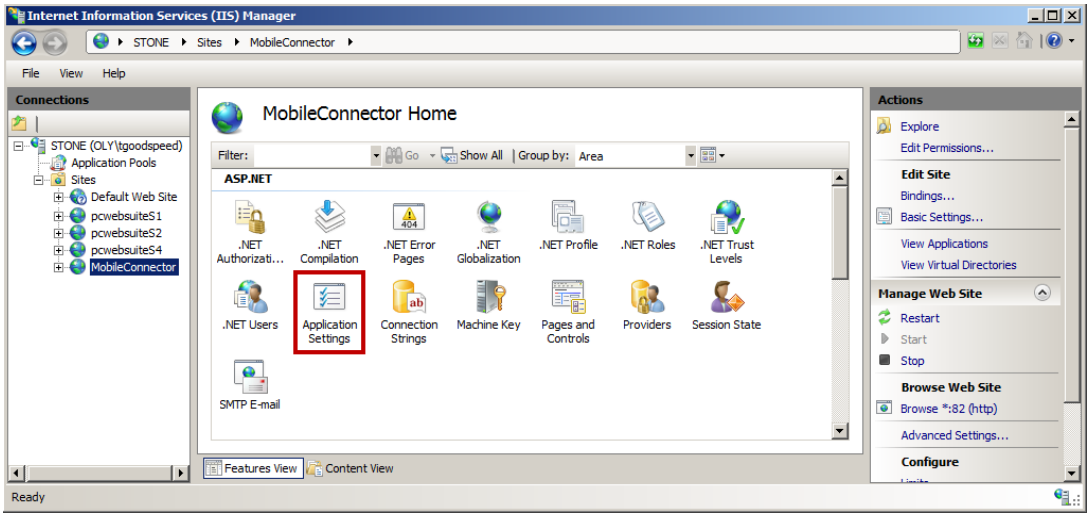


Configure MobileConnector Web Site Settings

In the Connections Pane

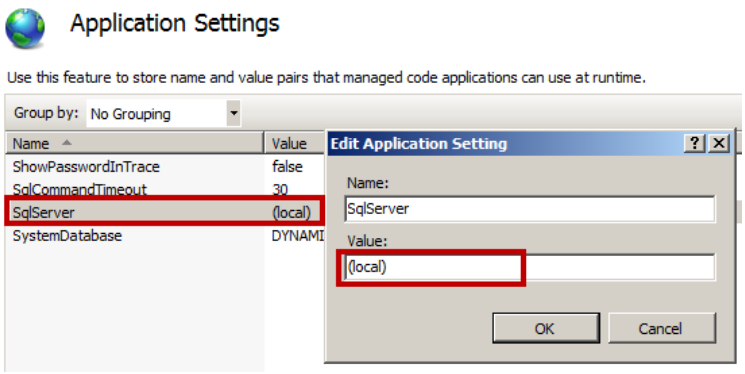
1. Click on the "►" to expand the **Site** view.
2. Click on the Site - in our example **MobileConnector.**
3. In the **Area Pane** under the **ASP.Net** section Double-Click on **Application Settings** icon.

If ASP.NET section is not visible in the Actions Pane See Trouble shooting section.



In the Application Setting Pane

1. Double-Click on **SqlServer** Feature.
2. In the **Edit Application Setting window**

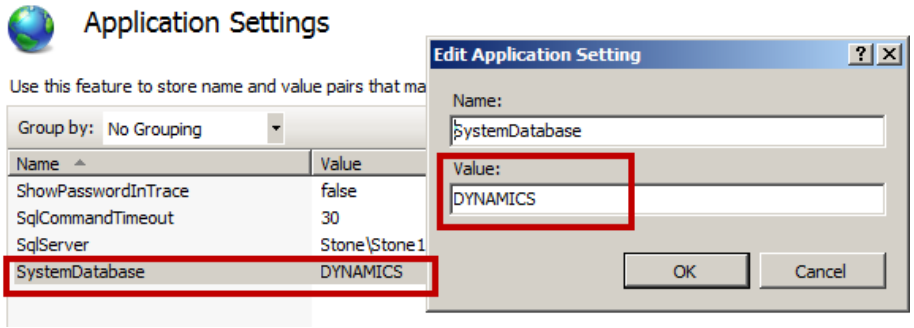


3. Enter the Name and Instance of your Sql Server in the Value field.

4. Click **OK**

In the Application Setting Pane

1. Double-Click on **SystemDatabase** Feature.



2. In the Edit Application Setting window

   Enter the Name of the GP system database. This is normally DYNAMICS however in v2013 an option to use a Named System Database was added.

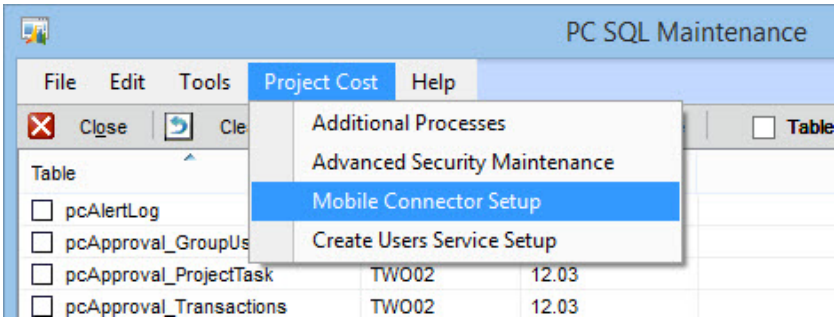
3. Click **OK**

Project Cost Mobile Connector Security Setup

Navigate to Project Cost SQL Maintenance Window

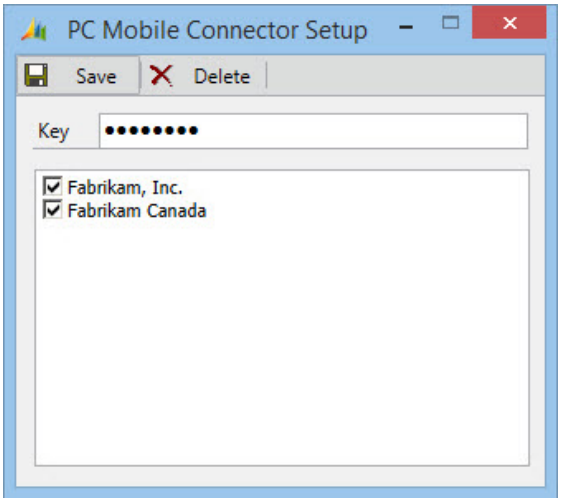
Microsoft Dynamics GP >> Tools >> Utilities >> Project Cost >> SQL Maintenance

- On the PC SQL Maintenance window Select Project Cost option.
- Select Mobile Connector Setup option



In the PC Mobile Connector Setup Window

- Enter the SQL Login name to be used by MoveOn Software:
- Enter the Password:
- Click the Check Box next to the Company database name.
- Click **Save** button.



Project Cost Mobile Connector Admin Portal

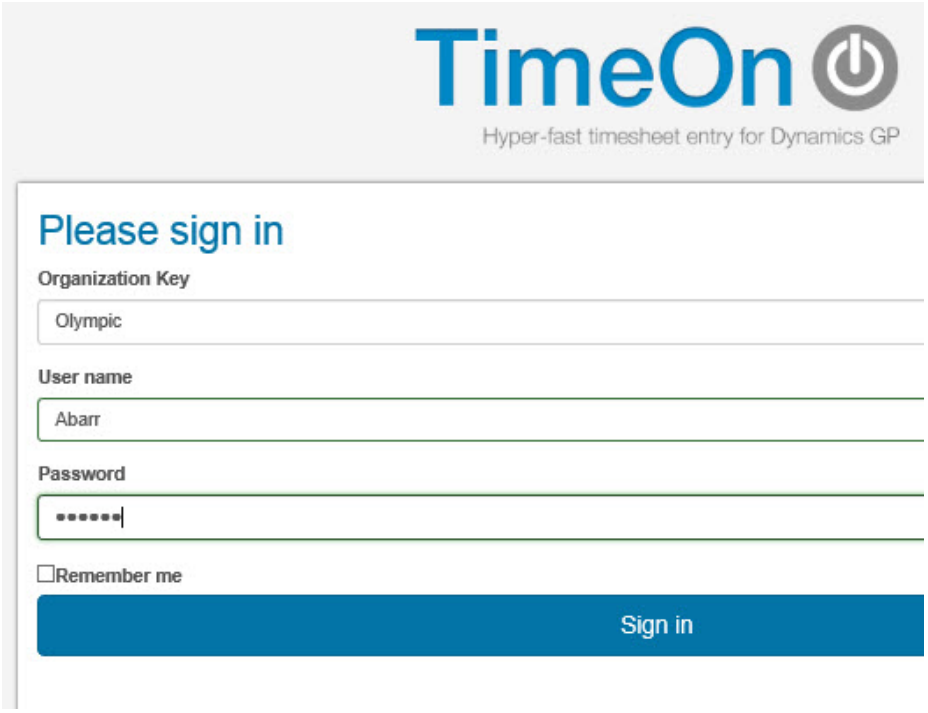
Mobile Connector - Admin Portal Logon

To access the Connector Admin Portal navigate to: http://timeon.apcurium.com:8040

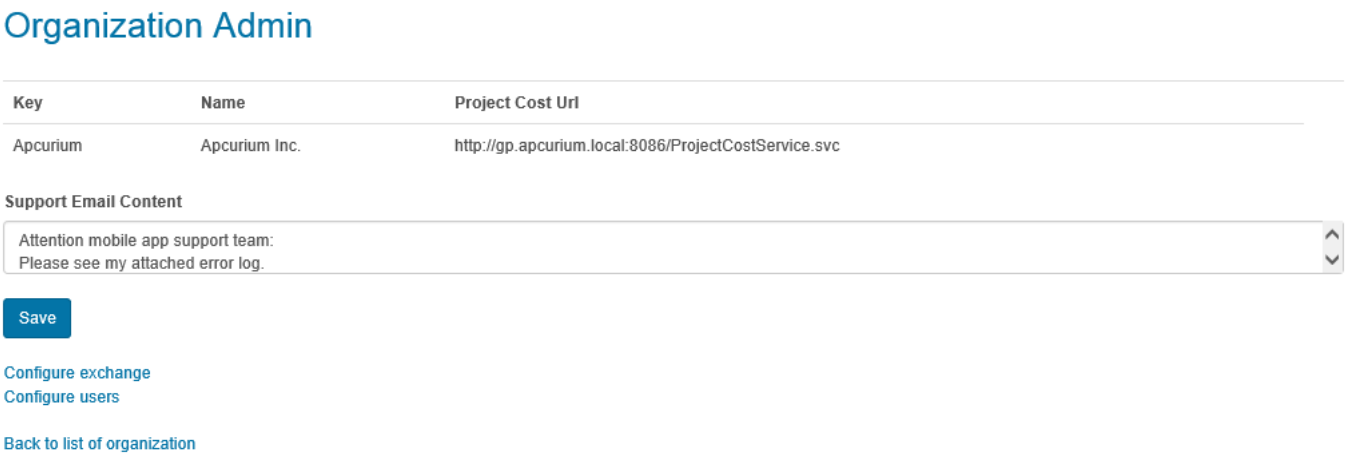
Enter the Organization Key

Enter the username (the Employee UserID you provided when requesting the Organization Key)

Enter the password



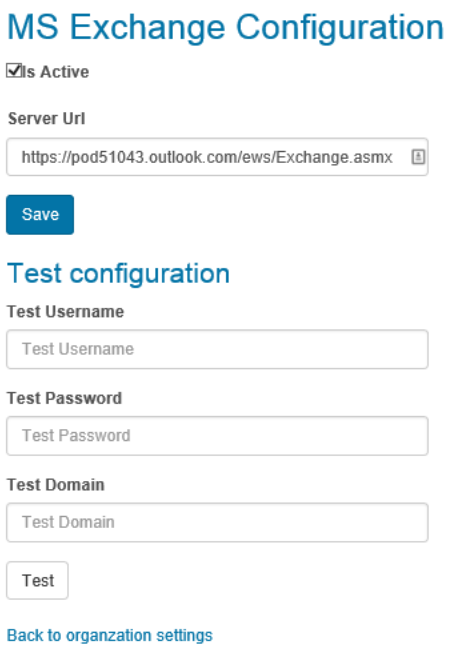
Mobile Connector - Organization Admin Support Email Default Message



As seen in the above screen, you may specify a default message body for emails support emails sent from users in the event of a problem.

Mobile Connector - Organization Admin MS Exchange Configuration

Select Configure exchange in order to specify your organization's MS Exchange Configuration

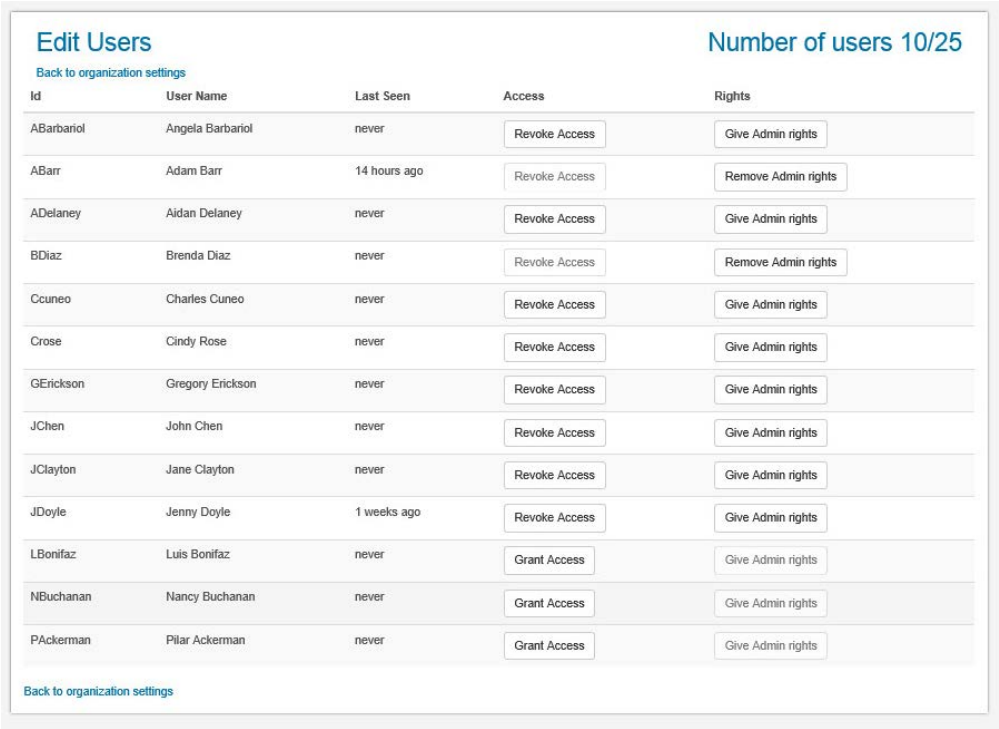


In the fields provided, specify your Organization's MS Exchange web service URL.

> Your Exchange administrator should provide the URL, and account credentials needed to test it.

Select "Back to organization settings", and then "Configure users"

Mobile Connector - Organization Admin Configure User Access



1. You may now grant access to each of your Olympic Project Cost employees. You may "Give Admin rights" to any user that should access the Mobile Connector Access Portal.

When you Grant Access, a Welcome Email is sent to each user, with instructions to download the mobile app.

Users must first be fully setup in Project Cost. See Project Cost User Guide for instructions on setup.

Mobile Connector - Organization Admin Welcome Email Template

The Welcome Email will be sent to the address on record for each employee in the PC User Setup window.

The email contents are:

> Dear <Firstname> <Lastname>,
>
> You've been given access to <Your Company>'s mobile app for Time & Expense. To get started, please download the app from the app store.
>
> Apple (iOS) users: https://itunes.apple.com/app/id703732379
> Google (Android) users: https://play.google.com/store/apps/details?id=com.apcurium.TimeOn&hl=en
>
> Your credentials
>
> Organization is : <Organization Key>
> Login username is : <PC EmployeeID>
> Password : use your existing Olympic Web Suite password.
>
> If you don't remember your password, please contact your Dynamics GP administrator.

Security Certificates & SSL for Project Cost Web Suite

WE HIGHLY RECOMMEND THAT USERS DEPLOY PROJECT COST WEB SUITE USING SECURE SOCKETS LAYER (SSL) OR SOME OTHER TRANSPORT LAYER SECURITY (TLS) PROTOCOL. WHILE THIS IS OPTIONAL FOR MOST OF OUR FUNCTIONALITY – IT IS REQUIRED IF THE ORGANIZATION WANTS TO USE CREDIT CARD STATEMENT DOWNLOAD FEATURE.

Security Certificates & SSL

Security certificates and secure sockets layer (SSL) are used to help improve the security of the data being transmitted by the Project Cost web Suite. The web site that hosts the web client *must* be configured to use SSL. The runtime service must be configured to use a security certificate.

Security Certificate Requirements

The security certificates that you use for your Project Cost Web Suite installation must meet some requirements to work properly.

Certificate Purpose

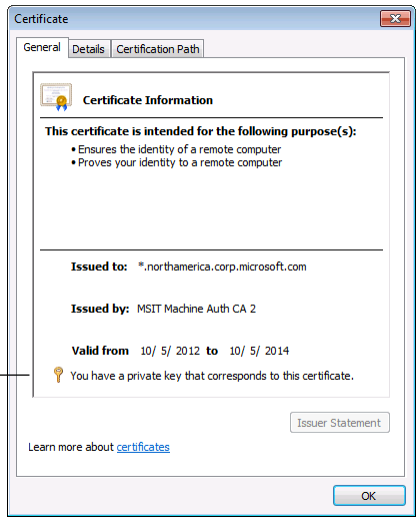
To be used for the Project Cost Web Suite, the security certificate must have "Server Authentication" listed as one of its intended purpose. You can use the Certificates snap-in for the Microsoft Management Console to view the Intended Purpose column for the certificate.

Private Key

It is essential that the security certificate that you are using has a private key. This allows the security certificate to be bound to the port that is assigned to the web site.

To verify that the security certificate has a private key, you can view the details of the certificate file. At the bottom of the details, you should see that the certificate has private key. If it does not, then the security certificate cannot be used.

The security certificate must have a private key in order to be bound to the runtime service port.



Externally Signed Security Certificates

Externally signed security certificates are the easiest way to implement SSL for the Project Cost Web Suite. They must be purchased from the third-party supplier. Due to the additional cost, externally signed security certificates are typically used in a production environments.

There are three basic types of externally signed security certificates:

Single Domain

This type of security certificate is issued for a specific machine. For example you could get a security certificate issued for the machine with the following name:

- pcwebsuite.ProjectCost.net

You would typically use this type of certificate when installing the Project Cost Web Suite in a single machine configuration. This is the least- expensive type of certificate to purchase.

Multiple Domain

This type of security certificate is issued for a set of specific machines. You must know the machine names at the time that you are purchasing the security certificate. For example, you could get a security certificate issued that could be used for machines with the following names:

- pcwebsuite.ProjectCost.net
- MobileConnect.ProjectCost.net
- ProjectCost.net

You would typically use the multiple domain certificates when installing the Project Cost Web Suite in a scale out configuration. The certificate would contain entries for each of the machines that will be part of your installation. This security certificate is more expensive, because the same certificate can be used on multiple machines.

WildCard

This type of security certificate is not issued for specific machines. Instead, it is issued for a specific domain. The security certificate can be used for any machines that follow the naming convention for the domain. For example, if you purchased a wildcard certificate for the *.ProjectCost.net domain, any machine in that domain (such as pcwebsuite.ProjectCost.net) could use the wildcard certificate.

You would typically use the wildcard certificate when installing the Project Cost Web Suite in the scale out configuration. The wildcard certificate is especially useful when you expect to add additional machines to the configuration, but do not know their names at the time you are purchasing the certificate. The extra flexibility does come with a cost. Wildcard certificates are the most expensive externally signed security certificates.

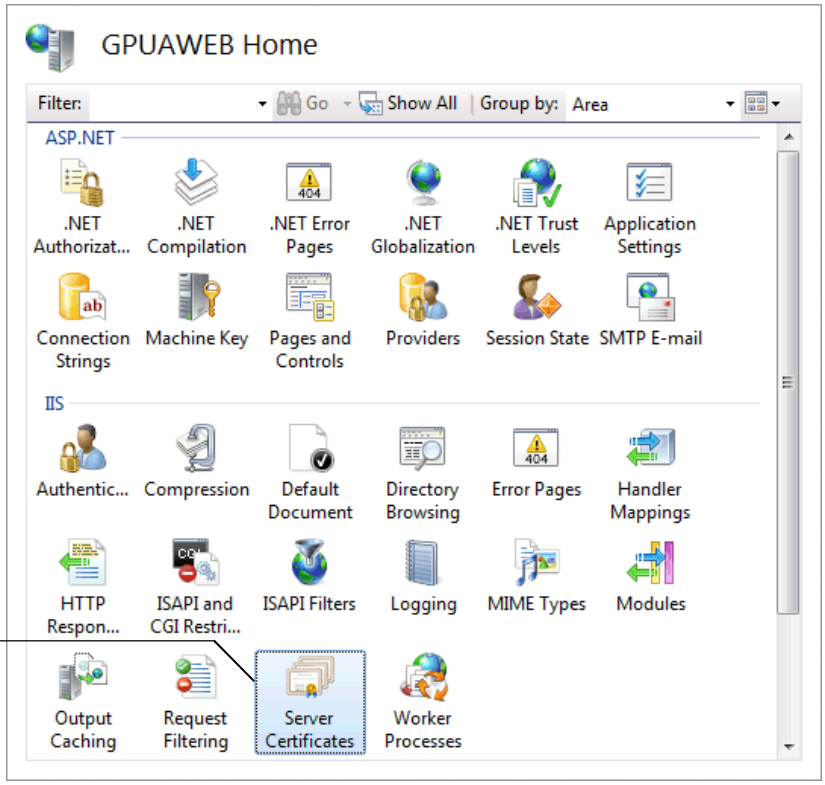
Using an Externally Signed Security Certificates

When an externally signed security certificate is used for a web site, the third-party certificate authority handles the certificate validation when users connect to the web client site. No additional action is needed by the Project Cost Web Suite users.

To Use an Externally Signed Security Certificate

1. Obtain the security certificate (.cer or .pfx) file from the third-party certificate supplier.
2. In Administrative Tools on the web server system, open Internet Information Services (IIS) Manager.
3. In the left pane, select the computer name.
4. In the IIS group, open Server Certificates.

Select the computer name and then open



5. Install the Certificate, based on the type of file that has been provided:
   - If your certificate has been provided as a .cer file, complete these actions. In the Actions pane, click Complete Certificate Request. Select the certificate (.cer) file that you obtained from the third-party certificate supplier. In the Friendly name field, enter the name that will be displayed for the certificate. Click OK.
   - If your certificate has been provided a .pfx file, complete these actions. In the Actions pane, click Import. Select the certificate (.pfx) file that you obtained from the third-party certificate supplier. Enter the password for the security certificate. Click OK.

Self-Signed Security Certificates

Self-signed security certificates are the least expensive way to implement SSL for the Project Cost Web Suite. You can generate these security certificates from within IIS Manager. They are typically used when you are setting up a Project Cost Web Suite installation for testing or development purposes.

Self-signed security certificates have some limitations. You must use the default subject alternative name (SAN) that is assigned when the security certificate is created. Self-signed security certificates have a limited lifespan, typically one year.

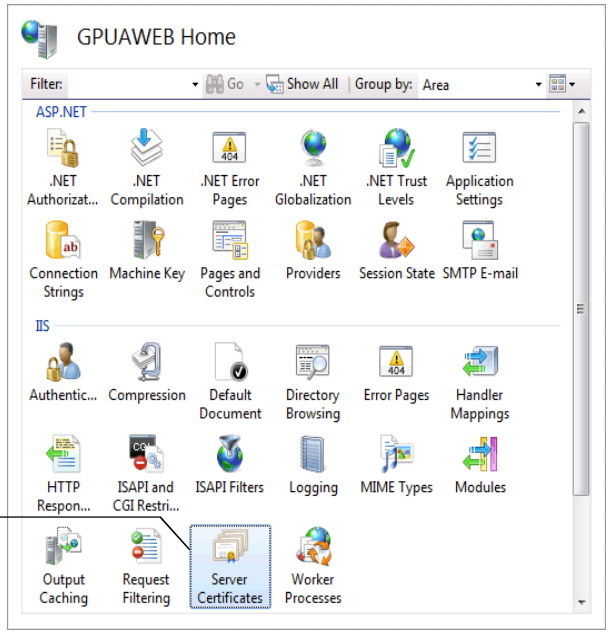
When you use a self-signed security certificate, there is no external authority to handle the certificate validation when users connect to the web client site. Because of this, a certificate error will be displayed when users access the Project Cost Web Suite site. To prevent the certificate error, users must import the security certificate onto their own machine.

Refer to for additional information on importing a Self-Signed Certificate.

To Use a Self-Signed Security Certificate

1. Open Internet Information Services (IIS) Manager.
2. In the left pane, select the computer name.
3. In the IIS group, open Server Certificates.

Select the computer name and then open Server Certificates.



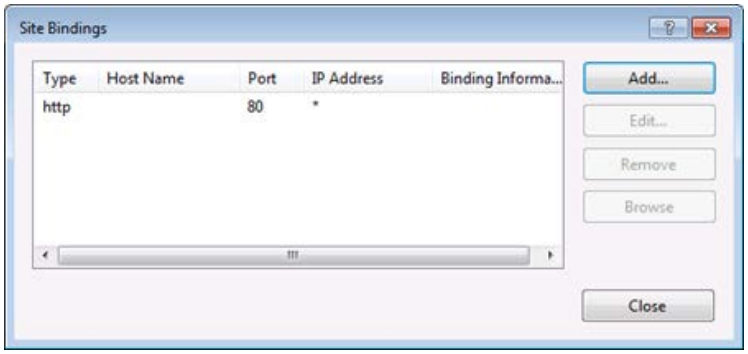
4. In the Actions pane, click Create Self-Signed Certificate.
5. Supply the friendly name for the security certificate.
6. Click OK. The security certificate will be created.

Configuring the Web Site to use SSL

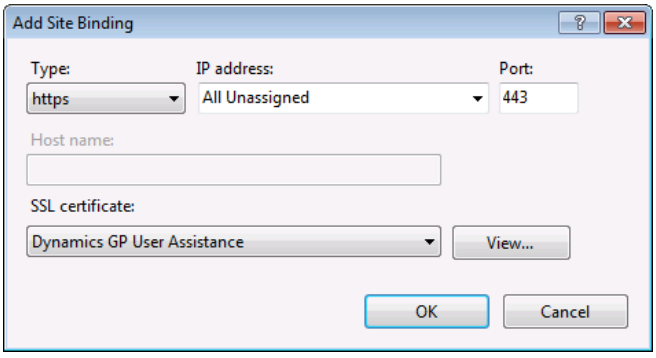
The web site used for the Project Cost Web Suite must be configured to use SSL. Before configuring the web site, be sure that you have imported an externally signed security certificate or have created a self-signed security certificate.

To Configure the Web Site for SSL

1. Open Internet Information Services (IIS) Manager.
2. In the left pane, expand the Sites group. Within the Sites group, select the site that you are configuring to use SSL. For example, select the Default Web Site.
3. In the Actions pane, click Bindings.
4. In the Site Binding window, click Add.



5. In the Add Site Bindings window, select https for the type, and then choose an SSL certificate that you installed.



6. Click OK.
7. Click Close.

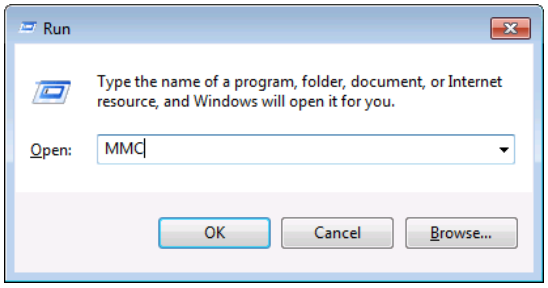
Installing a Security Certificate on a Server

If you are setting up the scale out configuration for the Project Cost Web Suite, the session host machines must have a security certificate that can be used when configuring the runtime session. If you are using an externally signed security certificate, you will need to install the security certificate onto each session host machine so that the certificate is available to be used.

To Install a Security Certificate

1. On the computer that will be used as a session host, open the Run prompt. (Choose Start > Run or press Window-R)

2. In the Open field, type MMC and then click OK.



3. In the Microsoft Management Console, open the File menu and choose Add/ Remove Snap-in.

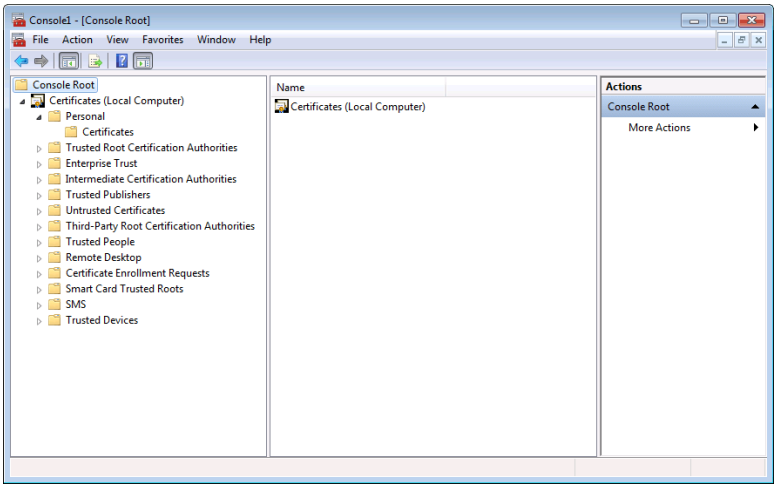
4. In the Add or Remove Snap-ins window, choose the Certificates snap-in from the Available snap-ins list, and then click Add.

5. In the Certificates snap-in dialog box, choose Computer account and then click Next.

6. In the Select Computer dialog box, choose Local computer and then click Finish.

7. In the Add or Remove Snap-ins window, click OK.

8. In the left pane, expand the Certificates (Local Computer) node, and then expand the Personal node.



9. Under Personal, right-click the Certificates node, point to All Tasks, and then click Import.

10. In the Certificate Import Wizard welcome screen, click Next.

11. In the File to Import screen, click Browse.

12. Browse to the location of the security certificate that you want to use. Typically, this will be a file with a .pfx extension, because the certificate contains a private key. Select the file and click Open. Click Next to continue.

13. Enter the password for the certificate. This is the private key password that was either provided with the certificate, or that you defined when you exported the certificate for use on another machine. Be sure that you mark the Include all extended properties box. Click Next to continue.

14. In the Certificate Store screen, verify that the certificate is being added to the Personal store. Click Next.

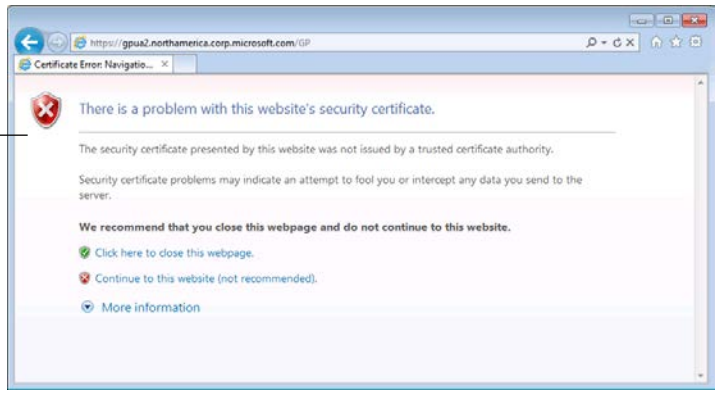
15. Click Finish to complete the import process.

16. Close the Microsoft Management Console window.

Importing a Self-signed Security Certificate

When you are using a self-signed security certificate, there is no certificate authority available to verify the certificate. If you use another computer to connect to the Microsoft Dynamics GP web client installation that is using a self-signed security certificate, you will see a certificate error displayed in the web browser.

If a self-signed security certificate is used for the Project Cost Web Suite installation, you will see a security certificate error when you try to connect from a different computer.



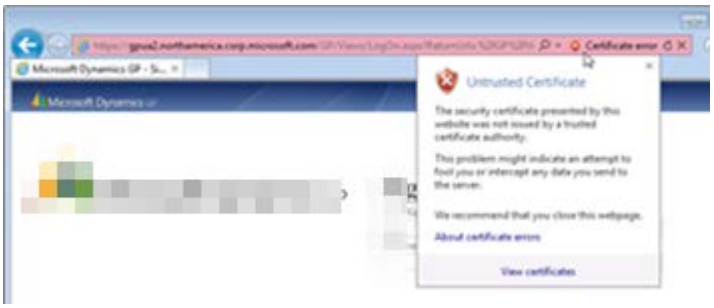
If a self-signed security certificate is used for the Project Cost Web Suite, the certificate error can prevent you from successfully logging into the site.

The solution is to import the security certificate into the machine that will be accessing the web client.

Step 1. Retrieve the Security Certificate

1. Open Internet Explorer on the computer that will be used to connect to the Project Cost Web Suite.
2. Connect to the Project Cost Web Suite site. The browser will display a message indicating that there is a problem with the web site's security certificate. Click **Continue to this website**.
3. The URL area of the browser you will appear in red, indicating a security certificate error.

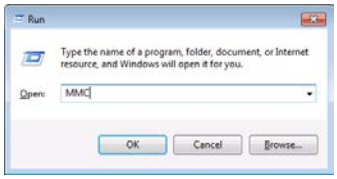
   Click **Certificate error** to display the details of the error.



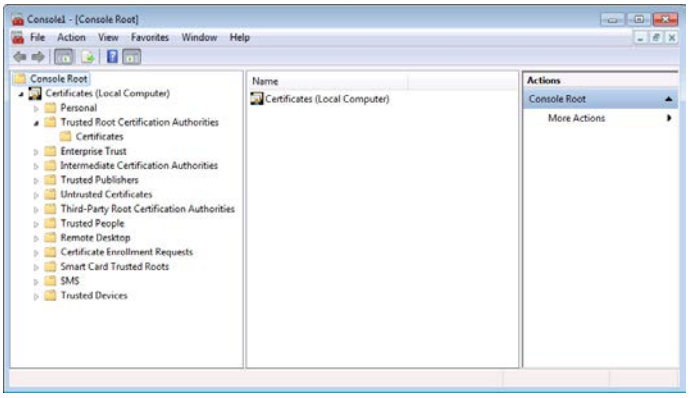
4. In the Drop-Down, Click **View Certificates.**
5. In the Certificate window, Click **Details** tab.
6. Click **Copy to File** to open the Certificate Export Wizard. Click **Next**
7. Select the **DER encoded binary X.509** format, and Click **Next**.
8. Click Browse to open a file dialog box that allows you to name the certificate file and select a location to store the file. Click Save.
9. In the Certificate Export Wizard, Click **Next**. Then click **Finish**. A message will be displayed indicating that the security certificate was exported.
10. Click **OK** to close the Certificate window.

Step 2. Install the Security Certificate

1. On the computer that will be used to connect to the web client, open the Run prompt. (Choose Start > Run or press Window-R)
2. In the Open field, type **MMC** and then click **OK**.



3. In the Microsoft Management Console, open the File menu and choose **Add/ Remove Snap-in**.
4. In the Add or Remove Snap-ins window, choose the **Certificates** snap-in from the Available snap-ins list, and then click **Add**.
5. In the Certificates snap-in dialog box, choose **Computer account** and then click **Next**.
6. In the Select Computer dialog box, choose **Local computer** and then click **Finish**.
7. In the Add or Remove Snap-ins window, click OK.
8. In the left pane, expand the Certificates (Local Computer) node, and then expand the Trusted Root Certification Authorities node.



9. Under **Trusted Root Certification Authorities**, right-click the **Certificates** node, point to **All Tasks**, and then click **Import**.
10. In the Certificate Import Wizard welcome screen, click **Next**.
11. In the File to Import screen, click **Browse**.
12. Browse to the location of the security certificate that you retrieved from the previous procedure. Select the .cer file and click **Open**. Click **Next** to continue.
13. In the Certificate Store screen, verify that the certificate is being added to the Trusted Root Certification Authorities store. Click **Next**.
14. Click **Finish** to complete the import process.
15. Close the Microsoft Management Console window.