

**NOTE**

The ISAPI Plug-In should only be installed on a Windows Server operating system.

Installing the ISAPI Plug-In

To install the ISAPI Plug-In

- 1 Place the Application CD-ROM in the CD-ROM drive of the Windows server. Open the D:\ISAPI Plug-in directory, where D:\ is the CD-ROM drive. The ISAPI Plug-in folder contains the following .dll files:
 - libeay32.dll
 - masisapi.dll
 - openssl.dll
 - ssleay32.dll
- 2 Copy the four .dll files to the Scripts folder under the root directory of your Web site. Create a Scripts folder if it doesn't already exist. Make sure that Web users have read-only access to the Scripts folder.

Registering the Server Side Include (SSI) on the IIS Server

To register the Server Side Include on IIS

- 1 Select Start > Settings > Control Panel. Double-click Administrative Tools. Double-click Internet Information Services (IIS) Manager.
- 2 In the Internet Information Services (IIS) Manager window, right-click the Web site used for e-Business Manager and click Properties.
- 3 In the Properties window, click the Home Directory tab and click Configuration.
- 4 In the Application Configuration window, click either the Mappings tab or the App Mappings tab, as applicable. Click Add.
- 5 In the Add/Edit Application Extension Mapping window, at the Executable field, click Browse and browse to the location of the MASISAPI.DLL file.
- 6 At the Extension field, type **PVX**. Accept all other default settings and click OK.
- 7 In the Application Configuration window, verify that PVX appears in the Application Extensions panel or the Application Mappings panel, as applicable. Click OK.
- 8 Click OK to close the Properties window.

**NOTE**

These instructions apply to Windows Server 2003. The procedure may be different for Windows 2000 and Windows NT 4.0 Servers.

**WARNING**

Do not select All Unknown ISAPI Extensions. This will cause a severe security risk on the server.

Enabling Web Service Extensions on the IIS Server

To enable Web service extensions on IIS

- 1 Select Start > Settings > Control Panel. Double-click Administrative Tools. Double-click Internet Information Services (IIS) Manager.
- 2 In the Internet Information Services (IIS) Manager window, select the Web Service Extensions folder.
- 3 Click Add a new Web service extension.
- 4 In the New Web Service Extension window, at the Extension Name field, type **PVX**. Click Add.

- 5 In the Add file window, click Browse and browse to the location of the MASISAPI.DLL file. Click Open. Click OK to close the Add file window.
- 6 Select the Set extension status to Allowed check box and click OK.
- 7 Verify that PVX appears with a status of Allowed in the Web Service Extensions panel.

**NOTE**

The ISAPI Plug-In does not need to be re-installed for each Web site.

After enabling the Web service extensions in the IIS server, you must configure the ISAPI Plug-In in the e-Business Manager Options window. Multiple Web sites on the same IIS can be configured the same way. Run Publish Files to Web for each company before accessing e-Business Manager Web pages. For more information, see e-Business Manager Options and Publish Files to Web in the Help system.

**NOTE**

If you are unfamiliar with generating a certificate for secure transactions, consult a network consultant or authorized Reseller.

Generating an SSL Key

To use the SSL capabilities of the Web Engine, create a .pem file that contains both the certificate and your private key in X509 format.

The instructions for generating an SSL key are available on the ProvideX Web site. Go to www.pvx.com and search for "certificates", "pem", or "CSR".

**NOTE**

This procedure is not necessary if each Web server is hosting just one SSL Web site or ...

Modifying the ISAPI for Hosting Multiple SSL Sites

Because Host Header Names are not supported with Secure Socket Layer (SSL), if you are hosting multiple SSL Web sites from one Web server, the SSL proxy server will have difficulties locating the correct SSL Web site that a client browser requests.

**NOTE**

You can place one MASISAPI.ini with all company information in the C:\Windows directory for all the SSL Web sites to share.

To resolve this problem, if you are hosting multiple SSL Web sites from one Web server, you must distinguish each SSL Web site with a different TCP port and modify the MASISAPI.ini file. If there are multiple MASISAPI.ini files on the Web server, one for each SSL Web site, then modify each MASISAPI.ini file.

To modify the MASISAPI.ini file

- 1 Open the MASISAPI.ini file in Notepad. The MASISAPI.ini file is located in the root directory of each Web site.
- 2 Add an entry for the server and port that the proxy is using to access each SSL Web site. Use the following example to determine the entry to add:

Example

Your Web server hosts two SSL Web sites. The Web server's IP address is 123.4.56.789. The first SSL Web site uses port 441 and its URL is <https://website1.example.com>. The second SSL Web site uses port 442 and its URL is <https://website2.example.com>. Based on this example, type the following entry:

[Http Proxy Remappings]

123.4.56.789:441=https://website1.example.com

123.4.56.789:442=https://website2.example.com

- 3 Select File > Save.