ECA IIS Instructions

January 2005

THIS PAGE INTENTIONALLY BLANK

Table of Contents

1. Install Certificate in IIS 5.0

Before proceeding with these instructions, you must visit the link below which provides a fix for a known error you will most likely encounter when installing your server certificate.

http://eca.orc.com/troubleshootingFAQ.html

To install the certificate retrieved (as per the notification e-mail) to the Microsoft IIS 5 Web server perform the following instructions. Do not attempt to perform these steps if you have not yet received your notification email.

Note: In this example, SSL is applied to the Default Web Site, which is the default Web site installed by Windows 2000/IIS5.

1. Click the [**Start**] button to start the Internet Information Service Manager, and then select **Programs→Administrative Tools→Internet Services Manager**. The **Internet Information Services** screen displays.

2. Expand the Default Web Site in the Console tree (the left panel).

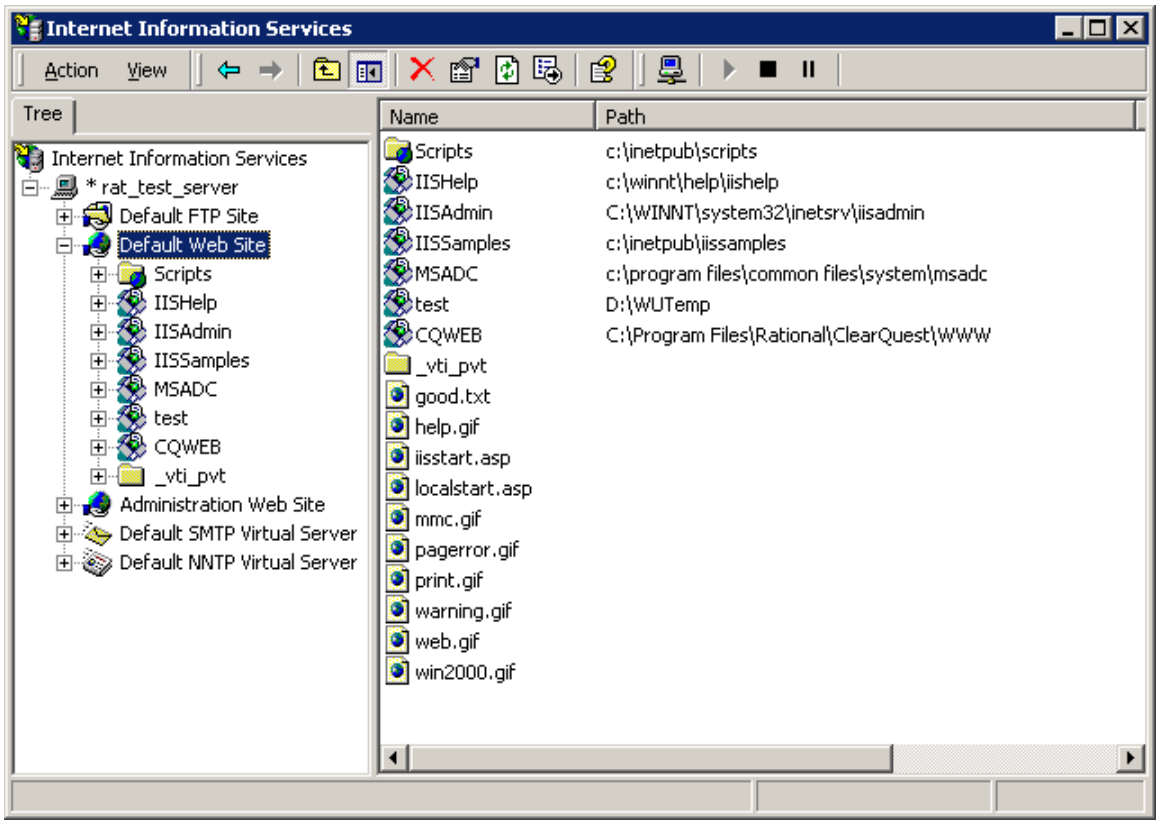

Figure 1:Internet Information Services screen

3. Right-click the **Default Web Site→ Properties** to open the **Properties** dialog box. The **Default Web Site Properties** dialog box appears. Set the **SSL Port** field to the number **443**.

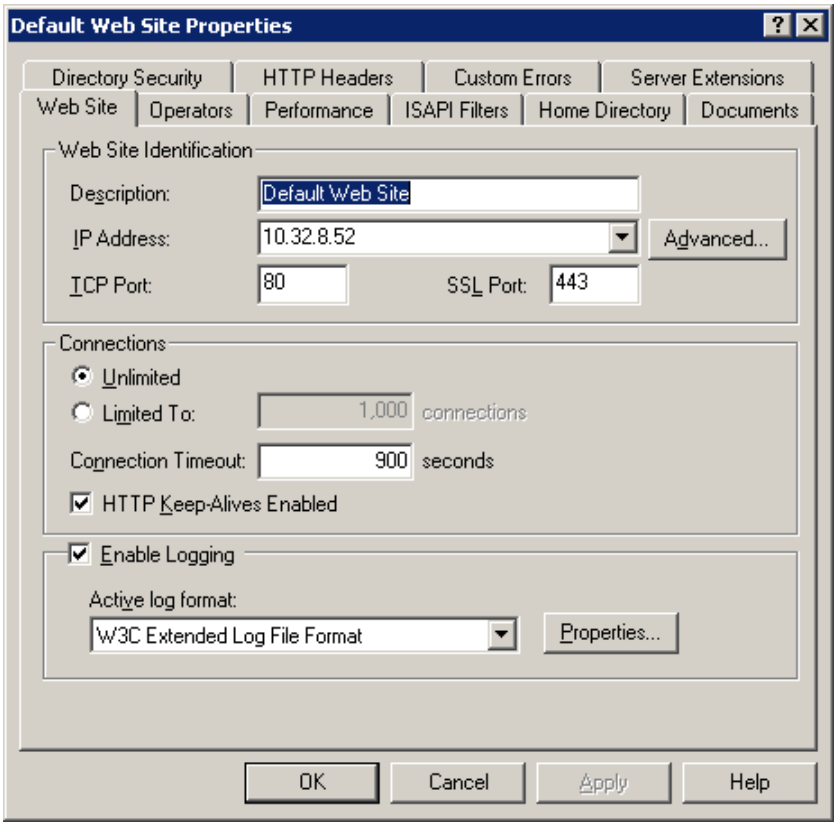

Figure 2 The Website Properties Screen

Note: The SSL port is shown as 443, which is the default port for SSL function. This block may be grayed out if no certificate has ever been installed on this Web site. If so, you must return to this screen after the certificate is installed and set the SSL port to 443. Failure to do so will deny you access to your Web site when you turn SSL on.

---

4. Click the *Directory Security* tab within the **Default Web Site Properties** screen. Click **Server Certificate** in the **Secure Communications** section. This will display the **Welcome to the Web Server Certificate Wizard**.

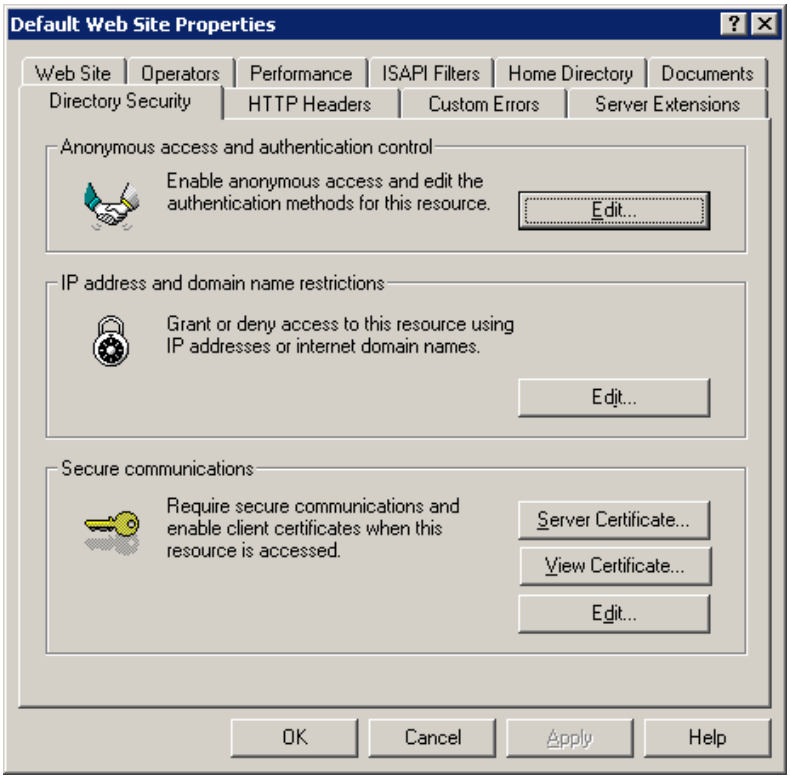

Figure 3 The Directory Security Tab

5. Click [**Next**] to display the **Pending Certificate Request** screen.

Figure 4 The Welcome to the Web Server Certificate Wizard Screen

6. Select the **Process the pending request and install the certificate** radio button from the **Pending Certificate Request** screen. Click [**Next**] to display the **Process a Pending Request** screen.

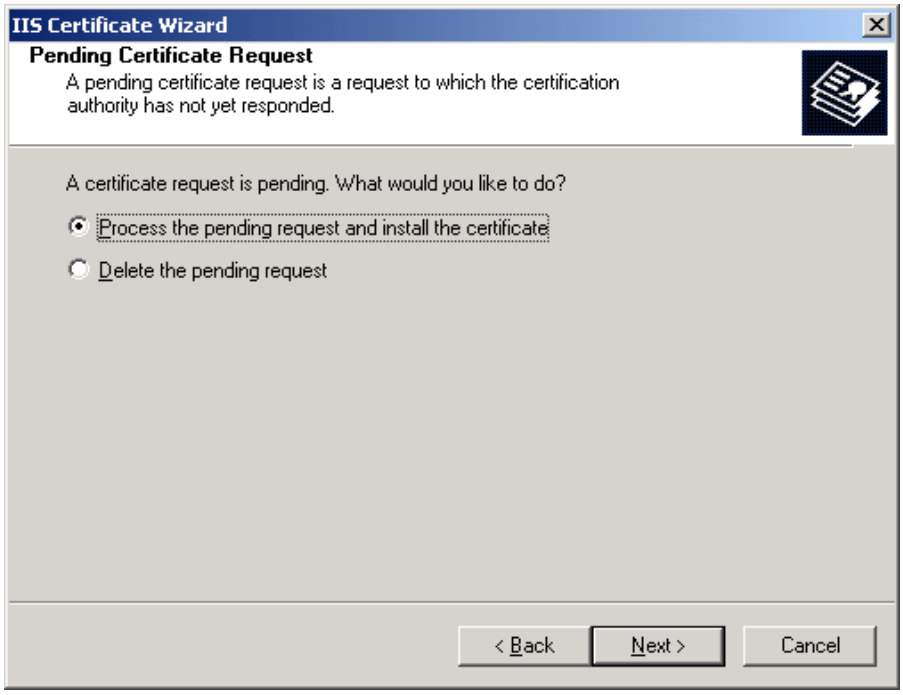

Figure 5 The Pending Certificate Request Screen

7. Enter the file name and path of where the certificate was saved. Or click [**Browse**] to locate the certificate. Click [**Next**] to display the **Certificate Summary** screen.

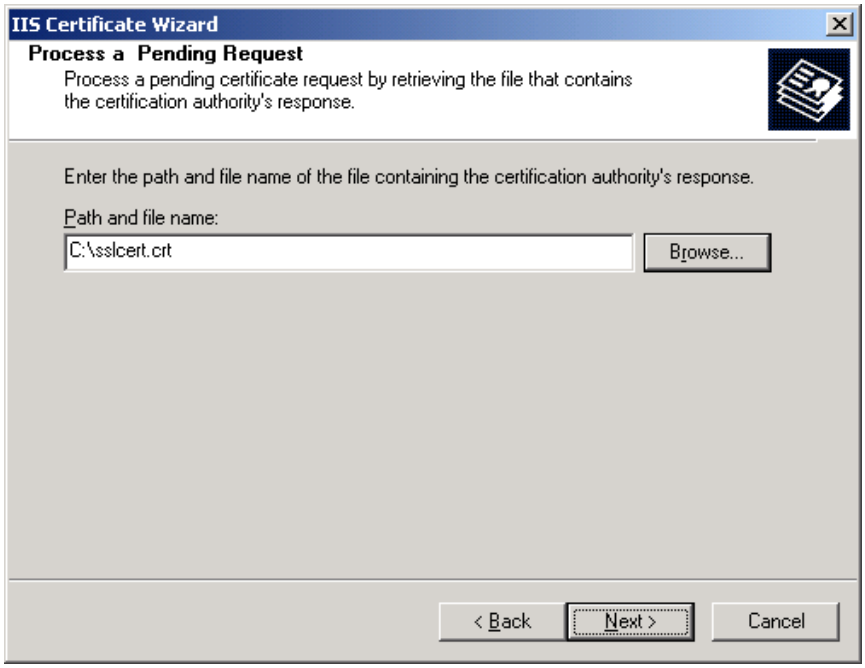

Figure 6 The Process a Pending Request Screen

8. Read the information contained in the **Certificate Summary** screen and then click [**Next**]. The **Completing the Web Server Certificate Wizard** screen will be displayed.

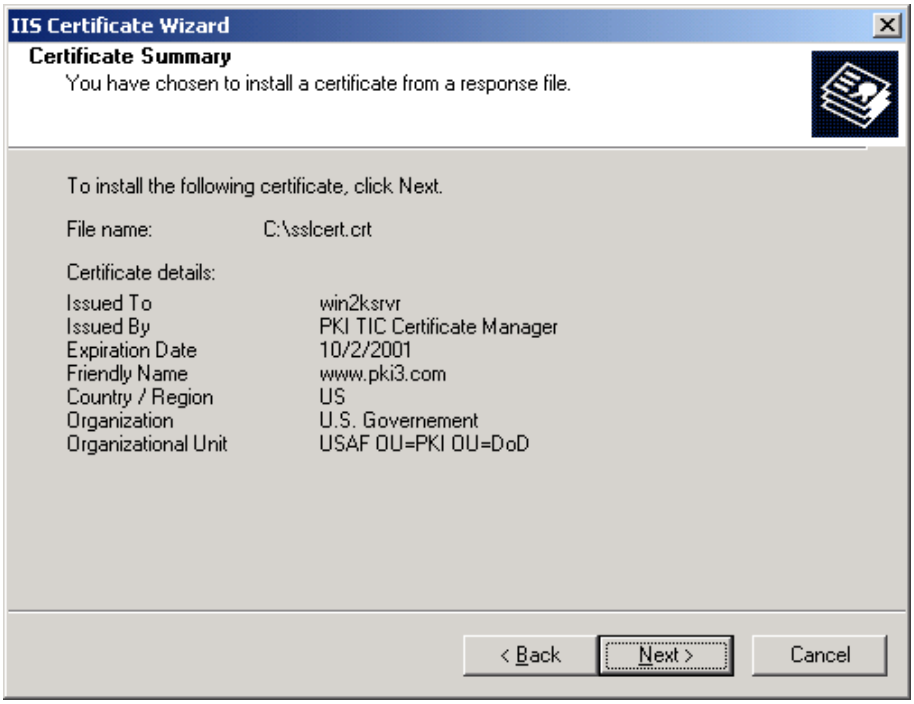

Figure 7 The Certificate Summary Screen

Note: Click [**Back**] if changes need to be made, to go back as many screens as needed and make the necessary changes. Click [**Next**] as many times as needed to return to the **Completing the Web Server Certificate Wizard** screen.

9. Click [**Finish**] to return to the *Directory Security* tab. The [**View Certificate**] and the [**Edit]** buttons are now available in the **Secure Communications** section.

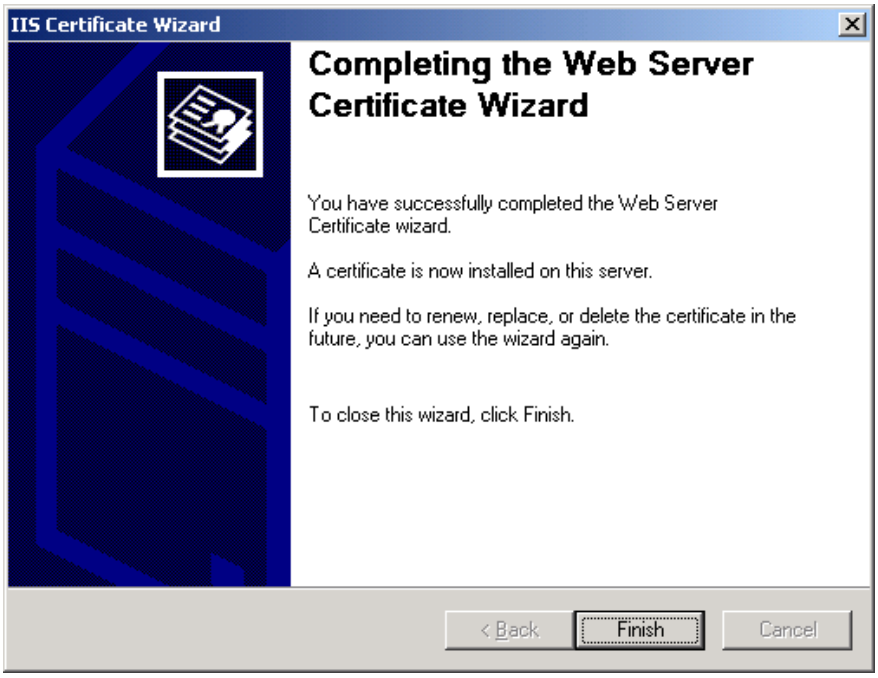

Figure 8 The Completing the Web Server Certificate Wizard Screen

10. From the *Directory Security* tab click **Edit**, then click the **Require Secure Channel (SSL)** box as well as the **Require 128-bit encryption** box to enable SSL Communications. Click [**OK**] to return to the **Default Web Site Properties** screen.

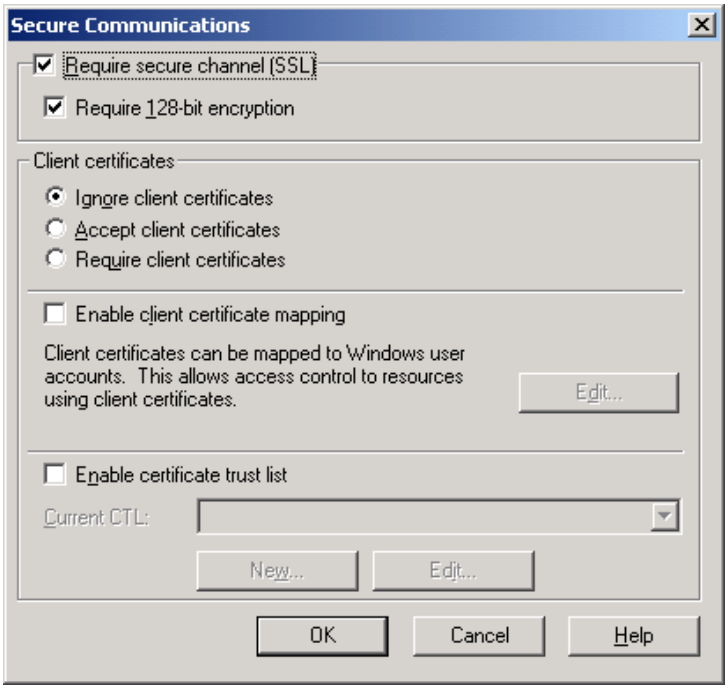

Figure 9 The Secure Communications Screen

Note: Depending on the requirement, the option to accept or require client certificates may be selected. Only select the require client certificates option to restrict access to the web server to clients who have their own identity certificates.

11. Click the *Web Site* tab on the **Default Web Site Properties** dialog box. Ensure the number **443** is displayed in the **SSL Port** field. Enter **443** if not present. This is the default port number for SSL communications.

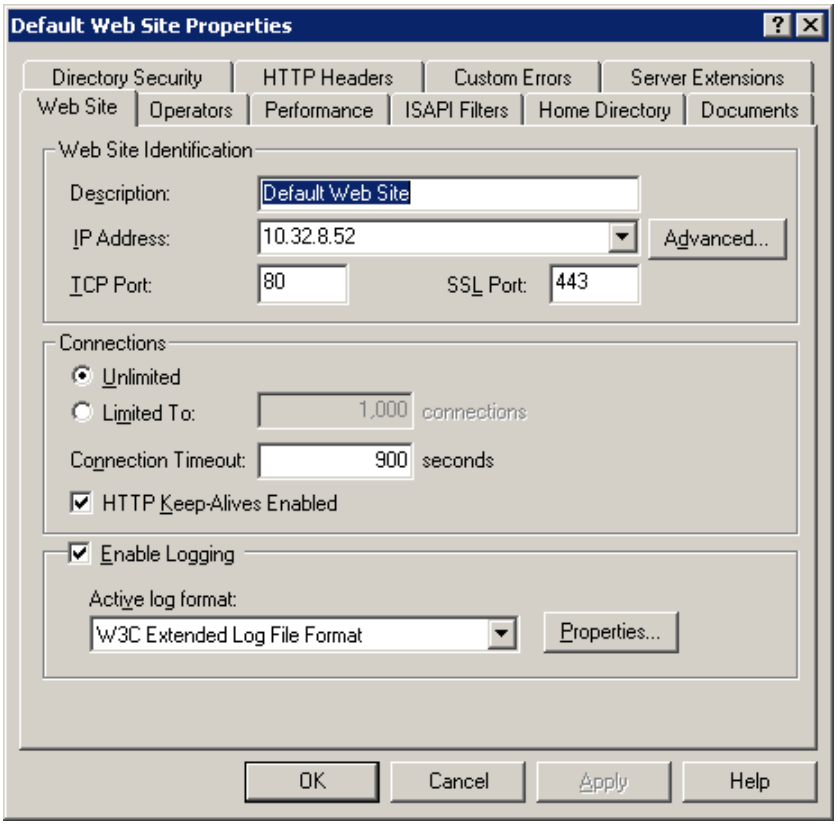

Figure 10 Default Web Site Properties Screen

12. Click [**OK**]. Close the Internet Information Services Manager and save all settings. At this point, the Web server is SSL enabled.

2. Obtain and Install the ECA Root Certificate Chain

Download and install the ECA Root Certificate Chain. This chain includes the ECA root certificate as well as the ORC ECA CA signing certificate. This action is necessary in order for the ECA server certificate to be trusted.

1. Download the Base 64 encoded certificates from the following URL: http://eca.orc.com.
    a. Place your cursor over the **ECA Repository** heading and select **ECA Root Certificate.**
    b. Select **Save** when the **File Download** dialog box appears. Save the file with the default name (eca_root.cer) to the desired location.
    c. Perform the above two steps a second time for the CA signing certificate (filename is orc_eca.cer).
2. Open **Windows Explorer** and locate the two ECA certificates downloaded from Step 1. Double-click the "eca_root.cer" file to start the Microsoft Certificate Wizard process. The **Certificate** screen appears. Click [**Install Certificate**] to begin the **Certificate Import Wizard.**

Note: This process must be performed as the Administrator.

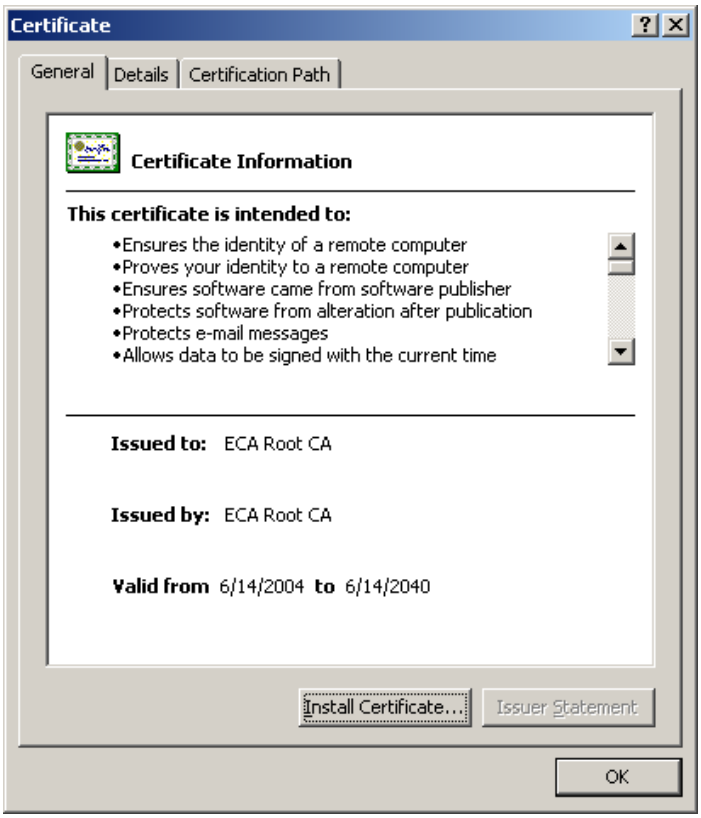

Figure 11 Certificate Information Screen

3. Read all the information in the **Certificate Import Wizard** screen, and then click [**Next**] to display the **Certificate Store** screen.

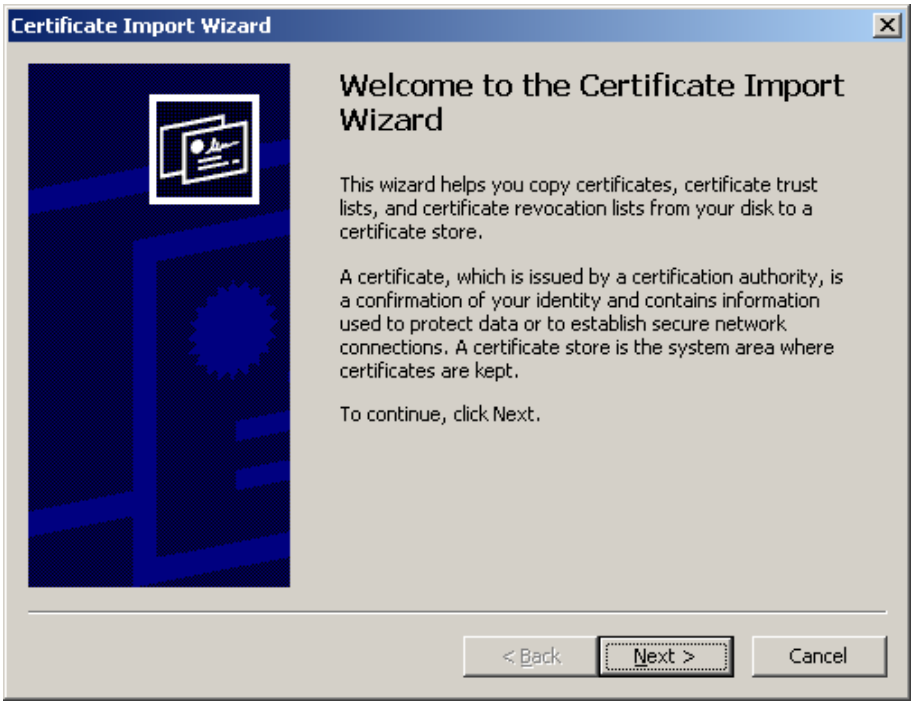

Figure 12 Certificate Import Wizard Welcome Screen

4. Select the **Place All Certificates in the Following Store** radio button then click [**Browse**] to choose a certificate store.

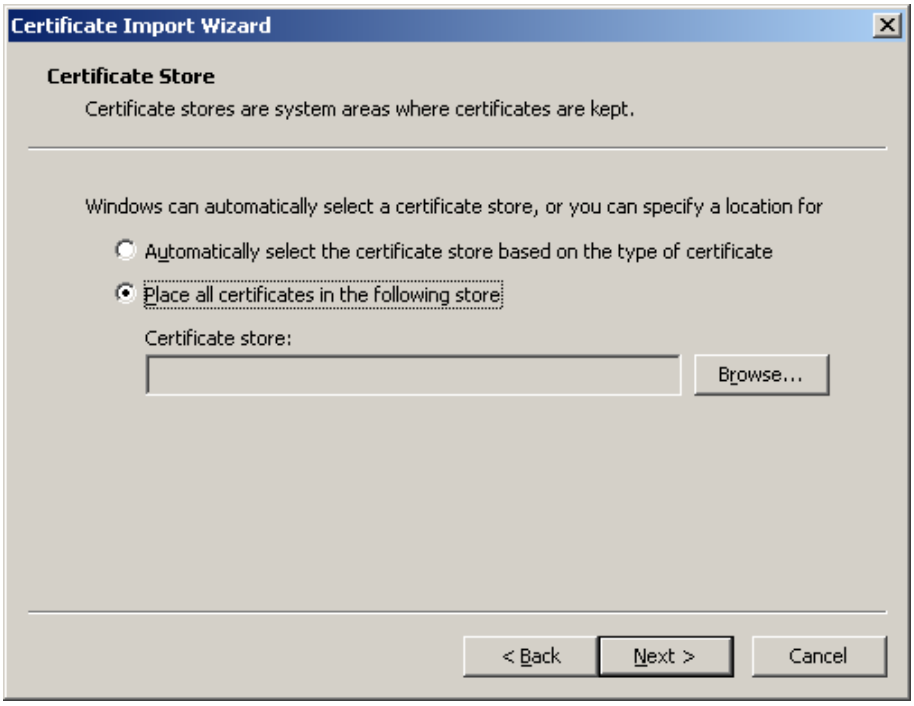

Figure 13 Certificate Store Screen

5. Check the **Show Physical Stores** box. Double-click the **Trusted Root Certification Authorities** and then select **Local Computer**. Click [**OK]**. Click [**Next]** to display the **Completing the Certificate Wizard** screen.

Figure 14 Select Certificate Store Screen

Note: When installing the ORC ECA certificate, select Intermediate Certification Authorities- Local Computer for the certificate store.

6. Click [**Finish**]. At this point, the ECA root certificate has been imported into the browser. A notice of successful completion appears.

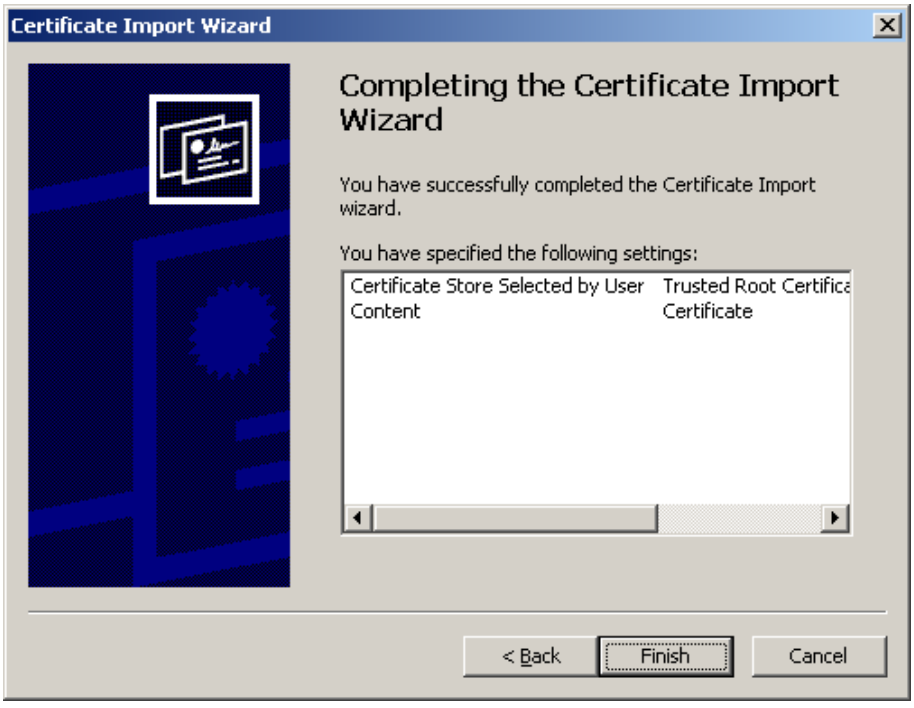

Figure 15 Completing the Certificate Import Wizard

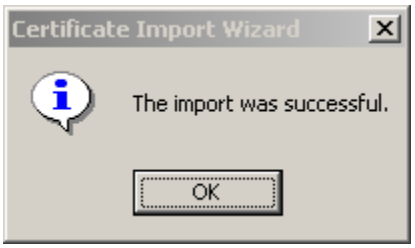

Figure 16 Successful Import Message

7. Repeat steps 2 through 6 using the "orc_eca.cer" file to install the ORC certificate signing certificate. When finished installing, close the certificate.

Note: When installing the "orc_eca.cer" place it in the **Intermediate Certification Authorities→ Local Computer** certificate storage area.

---

8. After installing the ECA chain into the IE browser, the default web server should be stopped and restarted from the **Internet Information Services** window. Right-click on the **Default Web Site** and select **Stop.** Once the **Default Web Site** has been stopped (as shown below), right-click it again and select **Start** to restart the web server.

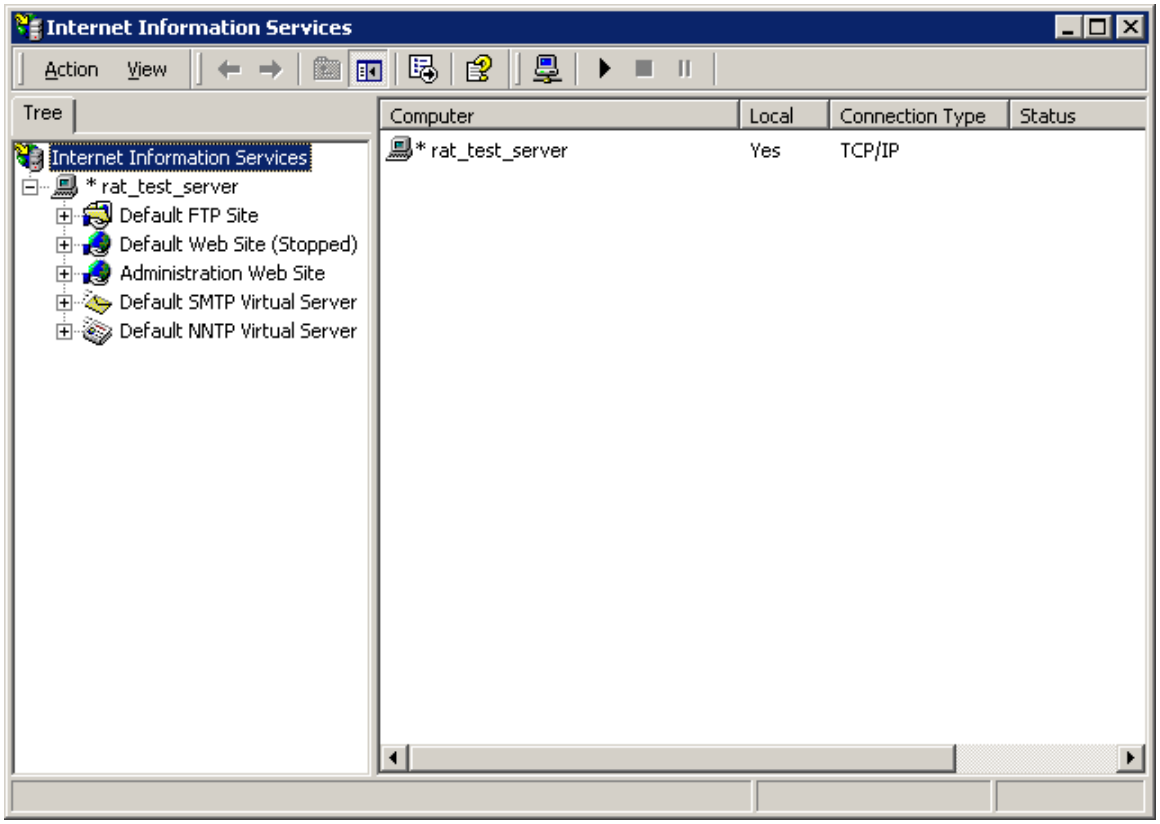

Figure 17 Internet Information Services (stopped)

3. Enable Certificate Mapping for IIS 5.0

After the ECA-issued server certificate and the ECA certificate chain have been installed on the server, the server can be made to ignore, accept, or require client certificates within IIS.

Ignore client certificates- Users can access website with or without a user certificate. Users are not prompted to select a certificate when logging into the website.

Accept client certificates- Users are not required to have a valid client certificate to access the website. If a user has a valid client certificate, he or she will be prompted to select it upon login.

Require client certificates- Users are required to present a valid client certificate when logging into the website. Users are denied access without presenting a valid client certificate.

In addition to ignoring, accepting, or requiring client certificates, the IIS server can be made to enable certificate mapping.

1. Click the [**Start**] button and then select **Control Panel→Administrative Tools→Internet Services Manager** to start the Internet Information Service Manager. The **Internet Information Services** screen displays.

2. Expand <*your Web server name*> in the Console tree (the left panel). For this example, the website being used is 'CQWEB'.

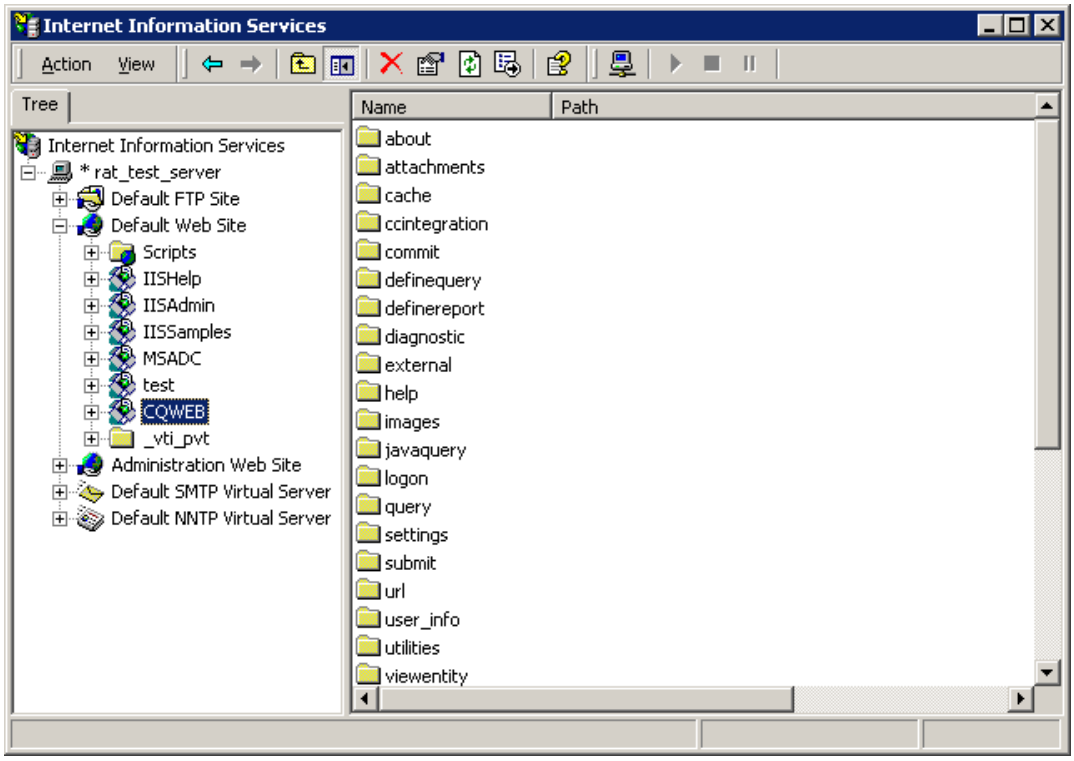

Figure 18 Internet Information Services Screen

3. Right-click the **CQWEB Web Site→ Properties** to open the **Properties** dialog box. The **CQWEB Properties** dialog box appears.

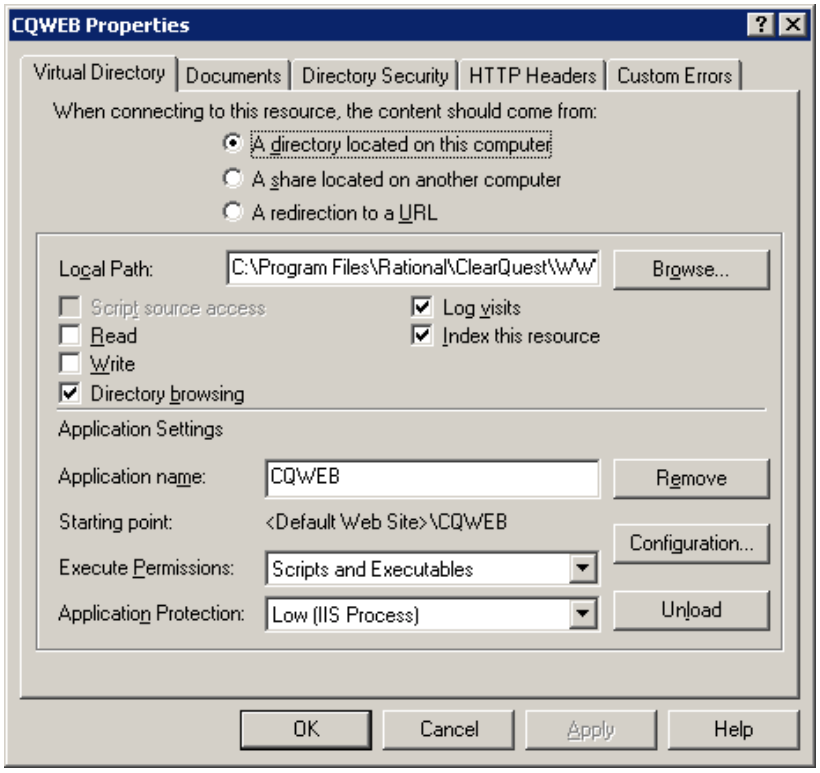

Figure 19 CQWEB Properties-Virtual Directory Tab

4. Click the *Directory Security* tab within the **CQWEB Properties** screen. Click the [**Edit**] button in the **Secure Communications** section. The **Secure Communications** screen appears.

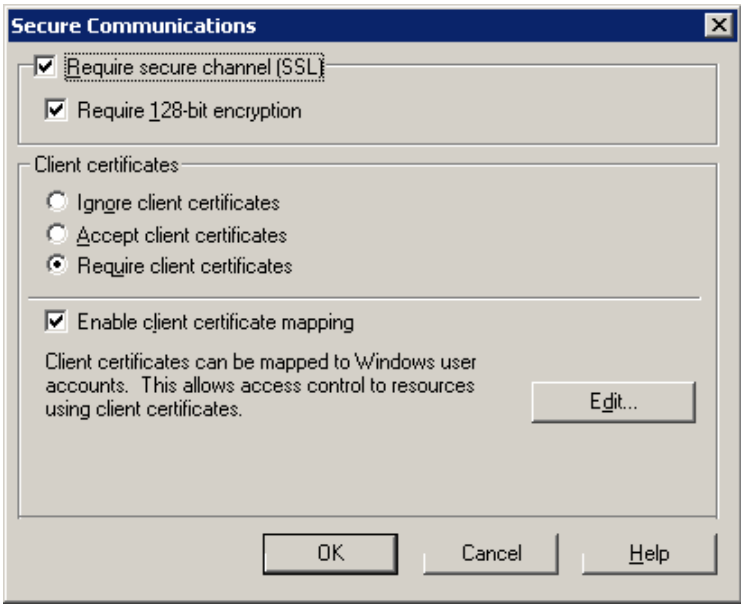

Figure 20 Secure Communications Screen

5. Select the **Require secure channel (SSL)** and **Require 128-bit encryption** check boxes to enable SSL communications on a particular web site.

6. Select the **Require client certificates** option in the **Client Certificates** section and the **Enable client certificate mapping** option at the bottom of the **Secure Communications** screen in order to fully PK-enable the web server using the most restrictive access.

7. Click [**Edit**] to map user certificates to user accounts on the web server. The **Account Mappings** screen appears.

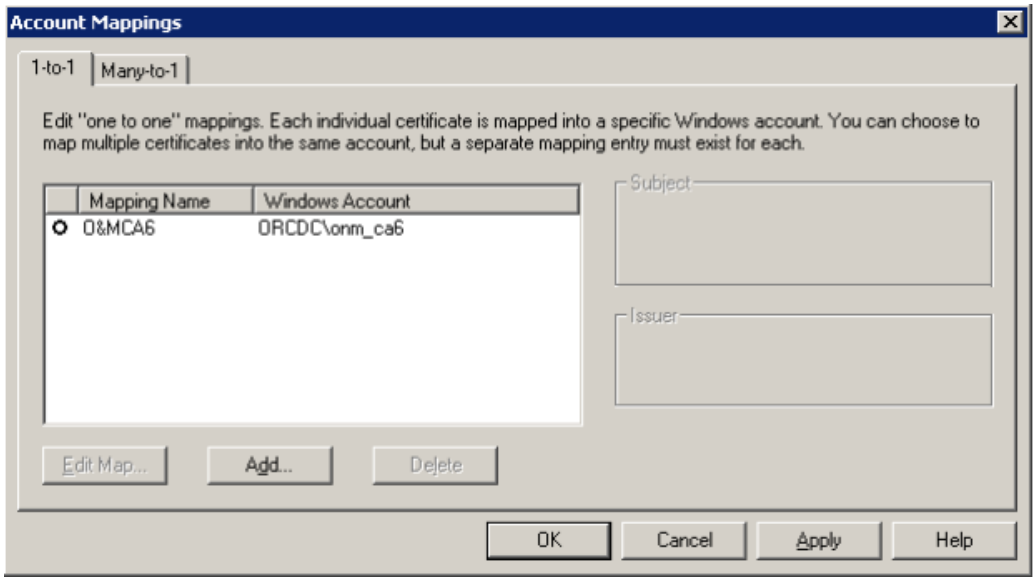

Figure 21 Account Mappings Screen

8. Click [**Add**] to create a new account mapping. Select a user certificate from the dialog box and click [**Open**]. The **Map to Account** screen will appear.

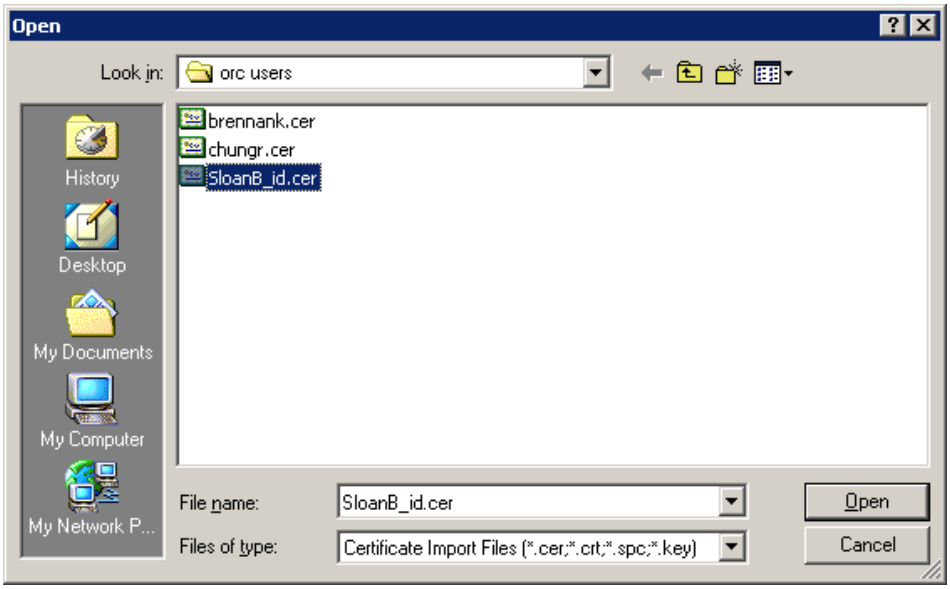

Figure 22 Select User Certificate Dialog Box

9. Ensure that the **Enable this mapping** box is selected. Enter a name for the new mapping.

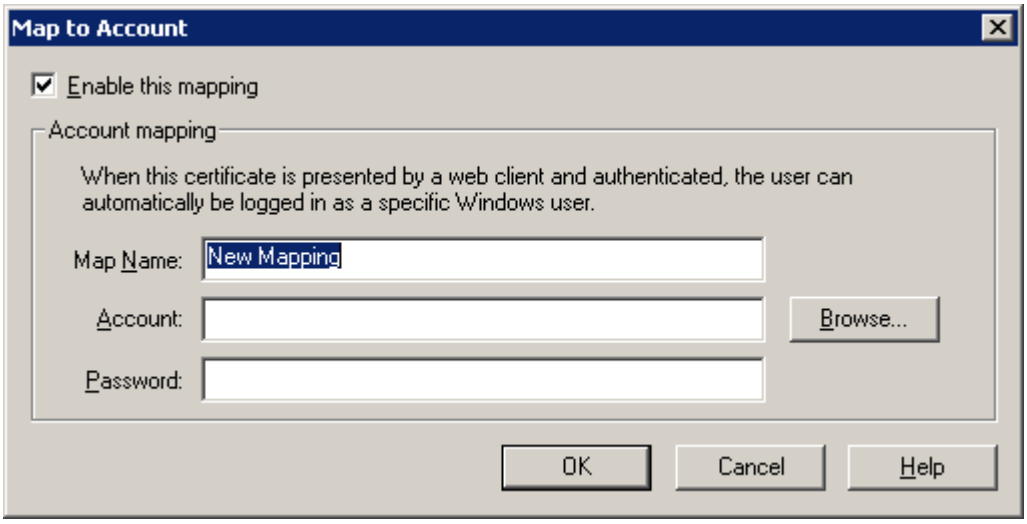

Figure 23 Map to Account Screen

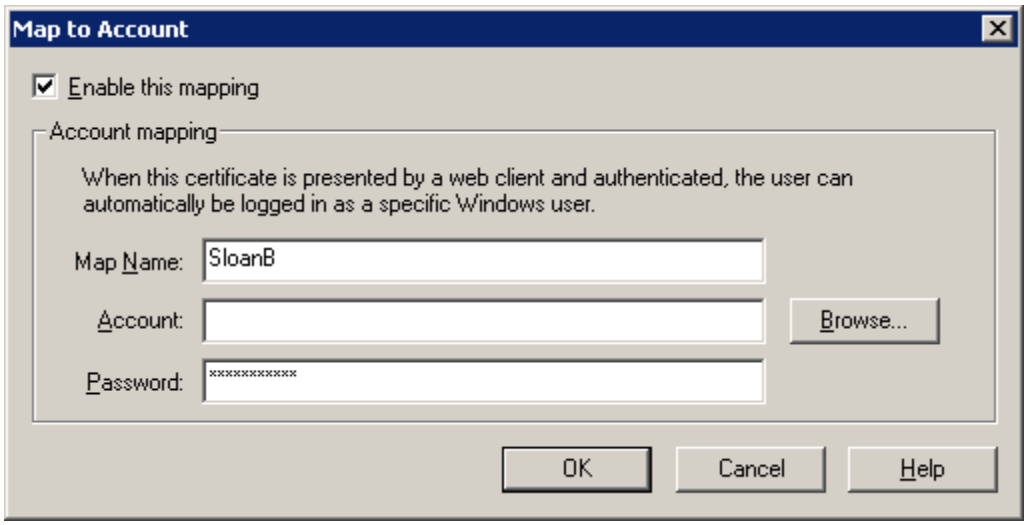

Figure 24 Map to Account Screen

10. Click [**Browse**] to find the user logon account associated with the certificate chosen for the mapping. The **Choose Mapping Account** screen appears. Select the user account which matches the certificate being mapped, and click **Add**, then click **OK** to return to the **Map to Account** screen.

11. Enter a password for this mapping. This password must be the same password as the password used when the user's logon account was created (for example, the **Active Directory** user account password). Click **OK**, and confirm the password when prompted.

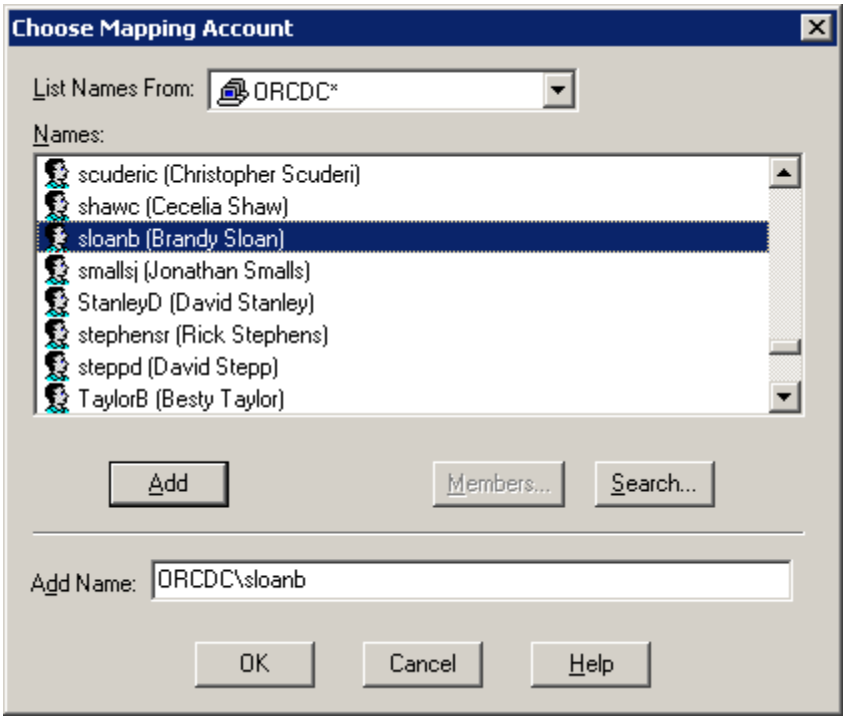

Figure 25 Choose Mapping Account Screen

12. From the **Account Mappings** screen, click **[OK]**. Notice, the new account mapping now appears on this screen. Click **[OK]** to return to the **Secure Communications** screen. Click **[OK]** to return to the **CQWEB Properties** screen. Click **[OK]** to return to the **Internet Information Services** screen. Close the **Internet Information Services** screen. The web server is now PK-enabled. Only users with a valid certificate AND a valid account mapping to that same valid certificate will be allowed to access the web site.

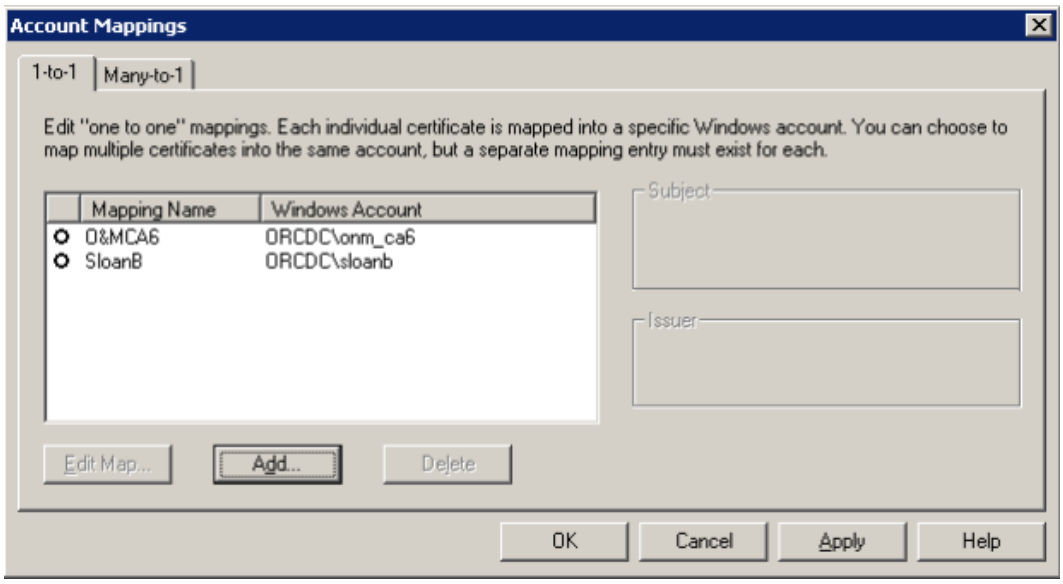

Figure 26 Account Mappings Screen

Note: Before proceeding with these instructions, you must visit the link below which provides a fix for a known error you will most likely encounter when installing your server certificate.

http://eca.orc.com/troubleshootingFAQ.html