Microsoft Exchange 2010

1. Go to **Start** > **Programs** > **Microsoft Exchange 2010** > **Exchange Management Console**.
2. Click the **Manage Databases** link and then click **Server Configuration**.
3. Under the **Actions** menu, click **New Exchange Certificate**.
4. Enter a name to easily identify this certificate in the future.
5. If you are generating a CSR for wildcard certificate, select the check box under **Domain Scope**.
6. On the Exchange Configuration menu, select the services that you will run. When prompted, enter the names through which you connect to those services.
7. Review the names that the Exchange 2010 suggests to include in your certificate request. Add if necessary.
8. Click **Browse** and save the CSR as a .req file, and then click **Next** > **New** > **Finish**.
9. Open the CSR file in a text editor and copy the text, including the `“Begin”` and `“End”` tags.
10. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
11. Paste the text from the CSR file into the field provided.

Microsoft Exchange 2007

1. Open the Exchange Management Shell command line and type the following:

```
New-ExchangeCertificate -GenerateRequest -KeySize 2048 -Path
c:certificate.txt -SubjectName “c=country, l=locality,
s=state, o=company, cn=yourdomain” -DomainName
otherdomain.com, nextdomain.com -PrivateKeyExportable:$true
```

where:

`“country”` is your two-letter ISO 3166 country code. For example, the code for the Japan is `“JP”`. For the other countries, refer to the ISO list of country codes.

`“locality”` is the full name of the locality or city where your company is headquartered.

`“state”` is the full name of the state or province where your company is headquartered.

`“company”` is the full legal name of your company.

`“yourdomain”` is the fully qualified domain name (FQDN) for which you are requesting the SSL certificate. For wildcard certificate, the common name must begin with an asterisk (*). For example, *.yourcompany.com.

`“-SubjectName”` after `“cn=”` is the first domain name.

" `–DomainName`" is the additional domain names separated by commas. You can add as many additional domain names as necessary.

2. Open the CSR file, which is located in the root of your c: drive, using a text editor and copy the text, including the "`Begin`" and "`End`" tags.
3. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
4. Paste the text from the CSR file into the field provided.

Microsoft Exchange 2003

1. Go to **Start** > **Programs** > **Microsoft Exchange** > **System Manager**.
2. Make sure that the **Display administrative groups** option is selected.
   a) Right-click the name of your organization, and then click **Properties**.
   b) Tick the **Display administrative groups** check box and click **OK**.
   c) Restart the Exchange System Manager.
3. Navigate to **Administrative Groups** > Name of your administrative group > **Servers** > Exchange Server that you want to configure > Protocols container.
4. Expand each protocol that you want to configure.
5. Right-click the default protocol name virtual server object, and then click **Properties**.
6. Under the **Access** tab, click **Certificate** and then click **Next**.
7. Click **Create a new certificate**, and then click **Next**.
8. Click **Prepare the request now, but send it later**, and then click **Next**.
9. Enter an appropriate name for the certificate in the **Name** field or leave the default setting of the default protocol name virtual server.
10. Select your preferred bit length from the **Bit Length** list, and then click **Next**.
11. On the **Organization** field, type the organization information for the CA where you want to request a certificate, and then click **Next**.

    Note: This information is available on the CA website or is sent to you upon registration.

12. Type the common name for your site on the **Common Name** field, and then click **Next**.

    Note: To allow access from the Internet, the name must be a fully qualified domain name that can be resolved externally. This FQDN must map to the IP address that is linked to the virtual server.

13. Select your country or region name from the **Country/Region** list.

14. Provide the necessary details on the **State/Province** and **City/Locality** fields and click **Next**.
15. On the **File name** box, type a name and path where you want to create the certificate, or keep the default file name. Click **Next**.
16. Review the information on the Request File Summary page. If you have corrections, click **Back** to modify the configuration. If you do not have any corrections, click **Next**.
17. Click **Finish**.
18. Open certreq.txt in a text editor and copy the text, including the “Begin” and “End” tags.
19. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
20. Paste the text from the CSR file into the field provided.

Microsoft IIS 7.x

1. Go to **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Click the server name.
3. On the **Security** section, double-click **Server Certificates**.
4. Click **Create Certificate Request** from the Actions menu.
5. Provide the following information:
    - **Common Name**: The fully qualified domain name (FQDN) for which you are requesting the SSL certificate. For a wildcard certificate, the common name must begin with an asterisk (*). For example, *.yourcompany.com.
    - **Organization**: The full legal name of your company.
    - **Locality or City**: The full name of the locality or city where your company is headquartered.
    - **State or Province**: The name of the state or province where your company is located.
    - **Country**: The two-letter ISO 3166 country code. For example, the code for the Japan is “JP”. For the other countries, refer to the [ISO list of country codes](#).

    *Note: Microsoft Windows IIS will not allow you to include the **Email Address** field in your CSR.*

6. Click **Next**.
7. On the Cryptographic Service Provider Properties window, keep the default settings (Microsoft RSA SChannel and 2048) and then click **Next**.
8. Enter a file name and location for your CSR file.
9. Open the CSR file in a text editor and copy the text, including the “Begin” and “End” tags.
10. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
11. Paste the text from the CSR file into the field provided.

Microsoft IIS 5.5 or 6.x

Note: Completing this procedure creates a pending request on your website. Do not delete this pending request. When you receive the certificate, you must install it to this pending request.

1. Go to **Control Panel** > **Administrative Tools** > **Internet Information Services**.
2. Right-click the website you are securing and click **Properties**.
3. On the **Directory Security** tab, click **Server Certificate**, and then click **Next**.
4. Select **Create a new certificate** and click **Next**.

   Note: If you are renewing an existing certificate, select the renew option and proceed to step 10.

5. Select **Prepare the request now, but send it later** and click **Next**.
6. On the **Name** field, enter a name to easily identify this certificate in the future.
7. Set the bit length to 2048. Leave the other boxes on this panel unchecked and click **Next**.
8. Enter the full legal name of your company on the **Organization** field and click **Next**.
9. Type the fully qualified domain name of your site on the **Common Name** field and click **Next**.
10. Enter the location of your organization: **Country**, **State**, and **City** and click **Next**.
11. On the **File name** box, enter the file name and the location where to save your SSL CSR. The file should have an extension of .txt. Click **Next**.
12. On the Request File Summary pane, click **Next** to generate the CSR file.
13. Open the CSR file in a text editor and copy the text, including the "`Begin`" and "`End`" tags.
14. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
15. Paste the text from the CSR file into the field provided.

Microsoft IIS 4.x

1. Open the Microsoft Management Console (MMC) for IIS.
2. Expand the **Internet Information Server** and expand the computer name you are securing.
3. Right-click the name of the website you are securing, and click **Properties**.
4. Open the **Directory Security** folder.
5. Under Secure Communications, click **Key Manager** > **Create New Key**.
6. Select **Put the request in a file that you will send to an authority** and specify a filename or accept the default.
7. Provide your company information.
8. Click **Next** and then click **Finish**.

9. Click **Yes** when prompted to save changes.
10. Open the CSR file in a text editor and copy the text, including the `"Begin"` and `"End"` tags.
11. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
12. Paste the text from the CSR file into the field provided.

Microsoft Office Communications Server (OCS) 2007

1. Go to **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007**.
2. Navigate to the Enterprise Edition Server that you installed.
3. Right-click the server name and click **Certificates**, and then click **Next**.
4. Select **Create a new certificate** and click **Next**.
5. Select **Prepare the request now, but send it later** and click **Next**.
6. On the **Name** field, enter a name to easily identify this certificate in the future.
7. Select **Mark cert as exportable** to enable export of the certificate to other servers. Click **Next**.
8. Enter the complete legal name of your company on the **Organization** field and click **Next**.
9. On the **Subject name** field, enter the fully qualified domain name of the pool.
10. Select **Automatically add local machine name to Subject Alt Name** and click **Next**.
11. Type the necessary details on the **Country**, **State/Province**, and **City/Locality** fields. Click **Next**.
12. Choose a location and file name for your new CSR. The file should have a .txt extension. Click **Save**.
13. Review the settings and finish the certificate wizard.
14. Open the CSR file in a text editor and copy the text, including the `"Begin"` and `"End"` tags.
15. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
16. Paste the text from the CSR file into the field provided.

Microsoft Outlook Web Access (OWA)

1. Open the Internet Services Manager.
2. Right-click **Default Web Site** or the site hosting your OWA component, and click **Properties**.
3. On the **Directory Security** tab, click **Server Certificate** and click **Next**.
4. Select **Create a new certificate** and click **Next**.
5. Select **Prepare the request now, but send it later** and click **Next**.
6. On the **Name** field, enter a name to easily identify this certificate in the future.
7. Set Bit length to 2048. Leave the other boxes unchecked and click **Next**.
8. Type the full legal name of your company on the **Organization** field and click **Next**.

9. On the **Common Name** field, type the FQDN of your OWA Server. Click **Next**.
10. Provide the necessary details on the **Country/Region**, **State/province**, and **City/locality** fields, and then click **Next**.
11. Choose a file name and location for the CSR and save the file as a .txt file.
12. Click **Next** to generate the file.
13. Open the CSR file in a text editor and copy the text, including the `“Begin”` and `“End”` tags.
14. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
15. Paste the text from the CSR file into the field provided.