Microsoft Exchange 2010 and 2007

Download the server certificate and intermediate certificates. Perform the following procedure for each of the intermediate certificates and then for the server certificate.

1. Go to **Start** > **Run**.
2. Type "mmc" to show the Microsoft Management Console.
3. Click **File** > **Add/Remove Snap-in**. The Add or Remove Snap-ins window appears.
4. Select **Certificates** and click **Add**.
5. Select **Computer Account**, and then click **Next**.
6. Select **Local Computer** and click **Finish** > **OK**.
7. Expand the **Certificates** folder on the left.
8. Right-click **Intermediate Certification Authorities**, and then click **All Tasks** > **Import**.
9. On the Certificate Import Wizard, click **Next**.
10. Click **Browse** and locate the intermediate certificate file.
11. Change the file extension filter to **PKCS #7 Certificates (*.spc;*.p7b)** and select the intermediate file.
12. Click **Open**, and then click **Next**.
13. Select **Place all certificates in the following store**.
14. Click **Browse**, select **Intermediate Certification Authorities**, and then click **Next**.
15. Click **Finish** and close the console window.
16. Do one of the following depending on your Microsoft Exchange version. For Microsoft Exchange 2010:

    a) Go to **Start** > **Programs** > **Microsoft Exchange 2010** > **Exchange Management Console**.
    b) Click **Manage Databases** and then click **Server Configuration**.
    c) Select your certificate on the Exchange Certificates.
    d) Click **Complete Pending Request** under the Actions panel.
    e) Click **Browse** to locate the certificate file. The file extension can be .txt or .crt.
    f) Click **Open** and then click **Complete**.

    *Note: If you receive the error, "The source data is corrupted or not properly Base64 encoded," check the **Self Signed** field. If it is "True", refresh console by pressing F5. If it still displays "True", create a new CSR and regenerate your certificate.*

    g) Click **Finish**.

h) From the **Actions** menu, click **Assign Services to Certificate**.

i) Select servers, and then click **Next**.

j) Select the services you want to assign to the certificate, and then click **Next**.

k) Click **Assign** and then click **Finish**.

For Microsoft Exchange 2007:

a) Go to **Start** > **Microsoft Exchange Server 2007** > **Exchange Management Shell**.

b) Type the following command to import the certificate:

```
Import-ExchangeCertificate -Path C:CertificateFile.crt
```

where "C:CertificateFile.crt" is the complete path and file name of your certificate.

c) Copy the thumbprint of the certificate.

d) Type the command below to enable the certificate:

```
Enable-ExchangeCertificate -Thumbprint
paste_thumbprint_here -Services "SMTP, IMAP, IIS"
```

where "paste_thumbprint_here" is the thumbprint that you copied in the previous step. Specify the services that this certificate covers inside the quotation marks. Valid service identifiers are SMTP, POP, IMAP, UM, and IIS. Do not enable unused services.

e) Close the Exchange Management Shell window.

Microsoft Exchange 2003

1. Open the Internet Information Services Manager or the custom MMC containing the Internet Information Services snap-in.
2. Expand **Internet Information Services** and browse the website where you have a pending certificate request.
3. Right-click the site name and click **Properties**.
4. Go to **Directory Security** tab > **Secure Communications** and click **Server Certificate**.
5. In the Web Server Certificate Wizard, click **Next**.

6. Select **Process the pending request and install the certificate** and click **Next**.
7. Enter the location of the certificate response file and click **Next**.
8. Read the summary screen to ensure that you are processing the right certificate and click **Next**.
9. Read the confirmation screen and click **Next**.
10. Using the Internet Services Manager, open the properties for the Exchange virtual directory.
11. Navigate to **Directory Security** tab > **Secure Communication** and click **Edit**.
12. In the Secure Communications dialog box, select **Require Secure Channel (SSL)** or select **Require 128-bit encryption**. If you select the **128-bit** check box, only the browsers that support 128-bit encryption can connect to OWA.

    Note: When users enter http://www.yourdomain.com/exchange, "HTTP 403.4 – Forbidden: SSL required Internet Information Services" error appears because OWA is configured to require SSL. The SSL uses the HTTPS protocol, thus, the users must enter the URL as https://www.yourdomain.com/exchange.

Microsoft IIS 7.x

Note: This procedure uses an individual certificate instead of a PKCS#7 certificate.

To install the intermediate certificate:

1. Go to **Start** > **Run.**
2. Type "mmc" to open the Microsoft Management Console (MMC) window.
3. Click **File** > **Add/Remove Snap-in**. The Add or Remove Snap-ins window displays.
4. On the Available Snap-ins, select **Certificates** and then click **Add**.
5. Select **Computer Account** and then click **Next**.
6. Select **Local Computer** and then click **Finish** > **OK**.
7. Return to the MMC.
8. Right-click **Intermediate Certification Authorities**, and click **All Tasks** > **Import**.
9. Import Affirmtrust_Networking.crt and then repeat the steps above to import Trend_Micro_CA.crt. After importing, these certificates should appear under Intermediate Certification Authorities**.**

To install the server certificate:

1. Go to **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Click the server name in the left pane.

3. Double-click **Complete Certificate Request** and select the server certificate you received. For example, www.trendmicro.com.crt.
4. Enter a name for the certificate file and click **OK**. The server certificate appears in the list of Server Certificates.
5. Select the web site where you want to install the certificate and click the **SSL Settings** icon.
6. On the Actions panel, double-click **Bindings** and highlight the https, and then click **Remove**.
7. Click **Add** and select **https** in the Type list.
8. Under the SSL certificate list, select the name you specified in step 4, and then click **OK**.
9. Click **Close** to exit the Site Bindings window.
10. Restart your website.

Microsoft IIS 5.5 or 6.x

To install an OV Server certificate:

1. Download the server certificate to the web server you are securing.
2. Navigate to **Control Panel** > **Administrative Tools** > **Internet Services Manager**.
3. Right-click the **Default Web Site** or the website where the CSR was created and click **Properties**.
4. On the Directory Security panel, click **Server Certificate**, which launches the certificate wizard, and then click **Next**.
5. Select **Process the pending request and install the certificate** and click **Next**.
6. Click **Browse** and locate your SSL certificate (your_domain.cer), and then click **Next**.
7. Follow the steps prompted by the wizard.
8. Test your certificate by visiting the secure URL with a browser other than Internet Explorer. Internet Explorer can verify if a site is trusted without the intermediate certificates. If the other browsers detect the site as untrusted, import the intermediate certificates.

   Note: If you are using ISA 2004 or 2006 and the server is not sending the intermediate certificates, you must fully reboot the server. If the server continues to use an old certificate or if the server does not load https at all, you may need to shut down and restart the server.

9. Back up your certificate and private key in case your server crashes.

To install an EV certificate to a Windows 2000 or 2003 server:

1. Download the server certificate to the web server you are securing.
2. Go to **Control Panel** > **Administrative Tools** > **Internet Information Services**.

3. Right-click the website where you created the CSR and click **Properties**.
4. Select the **Directory Security** tab and click **Server Certificate**, and then click **Next**.
5. Select **Process the pending request and install the certificate** and click **Next**.
6. Click **Browse** and locate your EV certificate file (your_domain_name.cer), and then click **Next**.
7. Follow the steps prompted by the wizard.
8. Get your site seal code. The AffirmTrust EV Site Seal enables all versions of Internet Explorer 7 to display a green URL bar. It should be displayed on a webpage that visitors view before they go to any of your secured pages.
    a) From the SSL AffirmTrust console, go to **Protection** > **Certificates**.
    b) Click the common name of the certificate to show the Details page.
    c) Click the **Site Seal** button and copy the Site Seal HTML code.
    d) Paste the code on the HTML of you website where you want the site seal to appear.

    Note: Internet Explorer 7 also requires the phishing filter to be enabled for the address bar to turn green.

9. Restart IIS to use the new certificate. If it does not work, shut down and restart the server.

To import the intermediate certificates:

Note: This process is unnecessary for successful installations. However, you may follow this procedure if you receive a warning that the certificate is from the company you do not trust.

1. Download and save the intermediate certificates (.crt) on your server.
2. Double-click the certificate to open the Certificate dialog box.
3. Under the **General** tab, click **Install Certificate** and click **Next**.
4. Select **Place all certificates in the following store** and click **Browse**.
5. Tick the **Show physical stores** check box.
6. Expand the **Intermediate Certification Authorities** folder and select **Local Computer**.
7. Click **OK** > **Next**, and then click **Finish**.
8. Perform this procedure for each intermediate certificate (AffirmTrust_Networking.crt and Trend_Micro_CA.crt). You may need to restart your server.

To install a Unified Communications or Wildcard certificate on multiple IIS sites:

1. Set up SSL Host Headers rather than assigning each site to use the certificate.
2. Make sure that the names of all IIS sites where you use the certificate are covered by the Unified Communications or Wildcard certificate.

Microsoft IIS 4.x

1. Obtain your root, intermediate, and server certificate files from the AffirmTrust console.
2. Open Key Manager.
3. Click the **IIS Primary SSL certificate** key in the www directory.
4. Click **Install Key Certificate** and enter the password.
5. Add the IP and Port Number when prompted for bindings. If you have no other IIS SSL certificates installed on the web server, select **Any assigned**.

   Note: If multiple certificates are installed on the same web server, each requires a separate IP address because SSL does not support host headers.

6. Click **Computers** > **Commit Changes**, or close Key Manager and click **Yes** when prompted to commit changes. The new IIS Primary SSL Server certificate is now successfully installed.
7. Back up the key in Key Manager.
   a) Click **Key** > **Export** > **Backup File**.
   b) Store the backup file on a hard drive and on another server.
8. Restart the server running IIS 4.
9. Do any of the following depending on your Service Pack:

   For Service Pack 3:

   a) Install the intermediate and root certificates in your Internet Explorer by opening each certificate and clicking **Install Certificate**.
   b) Use this IIS CA batch file to transfer all root certificates from your Internet Explorer to the IIS Certificate store.

   For Service Pack 4 or later:

   a) Double-click the root certificate to open the installation wizard.
   b) Select **Place all certificates in the following store** and click **Browse**.
   c) Click **Show Physical Stores** > **Trusted Root Certification Authorities** > **Local Computer**.
   d) Click **OK** > **Next** > **Finish**.
   e) Repeat these steps for the intermediate certificate, but place it in **Intermediate Certification Authorities**.
10. Restart the server to update the SSL certificate.

Microsoft Office Communications Server (OCS) 2007

1. Download the server certificate file to the Office Communications Server where you generated the CSR.
2. Go to **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007**.
3. Navigate to the Enterprise Edition Server.
4. Right click the Office Communications Server where the CSR was generated and click **Certificates** and then click **Next.**
5. Select **Process the pending request and install the certificate**.
6. Browse to your server certificate file and click **Next** to install the certificate.
7. Close the certificate wizard. Your SSL Certificate is now installed and ready to use.

Microsoft Outlook Web Access (OWA)

1. Copy the server certificate to the server you are securing.
2. Under the Administrative Tools, open the **Internet Services Manager**.
3. Right-click **Default Website** or the website where the CSR was created and click **Properties**.
4. On the Directory Security panel, click **Server Certificate** to start the certificate wizard, and then click **Next**.
5. Choose **Process the pending request and install the certificate**. Click **Next**.
6. Browse for the SSL certificate and click **Next**.
7. Follow the steps prompted by the wizard. The certificate is now installed.
8. You may opt to configure your OWA server to accept only 128-bit encrypted connections. This configuration enforces secure connections to the server:
    a) On the Internet Services Manager, open the properties of the Exchange virtual directory.
    b) Go to **Directory Security** tab > **Secure Communication** and click **Edit** to show the Secure Communications panel.
    c) Select the **Require secure channel (SSL)** option. To disallow users connecting with older, 40-bit encrypted browsers, select **Require 128 Bit encryption**. The certificate is capable of up to 2048 Bit encryption, but it is scalable and allows 40-bit and 56-bit connections. This also disables HTTP connections, so only 128-bit HTTPS connections will be allowed.
    d) Ensure that your firewall is configured to accept HTTPS connections. The default port is 443.