Server software page

Certificate Installation

Software

Apache (Mod_SSL and OpenSSL)

Installing a certificate using Apache (with mod_ssl) and OpenSSL

You should have received your certificate file from us, typically named "your_domain_com.crt" as well as the "CA bundle" file containing the intermediate certificates, typically named "your_domain_com.ca-bundle" or "TrustedSecureCertificateAuthority.crt."

Installing the certificate requires you to be able to make changes to Apache's configuration files, and restart the Apache server process. Please ensure you can do this before you continue.

To install a certificate using Apache:

- Copy the certificate and CA bundle file to your server into a directory where you plan to keep your certificates.
    - This is commonly /etc/ssl/.
- Edit the Apache configuration file.
    - The location of this file can vary depending on your distribution (Microsoft® Windows®, Debian/CentOS/Fedora, etc. under Linux) and the version of Apache you are using.
    - Once located, open the file in your preferred editor.
- Locate the VirtualHost section for the SSL-enabled site you are installing the certificate for.
    - This will commonly begin <VirtualHost 127.0.0.1:443>.
- Add the following lines into the VirtualHost section, making sure to change the paths of the files to correspond to the locations of the files on your server.
    - Apache 1.3.x:

      SSLEngine on
      SSLCertificateKeyFile /etc/ssl/ssl.key/server.key
      SSLCertificateFile /etc/ssl/ssl.crt/yourDomainName.crt
      SSLCACertificateFile /etc/ssl/ssl.crt/yourDomainName.ca-bundle
    - Apache 2.x:

      SSLEngine on
      SSLCertificateKeyFile /etc/ssl/ssl.key/server.key
      SSLCertificateFile /etc/ssl/ssl.crt/yourDomainName.crt
      SSLCertificateChainFile /etc/ssl/ssl.crt/yourDomainName.ca-bundle
- Save the changes to the file.
- Restart Apache.
    - It is sometimes required to stop then start Apache, instead of issuing the restart command for the changes to take effect.

Please note: If you have password protected your private key, you will be prompted to enter the password each time Apache is started or restarted, otherwise, Apache will not fully start.

The configuration file is often called httpd.conf or apache.conf, although sometimes the SSL-specific section is placed in a separate file called ssl.conf and linked from the main configuration by an "include" command. Sometimes, the VirtualHost section will be in a specific file for that site, in a sub-directory often labelled sites-enabled/.

Much of the layout of Apache's configuration files and directory naming conventions is controlled by the distribution of operating system you are using. It is recommended that you look at the distribution's own site and documentation to confirm the locations: Debian, CentOS, Fedora, etc.

cPanel and WHM

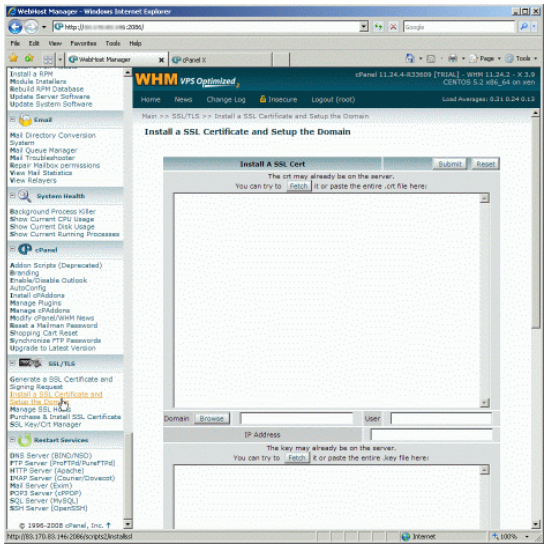
Installing a certificate on cPanel or WHM

To install your certificate, you will need to log into your cPanel or WHM account. Both cPanel (the end-user control panel) and WHM (the administrator panel) have slightly different ways to install certificates.

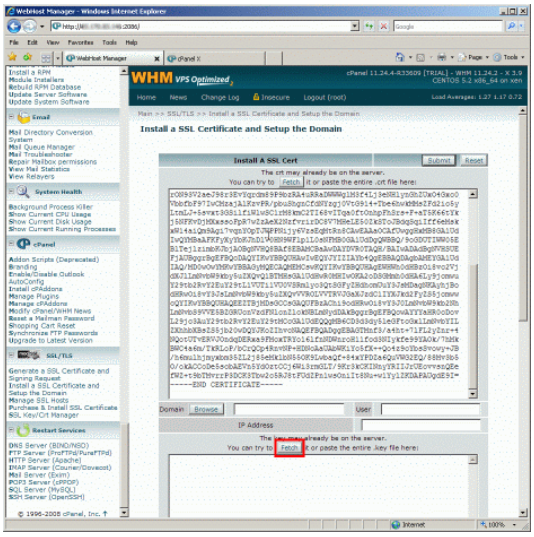
You will have received your certificate file from us, typically named "your_domain_com.crt," as well as the "ca-bundle" file, which has the extension ".ca-bundle."

To install a certificate using WHM:

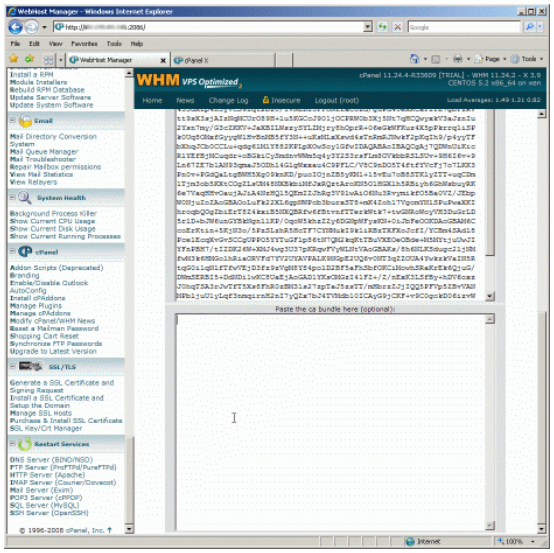
- Log into WHM. From the menu, navigate to the SSL/TLS section, and click "Install a SSL Certificate and Setup the Domain."



- Open the certificate file in a text editor (this is the file with your domain in the filename), and copy and paste the contents into the top box. Click the second “Fetch” button, near the key file section (highlighted in red).
    - This will retrieve the private key and domain, user and IP address information from the server and populate it into the form for you.

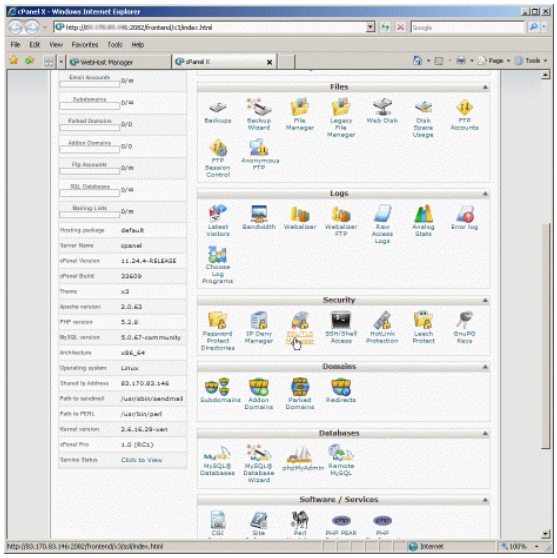


- At the bottom of the form, locate a box labelled “Paste the ca bundle here (optional).”
- Copy and paste the contents of the “ca-bundle” file into the aforementioned box.
- Click “Submit.”
    - A minute or two later, the certificate will be installed and setup on the domain.
- See notes below if you did not receive the “ca-bundle” file.

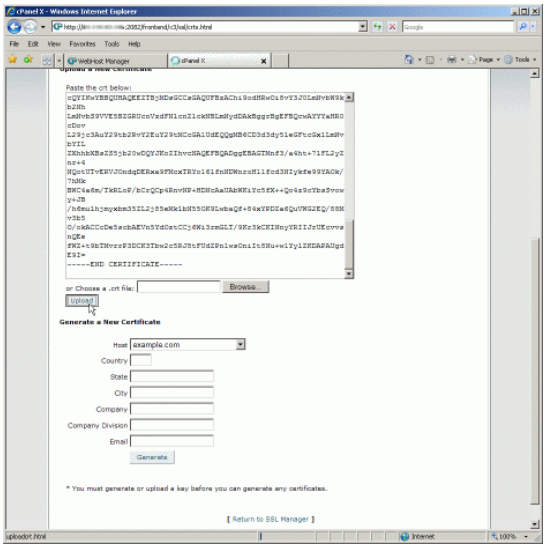


To install a certificate using cPanel:

- Log into cPanel.
- Under the Security menu, click the “SSL/TLS Manager.”



- Click the bottom link for “Certificates.”
- Copy and paste the contents of your certificate file, typically named “your_domain_com.crt,” in the box saying “Paste the crt below.”
- Alternatively, you can upload it through the browser by clicking the “Upload” button.



Please note: If you did not receive the “ca-bundle” file, it can be constructed from the intermediate certificate(s). Simply create a new text file, and copy the contents of the intermediate certificates into it, one after another. Copy them in order, top-to-bottom: “TrustedSecureCertificateAuthority.crt.”

Microsoft Exchange 2007

Installing a certificate on Microsoft Exchange 2007

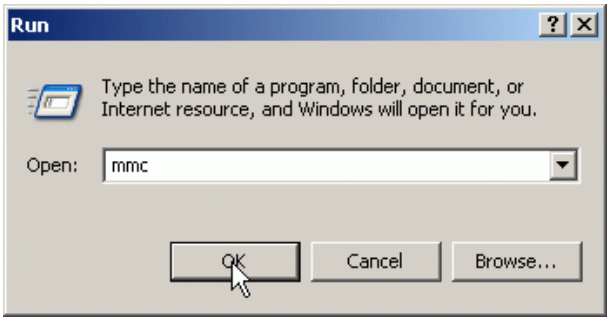
You will have received your certificate file from us, typically named “your_domain_com.cer.” Alternatively, you may have received it as several files: “your_domain_com.crt” and “TrustedSecureCertificateAuthority.crt.” The root certificate “EntrustSecureServerCA.crt” may also be provided.

To install a certificate using Microsoft Exchange 2007:

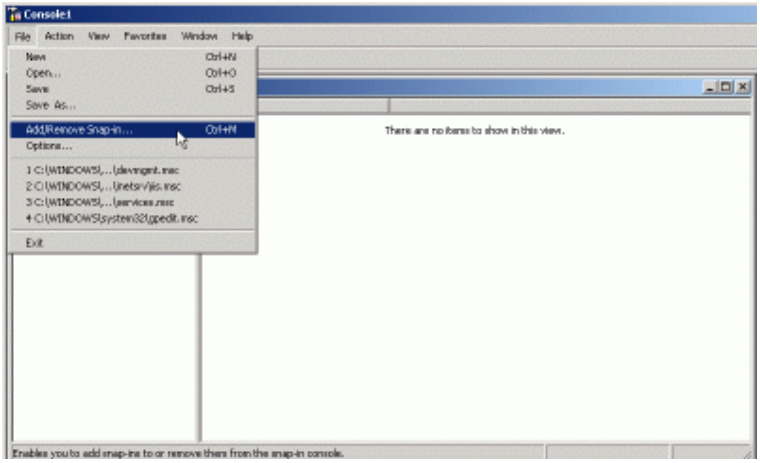
- Copy the file(s) you received to the server, we suggest to the main drive - C:\
- Open the Exchange management shell. This is done by clicking Start > Programs > Microsoft Exchange Server 2007 > Exchange Management Shell.
- Type the following command onto a single line, and run it.
    - Import-ExchangeCertificate -Path C:\your_domain_name-or-order_number.crt | Enable-ExchangeCertificate -Services "SMTP, IMAP, POP, IIS"
- The certificate is now installed. You may also need to follow the next steps to install the intermediate certificate(s) on the server.

Installing the intermediate certificate(s):

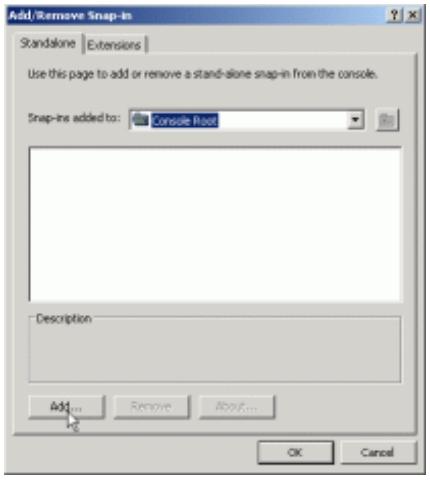
1. Click the Start menu, and choose “Run.”
2. Enter the command “mmc” and click “OK.”



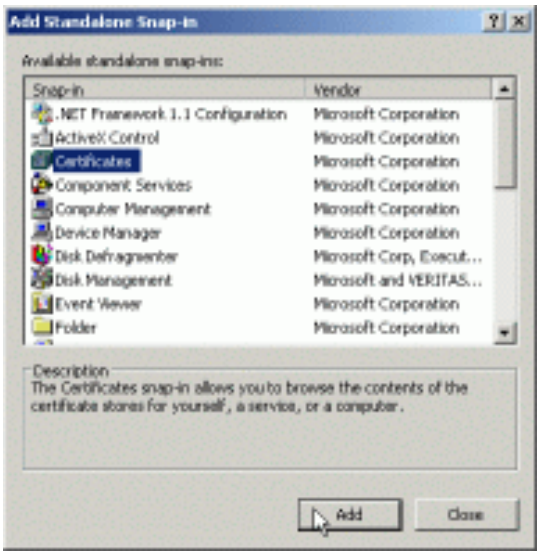
3. Click the File menu, and select the “Add\Remove Snap-in” option.



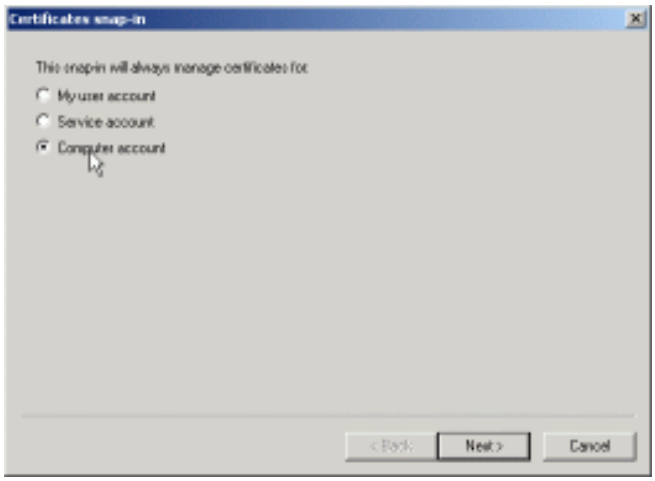
4. From the pop-up window, click the “Add” button.



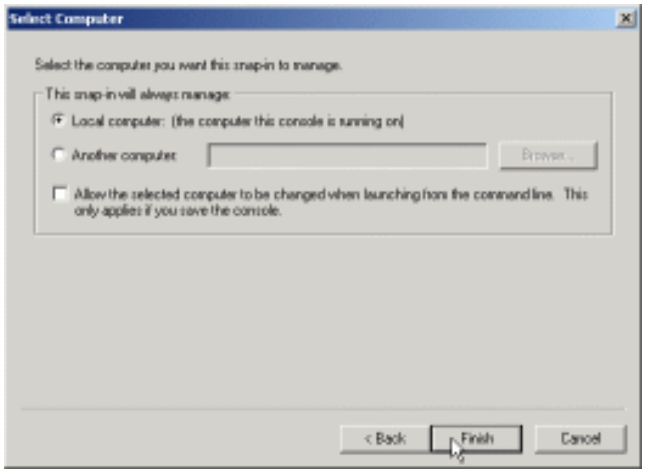
5. Choose “Certificates,” click the “Add” button.



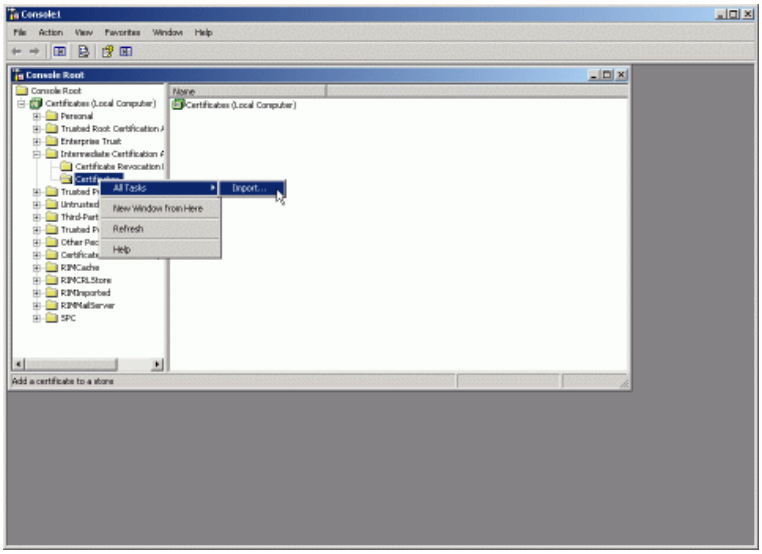
6. Change the setting to “Local Computer.” Click “Next.” **This step is extremely important!**



7. Choose “Local Computer.” Click “Finish.” Click “Close” in the “Add Standalone Snap-in” window, and “OK” in the remaining window.



8. On the left side, expand the folder for “Intermediate Certification Authorities.”
9. Right-click on the “Certificates” sub-folder, selecting “All Tasks” then clicking “Import.”
10. This will start the Certificate Import Wizard. Click “Next.”



11. When prompted to choose a file, select the “TrustedSecureCertificateAuthority.crt” file.
12. Click “Next,” “Next,” and then “Finish” to complete the wizard.
13. If required, repeat steps 8 through 11 with the certificate, named “TrustedSecureCertificateAuthority.crt” files.

Please note: If you use an ISA server in front of your Exchange server(s), you will need to export the certificate from Exchange onto the ISA server, and import. When doing so, you must be sure to include the whole certificate chain.

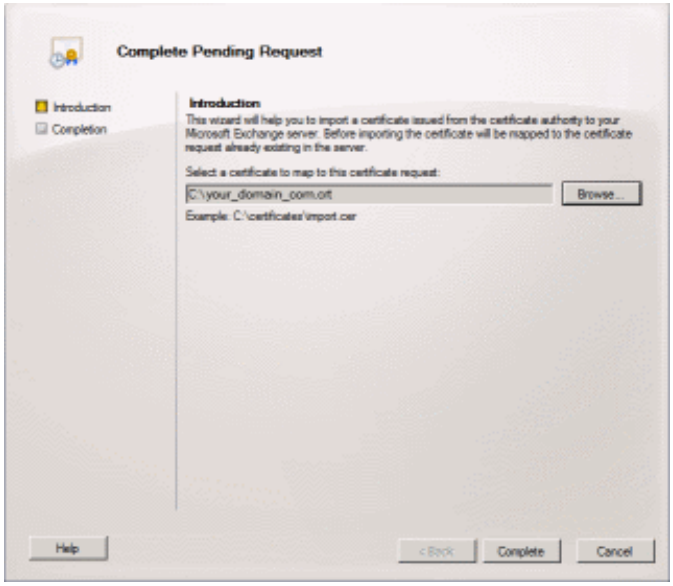
Microsoft Exchange 2010

Installing a certificate on Microsoft Exchange 2010

You will have received your certificate file from us, typically named "your_domain_com.cer." Alternatively, you may have received it as several files: "your_domain_com.crt" and intermediate certificate, named "TrustedSecureCertificateAuthority.crt." The root certificate "EntrustSecureServerCA.crt" may also be provided.

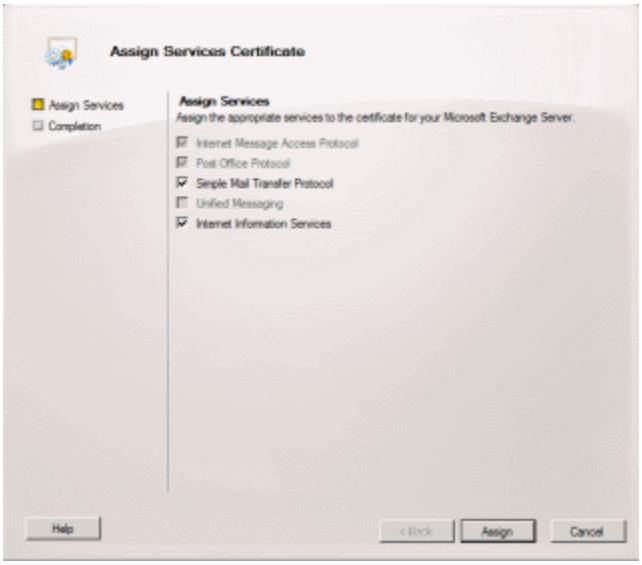
To install a certificate using Microsoft Exchange 2010:

- Copy the file(s) you received to the server, we suggest to the main drive - C:\
- Open the Exchange management shell. This is done by clicking Start > Programs > Microsoft Exchange Server 2010 > Exchange Management Shell.
- Click the link for "Manage Databases," and then "Server Configuration."
- Select your certificate from the list at the bottom-middle of the screen.
- Click "Complete Pending Request" from the right menu, or right-click on the certificate and choose "Complete Pending Request."
- When the wizard starts, choose your certificate file, typically named "your_domain_com.cer."
- Click "Complete."



- Select your certificate again from the list at the bottom of the screen.
- Click "Assign Services To Certificate" from the right menu, or right-click on the certificate and choose "Assign Services To Certificate."

- Check or uncheck the services required, and click “Assign.”



- Click “Finish” on the final stage of the wizard, and the certificate will be correctly installed and assigned.

Please note: Often Microsoft Exchange 2010 will show an error message stating “The source data is corrupted or not properly Base64 encoded” when completing the pending request. This error is incorrect and can be ignored.

If you use an ISA server in front of your Exchange server(s), you will need to export the certificate from Exchange onto the ISA server, and import. When doing so, you must be sure to include the whole certificate chain.

F5 BigIP

Installing a certificate on F5 Big-IP appliances

You will have received your certificate file from us, typically named “your_domain_com.crt,” and intermediate certificate named “TrustedSecureCertificateAuthority.crt.” The root certificate “EntrustSecureServerCA.crt” may also be provided.

Copy the file(s) you received to the server.

To install a certificate using F5 BigIP version 9 or later:

1. Open and log into the BigIP web interface.
2. Under the Local Traffic menu, select “SSL Certificates.”
3. Under “General Properties,” click on the name you assigned when generating the CSR.
4. Browse to the certificate file you received: “you_domain_com.crt.”
   Click “Open,” then “Import.”
5. Return to the Local Traffic menu, and again select “SSL Certificates.”
   Click “Import.”
6. Under “Import Type,” select “Certificate” and click “Create New.”
   Enter the name “CSC Trusted SecureRootCA.”
7. Browse to the intermediate certificate file “TrustedSecureCertificateAuthority.crt.”
   Click “Open,” then “Import.”
8. Configure your certificate for use.
   Go to the SSL profile that you require the certificate for.
   Click “Configuration,” then “Advanced.”
9. Choose the certificate that you installed in step 3.
   Under the section labelled “Chain,” choose the “CSC Trusted SecureRootCA” you imported in step 5.
10. Save the configuration and exit.
    The certificate installation and setup is complete.

To install a certificate using F5 BigIP version 4.x:

You should have been provided with a “ca bundle” file, named “your_domain_com.cabundle.” If not, downloaded it from: http://www.csctrustedsecure.com/root_intermediate.html.

- Copy the “ca bundle” file and the certificate file (“your_domain_com.crt”) to the Big-IP Appliance.
- Rename the “your_domain_com.crt” certificate file to “your.domain.com.crt” and move it into the folder: /config/bigconfig/ssl.crt/.
- Rename the “ca bundle file to “intermediate-ca.crt” if it is not already, and move the file to the folder: /config/bigconfig/ssl.crt/.
- Finally, execute the below two commands to install the certificate:
  # bigpipe proxy :443 disable
  # bigpipe proxy :443 enable

IBM HTTP Server

Installing a certificate signing request (CSR) using IBM HTTP server

You will have received your certificate file from us, typically named "your_domain_com.crt," as well as the intermediate file, %%INTERMEDIATE%%. The root certificate "EntrustSecureServerCA.crt" is also provided.

To install a certificate using IBM HTTP server:

1. Start the IKEYMAN software either by running the command "IKEYMAN" or loading the GUI version.
2. Select "Key Database File" from the main menu, and choose "Open."
3. Choose and enter a new key database name. Click "OK."
4. Enter your password for the database.
5. Select "Signer Certificates" in the key database content frame, click the "Add" button.
6. Add the root certificate, "EntrustSecureServerCA.crt," first.
   Select the root certificate file, and click "OK."
7. Repeat Steps 5 and 6 with the intermediate %%INTERMEDIATE%%
8. Return to the Key Database menu, and select "Personal Certificates."
9. Click the "Receive" button, and locate the certificate for the site (typically named "your_domain_com.crt").
   - Click "OK."
   - The certificate is now installed and can be used by the server.

iPlanet 4.x or SunONE 6.x

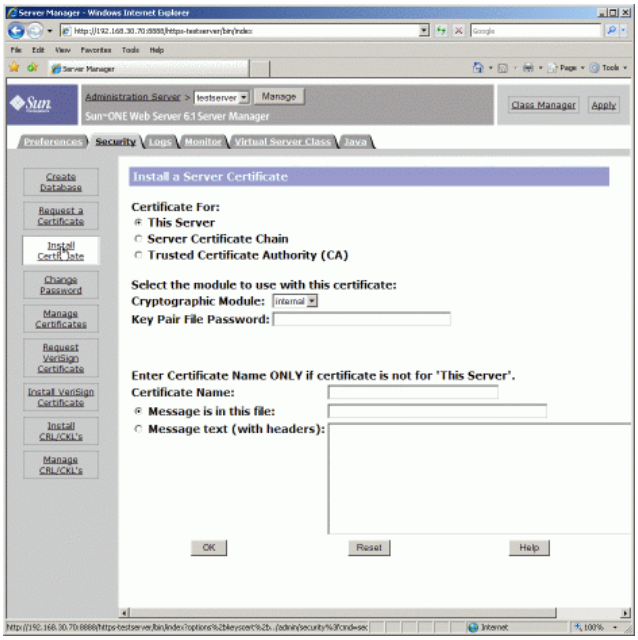
Installing a certificate on iPlanet 4.x or SunONE Application Server 6.x

You will have received your certificate file from us, typically named "your_domain_com.crt," as well as the intermediate, %%INTERMEDIATE%%. The root certificate "EntrustSecureServerCA.crt" is also provided.

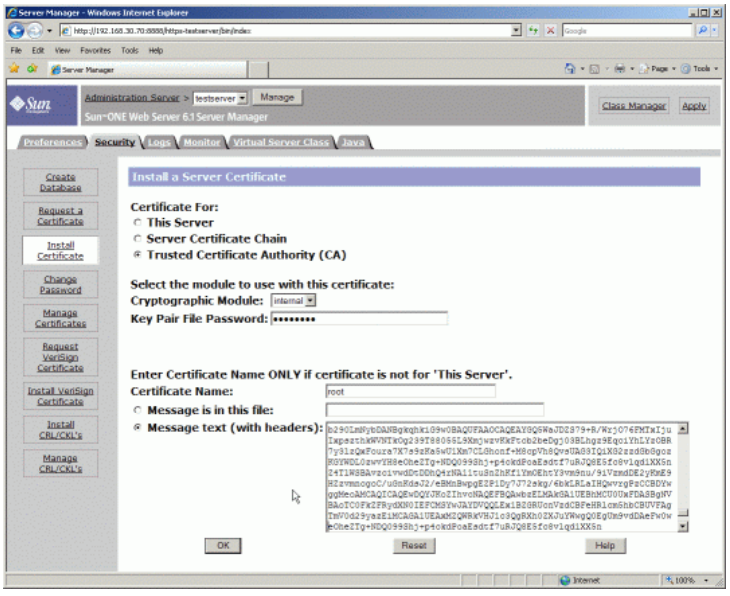
To install a certificate using iPlanet 4.x or SunONE 6.x:

Log into the administrative web-interface of your iPlanet or SunONE server. This is usually at: http://<yourserver>:8888/.

1. Log into the iPlanet or SunONE administation interface.
   Select the server instance you require the certificate for and click "Manage."
2. Click the Security tab, and from the left menu, and choose "Install Certificate."

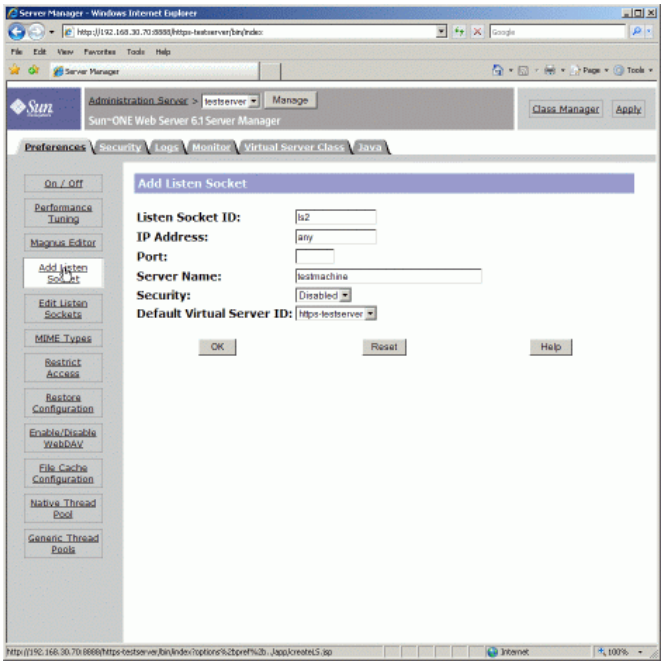


3. Change the “Certificate For:” option to “Trusted Certificate Authority.”
   - Enter the “Key Pair File Password” (the password when iPlanet was setup or the CSR was generated).
   - Enter a certificate name of “root.”
   - Now you need to upload the root certificate (the “EntrustSecureServerCA.crt” file). You can either enter the location to the file, or open it in a text-editor and copy and paste the contents into the box.
   - Click “OK.”



4. Click “Add Server Certificate” and accept any pop-up messages when you are shown the certificate information.
5. Now repeat steps 2 through 4 with the intermediate “TrustedSecureCertificateAuthority.crt.”
   Choose the “Certificate For:” option “Server Certificate Chain” for each intermediate(s).
6. Finally repeat Steps 2 through 4 using the site certificate (the file which has your domain in the filename).
   Choose the “Certificate For:” option, “This Server,” and do not enter a “Certificate Name.”
7. The certificate is installed, and now you can setup the server to use it.
   - Click the Preferences tab on the top menu.
   - Choose “Add Listen Socket.”

Please note: If you have iPlanet 4.x, encryption is turned on with the “Encryption On/Off” button under the Preferences menu. Simply choose “on” and enter a port number (usually 443). For other versions of iPlanet or SunONE, continue the steps.



- Enter the listen socket details.
  - Set the “Listen Socket ID” to a name for this setting.
  - Enter the IP address and port, usually 443.
  - Enter the server name and change the security drop-down to “Enabled.”
  - Set the “Default Virtual Server ID” (the default option is usually selected), click “OK.”
- The server is now configured to use the certificate.
- A restart of the server may be required for the changes to take effect.

Java-Based Webservers

Installing a CSR with a Java-based webserver such as Tomcat, using keytool

You will have received your certificate file from us, typically named “your_domain_com.crt” as well as the intermediate, %%INTERMEDIATE%%. The root certificate “EntrustSecureServerCA.crt” is also provided.

To install a certificate using Java-based webservers:

Copy the files to your server, and then move to the directory where the keystore that was used to generate the CSR is located.

1. Import the root certificate (called “EntrustSecureServerCA.crt”), with the following command:
    - keytool -import -trustcacerts -alias root -file EntrustSecureServerCA.crt -keystore my_keystore.jks
    - Replace the file “my_keystore.jks” with the filename and path you wish to locate the keystore. **Do this in all the commands below as well.**
2. Import the intermediate certificate (called “TrustedSecureCertificateAuthority.crt”), with the following command:
    - keytool -import -trustcacerts -alias TrustedSecureCA -file TrustedSecureCertificateAuthority.crt -keystore my_keystore.jks
    - Repeat this command with any other intermediates certificates you received, “TrustedSecureCertificateAuthority.crt.”
3. Import the site certificate (the file with your domain in the filename), with the following command:
    - keytool -import -trustcacerts -alias server -file your_domain_com.crt -keystore my_keystore.jks
    - The “server” alias should be the same alias name as you used when creating the CSR. For Tomcat servers, this should be “tomcat.”
4. The certificates are all installed in the keystore, and you can configure your software to use that keystore.
    - To do this with Apache Tomcat, you can edit the “server.xml” file.
        - Open the file, and search for a line that looks like the below, replacing the parts highlighted to match your keystore (port, keystoreFile and keypass): <Connector port="443" maxHttpHeaderSize="8192" maxThreads="150" minSpareThreads="25" maxSpareThreads="75" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="/path/to/my_keystore.jks"keypass="mykeystorepassword"/>

Please note: If you do not enter an alias with the "-alias" command flag when generating the CSR, the default alias used will be "mykey." Use this alias at step 3. For Tomcat, change the "-alias server" to "-alias tomcat."

Microsoft IIS 4.x

Installing a certificate on Microsoft IIS 4.x

You will have received your certificate file from us, typically named "your_domain_com.crt" as well as the intermediate named "TrustedSecureCertificationAuthority.crt." The root certificate "EntrustSecureServerCA.crt" is also provided.

To install a certificate using Microsoft IIS 4.x:

1. Copy all of the certificate files to the server.
2. Go to the "Key Manager."
   - Instructions for this can be found by following steps 1 through 7 of the Microsoft IIS 4.x CSR generation instructions.
3. Install the site certificate by clicking on the key in the "www" directory (usually represented by a broken key icon with a line through it).
   - Choose "Install Key Certificate" and select the certificate file.
   - This is the certificate file with your FQDN in the filename.
4. Enter a password.
   - If you chose one earlier during CSR generation, use that password. If not, leave the field empty.
5. You will be prompted for bindings for the site.
   - Enter the IP for the site, and the port number, usually 443 unless you specifically choose otherwise.
   - Using "Any Assigned" IP is acceptable if you do not have any other sites with SSL certificates on the server.
6. Close Key Manager, choosing "Yes" when prompted to save the changes. The certificate is now installed.
7. If you have not already installed the intermediate certificates, please continue with the next steps.

Installing the intermediate certificates:

1. Double-click on the "EntrustSecureServerCA.crt" certificate file. This will begin the installation wizard.
2. Choose "Place all certificates in the following store" followed by the "Browse" button.

3. Click “Show physical stores” and select, “Trusted Root Certification Authorities,” then choose “Local Computer.”
    - Click “OK,” then “Next.”
    - Choose “Finish” to complete the wizard.
4. Repeat steps 1 through 3 for the “TrustedSecureCertificateAuthority.crt” files, but instead of “Trusted Root Certification Authorities,” select “Intermediate Certification Authorities.”
5. Restart the server. The whole server will need to be restarted for the changes to take effect, not just IIS.

Microsoft IIS 5.x and 6.x

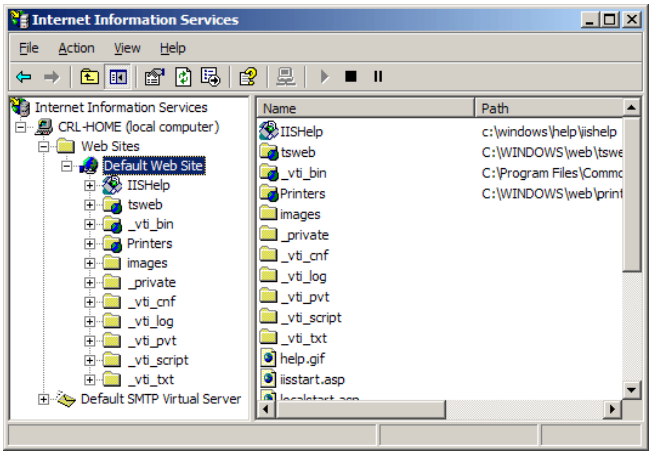
Installing a certificate on Microsoft IIS 5.x and 6.x

You will have received your certificate file from us, typically named “your_domain_com.cer.” Alternatively, you may have received it as several files: “your_domain_com.crt” and “TrustedSecureCertificateAuthority.crt.” The root certificate “EntrustSecureServerCA.crt” may also be provided.

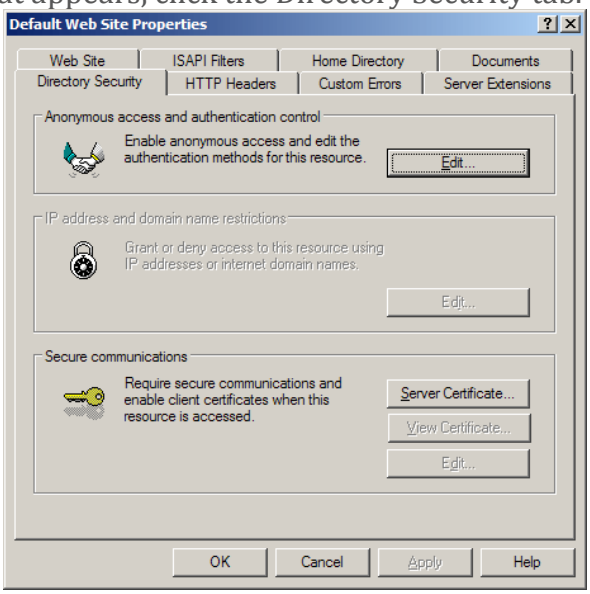
If you received a single file with a .cer extension, you only need follow the first half of the instructions. Otherwise, please follow the instructions completely.

To install a certificate using Microsoft IIS 5.x and 6.x:

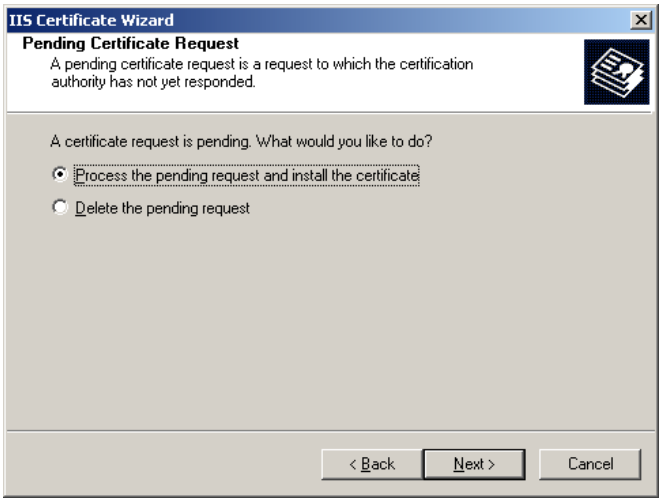
1. Copy the file(s) you received to the server.
2. Log in to the server.
3. Go to Control Panel > Administrative Tools and double-click “Internet Services Manager.”



4. Right-click on the website you wish to install the certificate on, and select "Properties."
5. From the window that appears, click the Directory Security tab.



6. Click the "Server Certificate" button to begin the Certificate Wizard. Select the option "Process the pending request and install the certificate."
   - Click "Next."

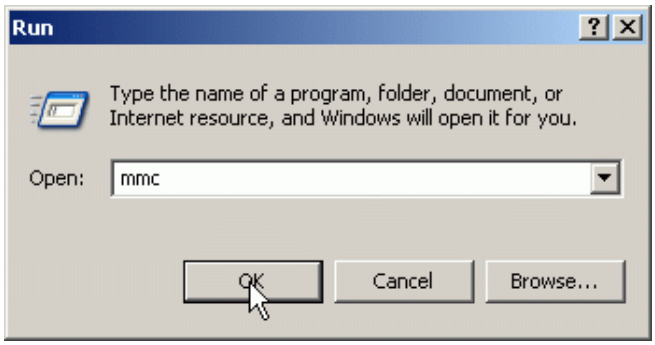


7. Browse to the location of the certificate file. This is the file with your domain name within the filename.
   - Click "Next."
8. Check the summary information screen, and click "Next."
   - Click "Next" or "Finish" to complete the wizard.

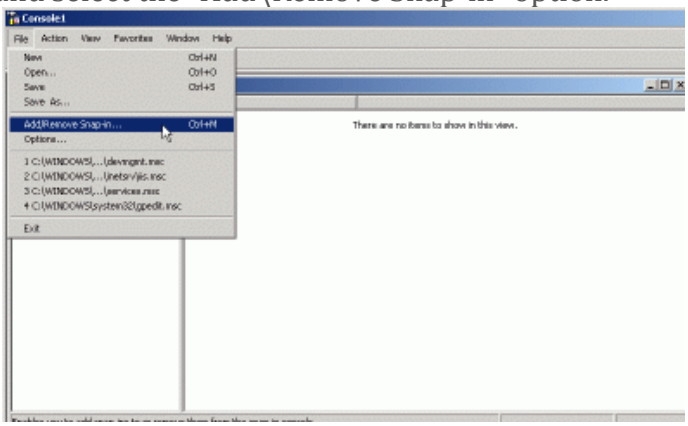
9. The certificate should now work, although it can sometimes require a restart of IIS to bring the new certificate into effect.

Installing the intermediate certificates:

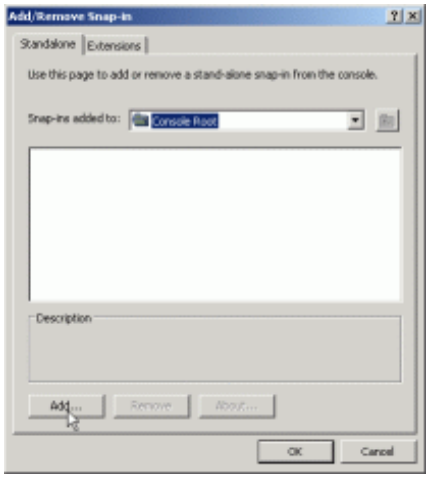
1. Click the Start menu, and choose “Run.”
2. Enter the command “mmc” and click “OK.”



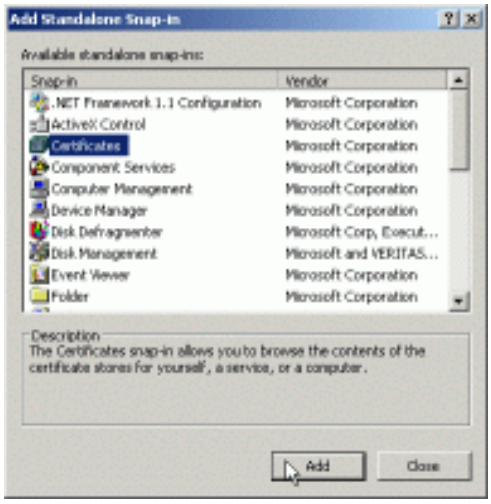
3. Click the File menu, and select the “Add\Remove Snap-in” option.



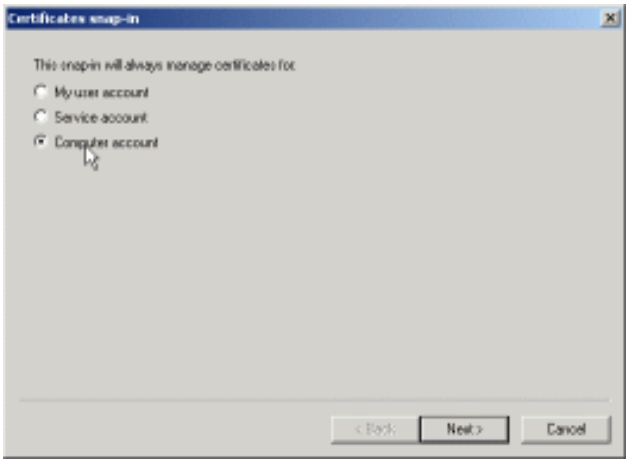
4. From the pop-up window, click the “Add” button.



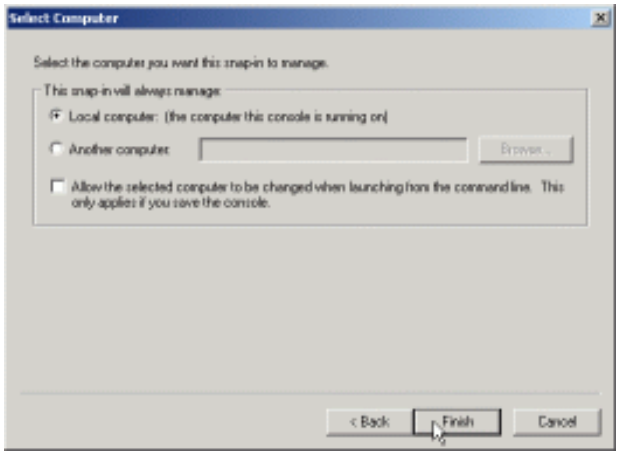
5. Choose “Certificates,” click the “Add” button.



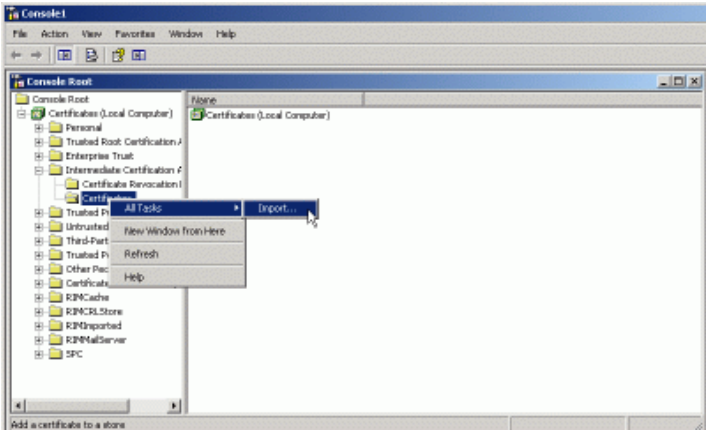
6. Change the setting to “Local Computer.”
7. Click “Next.” **This step is extremely important!**



8. Choose “Local Computer.”
    - Click “Finish.”
    - Click “Close” in the “Add Standalone Snap-in” window.
    - Click “OK” in the remaining window.



9. On the left side, expand the folder for "Intermediate Certification Authorities."
    - Right-click on the Certificates sub-folder, selecting "All Tasks" then clicking "Import." This will start the Certificate Import Wizard.
    - Click "Next."



10. When prompted to choose a file, select the "TrustedSecureCertificateAuthority.crt" file.
    - Click "Next," "Next," then "Finish" to complete the wizard.
11. If required, repeat steps 9 and 10 with the certificate, named "TrustedSecureCertificateAuthority.crt" files.

Please note: The installation should be performed on exactly the same server and site that the CSR was generated upon. The intermediate certificates need only be installed once per physical server.

Microsoft IIS 7.x

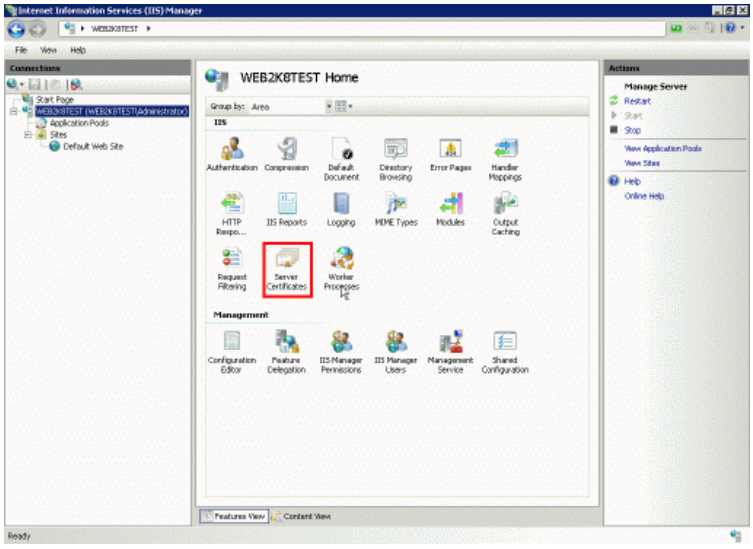
Installing a certificate on Microsoft IIS 7.x

You will have received your certificate file from us, usually named “your_domain_com.cer.” Alternatively, you may have received it as several files: “your_domain_com.crt” and intermediate certificate, named “TrustedSecureCertificateAuthority.crt.” The root certificate “EntrustSecureServerCA.crt” may also be provided.

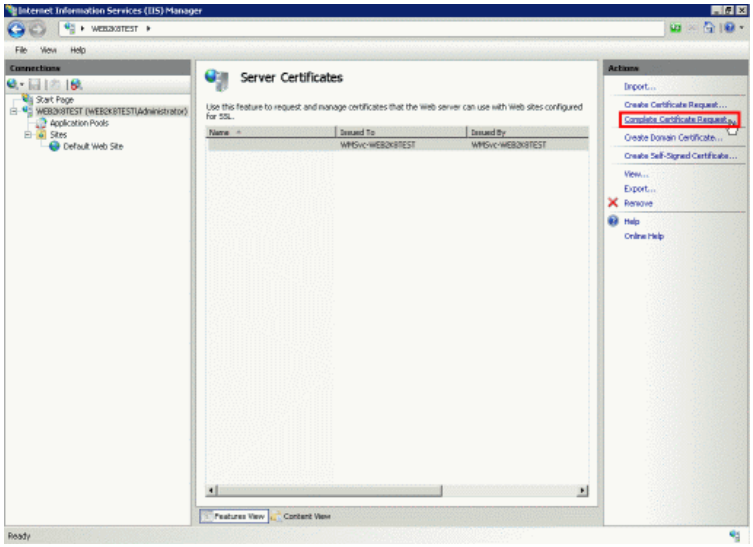
If you received a single file with a .cer extension, you only need follow the instructions here. Otherwise, please follow the instructions in this guide, and then you will need to install the necessary intermediate certificates by following the second half of the Installation Guide for IIS 5.x and 6.x - titled “Installing the Intermediate Certificates.”

To install a certificate using Microsoft IIS 7.x:

- Copy the file(s) you received to the server.
- Click the Start menu.
- Select “Administrative Tools,” then “Internet Information Services (IIS) Manager.”
- Click the server name.
- In the menu, click the “Server Certificates” button in the Security section.

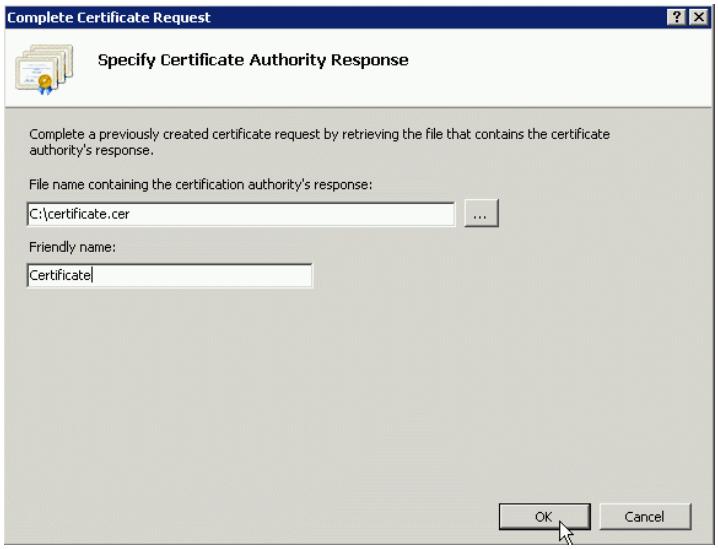


- On the right side, click the “Create Certificate Request.” Action to begin the Request Certificate Wizard.

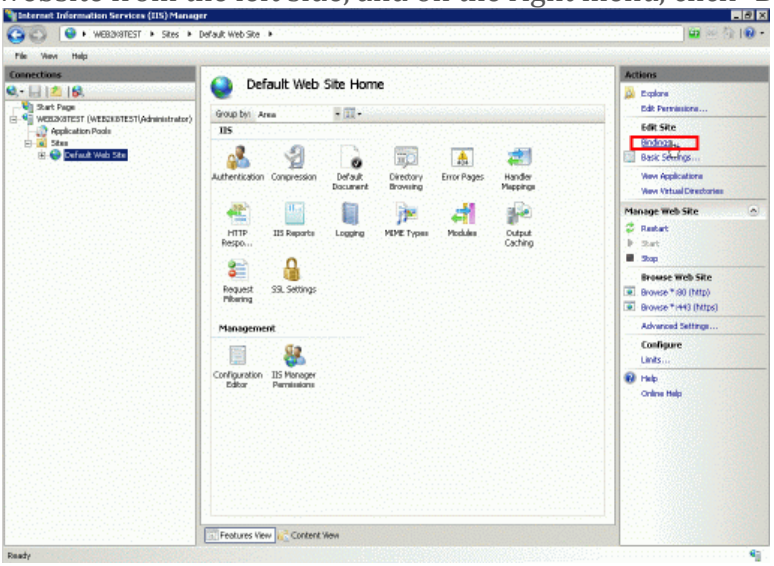


- The wizard will prompt for the certificate.
    - Enter the certificate path and filename (this can have a .cer or .crt extension).
    - Enter a “Friendly Name.” This is simply a name for the certificate for your own reference. We advise you to use the domain name of the certificate.
    - Click “OK,” and the certificate will be installed.

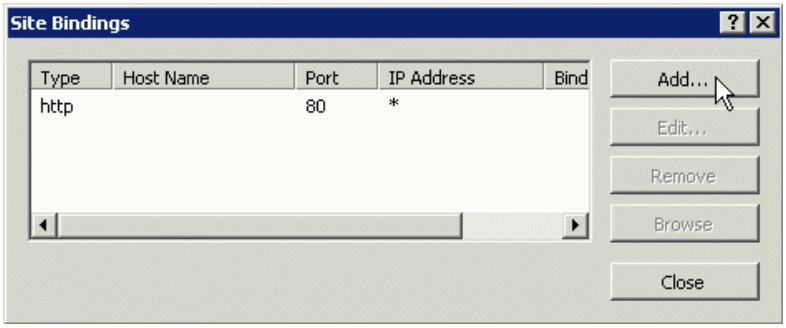
Please note: Due to a bug in IIS 7, you may receive an error message at this point, "Cannot find the certificate request associated with this certificate file. A certificate request must be completed on the computer where it was created,” or an error referring to a "Bad ASN1 tag.” As long as you generated the CSR on this server, you can simply click “OK” to the error message, and refresh the certificate list in IIS 7. In most cases, the certificate will actually be correctly installed.



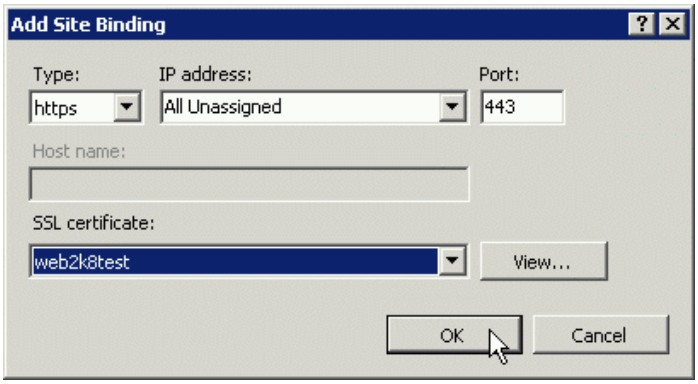
- Now that the certificate is installed, IIS 7 requires that bindings be added to the site requiring the certificate.
    - Select the website from the left side, and on the right menu, click “Bindings.”



- In the “Site Bindings” pop-up, click the “Add” button.



- Change the “Type” setting to “https.”
    - Select the site’s IP address (or leave to “All Unassigned” if this is the only site with an SSL certificate on this server).
    - Leave the Port at 443 unless you know you can change it.
    - From the SSL certificate menu, choose the name of the certificate you just installed. The “View” button can be used to confirm which certificate you have chosen.
    - Click “OK” to add the binding, and click “Close” in the “Site Bindings” window.



- The certificate is now installed on the site.

Oracle (Using Oracle Wallet Manager)

Installing a certificate on Oracle using Oracle Wallet Manager

You will have received your certificate file from us, typically named "your_domain_com.crt," as well as the intermediate, %%INTERMEDIATE%%. The root certificate "EntrustSecureServerCA.crt" is also provided.

It is important that the certificates are imported in the correct order for Oracle to accept the certificate.

To install a certificate using Oracle Wallet Manager:

1. Select "Operations" from the main menu.
    - Choose the option "Import Trusted Certificate."
2. Choose "Paste the Certificate" and click "OK."
    - A window will appear with the message "Please provide a base64 format certificate and paste it below."
        - Open the root certificate file ("EntrustSecureServerCA.crt") in a text-editor and copy and paste the contents into the area provided.
        - Click "OK."
3. The root certificate should now be installed.
4. Repeat the process with the intermediate %%INTERMEDIATE%%. Make sure to install them in order.
5. Select "Operations" from the main menu. Choose the option "Import Trusted Certificate."
6. Return to the main menu, and select "Operations."
    - Choose the option "Import User Certificate."

- As in step 2, click “Paste the Certificate” and copy and paste the certificate in as before. The certificate file is the one typically named with your domain, like: “your_domain_com.crt.”
- Click “OK” and the import should be successful.

7. The certificates are now all imported, and the status of the Wallet should be “ready.”
8. Save the changes to the wallet, and you can use it with your Oracle software.

Plesk

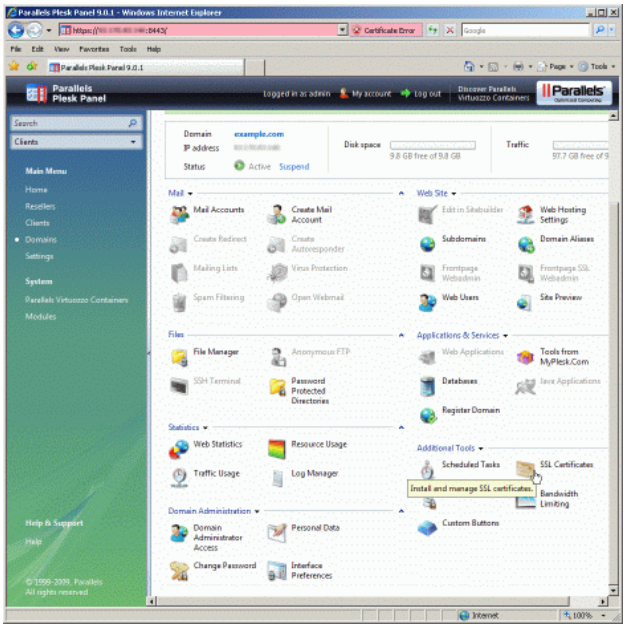
Installing a certificate on Parallels Plesk

To install your certificate, you will need to log in to your Plesk account. The screenshots are from the latest Plesk release (v9), but the instructions apply to versions 7-9.

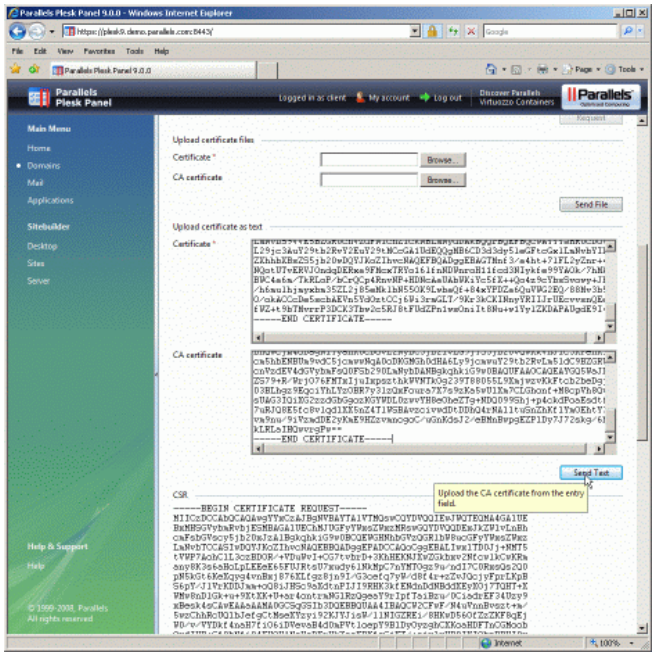
You will have received your certificate file from us, typically named ”your_domain_com.crt,” as well as the intermediate, %%INTERMEDIATE%%. The root certificate “EntrustSecureServerCA.crt” is also provided.

To install a certificate using Parallels Plesk:

1. Log into Plesk.
2. Click on “Domains” from the left menu, then click the domain you wish to request the certificate for.
3. Click the “SSL Certificates” icon.



4. Click the name of the certificate in the list.
5. Scroll down until you see two boxes for uploading text: “Certificate” and “CA certificate.”
    - Copy and paste the contents of the certificate file (typically named ”your_domain_com.crt”) into the “Certificate” box.
6. Now create the “CA certificate” to be pasted into the second box.
    - Paste in the contents of the root certificate (“EntrustSecureServerCA.crt”).
    - Then paste the contents of each intermediate certificate you have been sent, one after another (“TrustedSecureCertificateAuthority.crt”).



7. Click the “Send Text” button.
    - This will upload and install the certificate.
    - Should you receive an error along the lines of “The CA certificate does not sign the certificate,” check step 5, where you paste all the certificate files together.