User Guide
Generate Certificate Signing Request (CSR) & Installation of SSL Certificate

APACHE MODSSL

Generate CSR

1. Type this command to generate key:
   $ openssl genrsa -out www.virtualhost.com.key 2048

   ***Note**: Please make a backup of your key.*

2. Next type this following command to generate CSR:
   $ openssl req -new -key www.virtualhost.com.key -out www.virtualhost.com.csr

   ***Note**: Please do not enter your personal name.*

3. Submit CSR to TMCA.

Installation

1. Extract all of the contents of the ZIP file that was sent to you and copy/move them to your server. The extracted contents will typically be named: ***yourDomainName.crt*** and ***yourDomainName.ca-bundle***

   Note: If you received several .crt files in your ZIP file please use the step below to make ***yourDomainName.ca-bundle***

   GUI Text Editor

   a. Open All files in a text editor. (Remember, not your domain certificate.)
   b. Create a new blank text file.
   c. Copy contents of all files in reverse order and paste them into the new file.
      Example: Intermediate 3, Intermediate 2, Intermediate 1, Root Certificate.

   d. Save newly created file as '**yourDomain.ca-bundle**'.

      Command Line

      Linux or UNIX-like Operating Systems:
      -- **cat EssentialSSLCA_2.crt ComodoUTNSGCCA.crt UTNAddTrustSGCCA.crt AddTrustExternalCARoot.crt > *yourDomain.ca-bundle***

      Windows or DOS:
      -- **copy EssentialSSLCA_2.crt + ComodoUTNSGCCA.crt + UTNAddTrustSGCCA.crt + AddTrustExternalCARoot.crt *yourDomain.ca-bundle***

2. Move all of the certificates related files to their appropriate directories.

   A typical setup:
   - Move the Private Key that was generated earlier to the **ssl.key** directory, which is typically found in **/etc/ssl/**. This must be a directory which only Apache can access.

   - Move the ***yourDomainName.crt*** and ***yourDomainName.ca-bundle*** to the **ssl.crt** directory, which is typically found in the **/etc/ssl/** directory.

3. Edit the file that contains the SSL configuration with your preferred text editor.
   Examples: nano, vi, pico, emacs, mousepad, notepad, notepad++, etc.

   Note: The location of this file may vary from each distribution. It will be referenced in the Apache global configuration file. Look for the lines starting with **include**.

   Apache Configuration File:
   - **Fedora/CentOS/RHEL:** */etc/httpd/conf/httpd.conf*
   - **Debian and Debian based:** */etc/apache2/apache2.conf*

   SSL Configuration File:
   Some possible names:
   - httpd-ssl.conf
   - ssl.conf
   - In the **/etc/apache2/sites-enabled/** directory.

Note: If need be please consult your distribuiton's documentation on Apache and SSL or navigate to the Apache Foundation's Apache2 Documentation.

4. In the **VirtualHost** section of the file please add these directives if they do not exist. It is best to comment out what is already there and add the below entries.
   - **SSLEngine** on
   - **SSLCertificateKeyFile** /etc/ssl/ssl.key/server.key
   - **SSLCertificateFile** /etc/ssl/ssl.crt/yourDomainName.crt
   - **SSLCertificateChainFile** /etc/ssl/ssl.crt/yourDomainName.ca-bundle ***

   *** **Apache 1.x:**

   Please use **SSLCACertificateFile** instead of **SSLCertificateChainFile**.

Note: The above paths in the directives are only used as examples. Your server may have a different path and may need to be modified to suit your needs.

5. Save your **config** file and restart the Apache service.

APACHE SSL

Generate CSR

1. Firstly, install OpenSSL in your server.

2. Create a RSA key for your Apache server:
   If you have a different path, cd to your server's private key directory

3. Type the following command to generate a private key that is file encrypted. You will be prompted for the password to access the file and also when starting your webserver. Please remember your password because if you forgot to do so you have to purchase another certificate.
   openssl genrsa -des3 -out domainname.key 2048

   You may also create a private key without file encryption:
   openssl genrsa -out domainname.key 2048

   Note: You are recommended to name the private key using the domain name that you are purchasing the certificate such as ***domainname.key***

4. Next, type the following command to create a CSR with the RSA private key (output will be PEM format):
   openssl req -new -key domainname.key -out domainname.csr

   Note: You will be prompted for your PEM passphrase if you included the "-des3" switch in step 3.

5. Below are the conventions that you need to follow when creating a CSR. Enter the information to be displayed in the certificate. The following characters cannot be accepted: < > ~ ! @ # $ % ^ * / \ ( ) ?.,&

DN Field	Explanation	Example < /h4>
Common Name	The fully qualified domain name for your web server. This must be an exact match.	If you intend to secure the URL https://www.geotrust.com, then your CSR's common name must be www.geotrust.com.
Organization	The exact legal name of your organization. Do not abbreviate your organization name.	TABSB
Organization Unit	Section of the organization	CA
City or Locality	The city where your organization is legally located.	Old Klang Road
State or Province	The state or province where your organization is legally located. Cannot be abbreviated.	Kuala Lumpur
Country	The two-letter ISO abbreviation for your country.	MY

6. Do not enter extra attributes at the prompt.
   Warning: Leave the challenge password blank.

   Note: If you want to verify the contents of the CSR, please use the following command:
   openssl req -noout -text -in domainname.csr

7. Submit your CSR to TMCA.

8. Make sure that you do not forget your private key. If so, you need to purchase a new one.

9. Finally, to view the contents of the private key, please use the following command:
   openssl rsa -noout -text -in domainname.key

Installation

Apache v1.X

1. Download the appropriate Intermediate Certificate(s) and save it in a text editor as intermediate.pem:
   - DomainSSL / OrganizationSSL / ExtendedSSL: SSL Certificate Bundle

2. Copy your SSL Certificate out of the order fulfilment e-mail (or log into your GlobalSign Certificate Center account and download it) and paste it into a text editor and save as mydomain.pem.

3. Copy “mydomain.crt” and “intermediate.pem” to the directory in which you plan to store your certificates.

4. Open your httpd.conf file (some installations keep the SSL section separately in the ssl.conf file) using a text editor, and locate the virtual host section for the site for which the SSL Certificate will secure.

Your virtual host section will need to contain the following directives:

- **SSLCertificateChainFile** – This will need to point to the appropriate Intermediate root CA certificates.
- **SSLCertificateFile** – This will need to point to the end entity certificate (the one you have called “mydomain.crt”)
- **SSLCertificateKeyFile** – This will need to point to the private key file associated with your certificate.

5. Save the changes to the file and quit the text editor

6. Restart apache.

Apache 2.X

1. Download the appropriate GlobalSign root certificate and save it in a text editor as gs_root.pem:
   Note: The ExtendedSSL certificate uses the GlobalSign root CA RC2 Certificate.
   - DomainSSL and OrganisationSSL: GlobalSign Root CA
   - ExtendedSSL: GlobalSign Root CA RC2

2. Download the appropriate Intermediate Certificate(s) and save it in a text editor as intermediate.pem:
   - DomainSSL / OrganizationSSL / ExtendedSSL: SSL Certificate Bundle

3. Copy your SSL Certificate out of the order fulfilment e-mail (or log into your GlobalSign Certificate Center account and download it) and paste it into a text editor and save as mydomain.crt.

4. Copy “mydomain.crt” and “intermediate.pem” to the directory in which you plan to store your certificates.

5. Open your httpd.conf file (some installations keep the SSL section separately in the ssl.conf file) using a text editor and locate the the virtual host section for the site for which the SSL Certificate will secure.
   - Your virtual host section will need to contain the following directives:
   - **SSLCACertificateFile** – This will need to point to the appropriate GlobalSign root CA certificate.
   - **SSLCertificateChainFile** – This will need to point to the appropriate intermediate root CA certificates you previously created in Step 1 above.
   - **SSLCertificateFile** – This will need to point to the end entity certificate (the one you have called "mydomain.crt")
   - **SSLCertificateKeyFile** – This will need to point to the private key file associated with your certificate.

6. Save the changes to the file and quit the text editor

7. Restart apache.

IBM HTTP SERVER

Generate CSR

1. Firstly, create a new key database. Start the '**IKEYMAN**' software. You can choose either to run the command '**IKEYMAN**' or loading the GUI version.

2. Select '**Key Database File**' from the main menu and choose '**New**'.

3. Choose and enter a new Key Database name. Click '**OK**'.

4. Enter and confirm a password for the Key Database. Ensure that you always remember this password.

5. Now use the new Key Database to create a CSR. Start IKEYMAN again, select `**Key Database File**' and choose '**Open**'.

6. Then, enter the password from Step 4 and click **'OK**'.

7. Select '**Create**' from the main menu, and choose '**New Certificate Request**'.

8. A form will appear, and all the fields require completion. Click '**OK**' when completed. Notes on some of the fields are:
    - Key Label - simply a descriptive label for the CSR.
    - Keysize - we suggest the keysize be as large as possible, preferably 2048 bit.
    - Common Name - where you should enter the fully qualified domain name of the website you require the certificate for.
      Note: for wildcard certificates, the Common Name should be in the format: **.mydomain.com*
    - Country - the ISO-3166 two-letter country code for the country. 'US' for the USA, 'GB' for Great Britain 'MY' for Malaysia, etc.
    - Certificate Request Filename - the path and filename for the CSR.

9. Lastly, open the CSR file with a text-editor. Copy and paste the contents into the enrolment form when requested.

Installation

1. Start the 'IKEYMAN' software. You can choose either to run 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. Select the root certificate file, and click 'OK'.

7. Repeat Steps 5 & 6 with the intermediate.

8. Return to the main 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.

LOTUS NOTES DOMINO 6, 7 AND 8

Generate CSR

1. From the Notes client, open the Server Certificate Admin application on the server for which you want to enable SSL. From the main menu, select “Create Key Ring” option.

2. Enter the required field on the screen. Click “**Next**” to continue after each fields required through each interface is filled.

   Key Name - Enter the key ring file name. The default is KEYFILE.KYR.

   Key Size - should be the Fully Qualified Domain Name (FQDN) or the web address for which you plan to use your IIS SSL Certificate

   Key Password - Enter the password for the key ring.

   Common Name - should be the Fully Qualified Domain Name (FQDN) or the web address for which you plan to use your IIS SSL Certificate

   Organization Information

   Organization - The legally registered name of your organization/company. If your company or department has an &, @, or any other symbol using the shift key in its name, you must spell out the symbol or omit it to enroll, for example: XY & Z Corporation would be XYZ Corporation or XY and Z Corporation.

   Organizational unit - The name of your department within the organization
   Notes; You should enter in these fields what appears on your official company registration documents.
   Geographical details

   City/locality - The city in which your organization is located.

   State/province - The state in which your organization is located. Spell out the state completely; do not abbreviate the state or province name, for example: California.

   Country/region – Use the two-letter code without punctuation for country, for example: US or CA.
   Notes; select 2048 for the “Key Size”

3. Click **"Create Key Ring."** The information on the key ring created should be displayed afterward.

4. After you read the information about the key ring file and distinguished name, click “**OK”**. Lotus Notes creates the key ring file and stash (.STH) file and places them in the Lotus Notes data directory on the client machine used to create the key ring.

   Copy the key ring file and stash (.STH) file to the Domino data directory on the server.

5. Now that you have a Key Ring you can generate the Certificate Signing Request (CSR). Clicking “OK” returns you to the main menu. From the Lotus Notes client, open the “**Server Certificate Admin”** application on server for which you want to set up SSL. Select “**Create Certificate Request**” and provide the inputs as indicated.

   Key Name - Enter the key ring file name. The default is KEYFILE.KYR.

   Log Certificate Request
   -Choose one:
   “Yes” (default) to log information in the Server Certificate Admin application.
   “No” to not log information.

Method
-Choose one:
Paste into form on CA's site (recommended)
Send to CA by e-mail
Notes; you will be asked for the Key Ring password you entered above.

Click **"Create Certificate Request."**

6. Enter the password for the server key ring file.
Notes; If you selected **"Paste into form on CA's site"** in Step 4, do the following:
Copy the certificate request to the system Clipboard (include the Begin Certificate and End Certificate lines).

Use a browser to visit the CA's site, and then follow the instructions that the CA's site provides for submitting a request for a new certificate.

Installation

1. Copy the server program files onto the designated machine

2. Use the Domino server setup program to configure the server.

   Note Do not unpack installation kit files to the same directory to which you install the installation files. Specify a unique directory path for each set of installation files.

3. Name the server. Refer to the name that you created based on your company's structure.

4. Identify the function of the server -- for example, will it be a mail server or an application server? The function of the server determines which tasks to enable during configuration.

5. Locate the server physically and decide who administers it.

6. Decide whether the server is part of an existing Domino domain or is the first server in a new Domino domain.

7. If this is the first server in a Domino domain, do the following:
   a. Install the server program files.
   b. Use the Domino server setup program to set up the server.
   c. Complete network-related setup.
   d. Create organization certifier IDs and organizational unit certifier IDs as required by the hierarchical name scheme.
   e. Distribute certifier IDs to administrators.
   f. Implement Domino security.

8. If this server is part of an existing Domino domain, do the following:
   a. Use the Domino Administrator to register the server.
   b. Install the server program files on each additional server.
   c. Use the Domino server setup program to set up each additional server.

9. Perform additional configuration procedures, based on the type of services, tasks, and programs that you want to run on this server.

MICROSOFT IIS 6.0

Notes;
By far the most common problem users have when going through this process is related to private keys. If you lose or cannot access a private key, you cannot use the certificate we issue to you and will need to request a free reissue. This happen when you create a new CSR, or new Key for the same web site, you will overwrite the ones you used to request your certificate. If that happens, you cannot use the certificate we issue you and will need to request a reissue.

To ensure this never happens, we advise that a backup of the private key file is made and that a note is made of the password that is used to protect the export of the private key.
More on backup information is available on:
http://support.emerge.com.my/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=217

IIS Installation using Control Panel

During installation, IIS installs optional components like Common Files, Documentation, and the Internet Information Services snap-in. You can choose not to install the optional components; however, deselecting certain components can decrease IIS functionality or disable IIS services. Choose to install the IIs with the given default option if you are not familiar with the components. After you install IIS, you can view Installing IIS Optional Components in the IIS online documentation for more information.

1. Click **Start**, click **Control Panel**, and double-click click **Add or Remove Programs**.

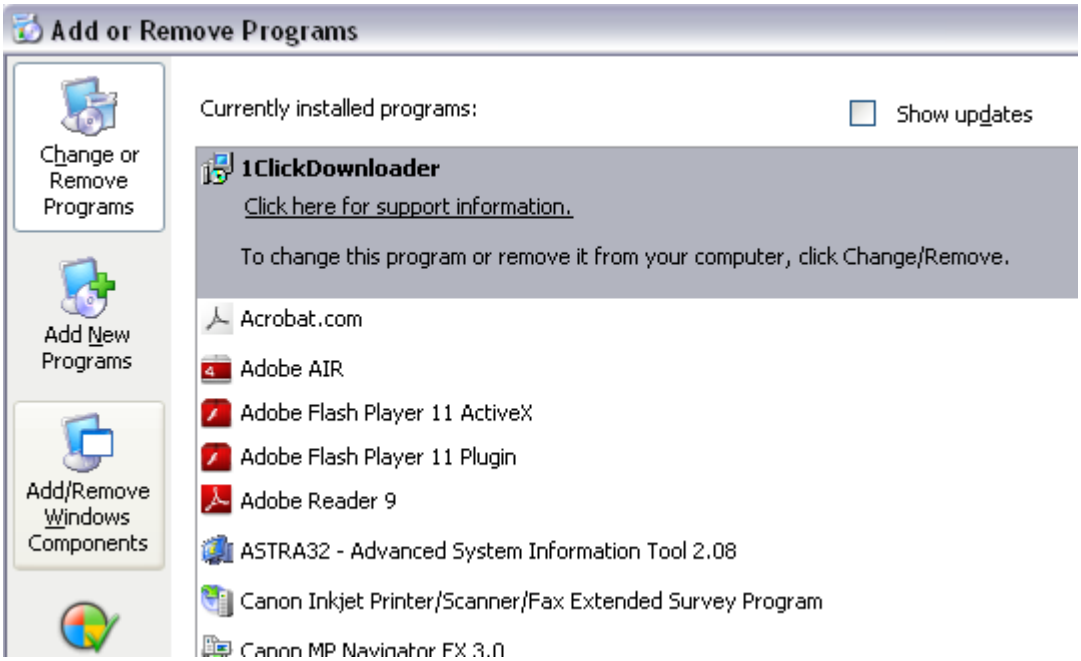
2. Click **Add/Remove Windows Components**. The Windows Components Wizard appears.

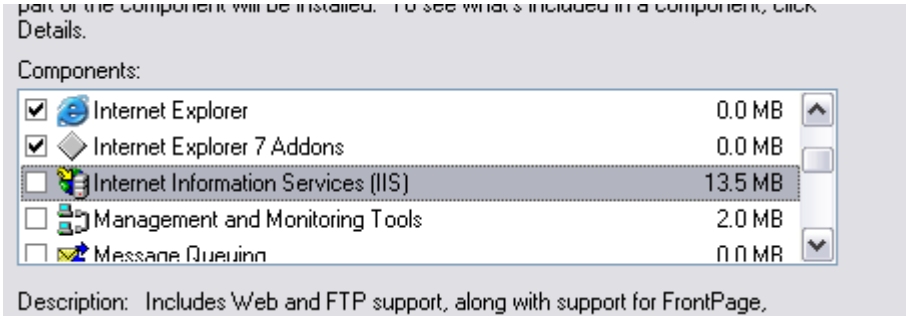
3. In the **Components** list box, click **Application Server**. Click **Details**.

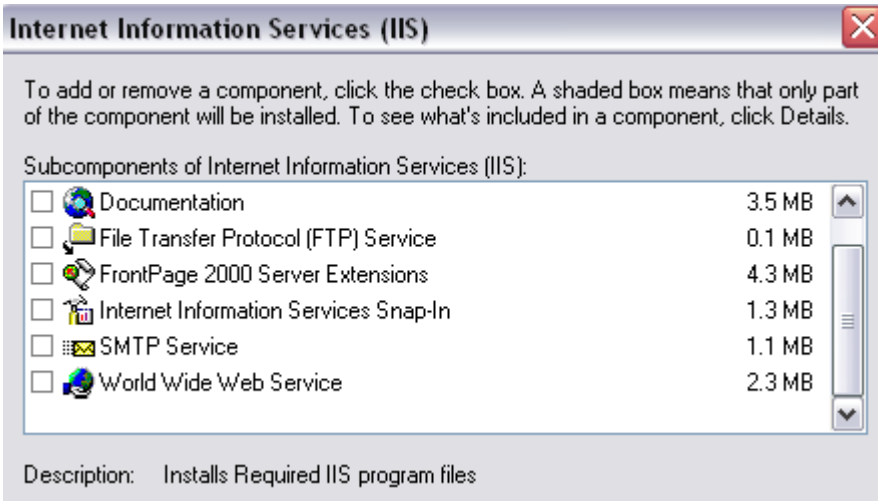
4. Click **Internet Information Services Manager**.
   Click **Details** to view the list of IIS optional components. For a detailed description of IIS optional components, see "Optional Components" in this topic.

5. Select (check) all optional components you wish to install.

6. Make sure the **World Wide Web Service** and **Internet Information Services Manager** are checked to be installed.
   Click **Next** and follow the on-screen instructions to install IIS component.







Generate CSR

1. Under **Administrative Tools (**category view: click **Performance and Maintenance**), open the **Internet Services Manager**. Then open up the properties window for the website you wish to request the certificate for. Right-clicking on the particular website will open up its properties.

2. Click the **Directory Security** tab and then click on the "**Server Certificate**" button in the **Secure**

communications section. This will start the **Web Site Certificate Wizard**.

3. Select "**Create a new certificate**" option.

4. Select the "**Prepare the request now, but send it later**" option from the list. You will need to prepare the request now but will only submit the request (CSR) via our online request forms. We do not accept CSR's via email.

5. Enter a certificate name and the certificate strength. Click "**Next**". You have now created a public/private key pair.

   Notes; Do not check the option "Select cryptographic service provider (CSP) for this certificate" option.

6. Next is to create a Certificate Signing Request (CSR). This information will be displayed on your certificate, and identifies the owner of the key to users. The CSR is only used to request the certificate. Certain characters must be excluded from your CSR fields, or your certificate may not work.

   Enter the required field following the on-screen instructions. Click "**Next**" after each fields required through each interface is filled.

   Common Name - The name through which the certificate will be accessed. Enter your exact host and domain name that you wish to secure.

   Organization Information

   Organization - The legally registered name of your organization/company.

   Organizational unit - The name of your department within the organization
   Notes; You should enter in these fields what appears on your official company registration documents.
   Geographical details

   City/locality - The city in which your organization is located.

   State/province - The state in which your organization is located
   .
   Country/region – MY (Malaysia).

6. Choose a filename to save the request.
   Enter the file name for the certificate request (CSR) and the location of where you would like to save the file. (you can browse for file location). Click "**Next**".

7. Confirm your request details. A summary of the certificate request will be available on the interface. Click "**Next**".

8. Click "**Finish**" to complete the "**Web Server Certificate wizard**" and exit the IIS Certificate Wizard.

9. Backup your private key.

Installation

1. Under "**Administrative Tools"** (category view: click **Performance and Maintenance**), open the "**Internet Services Manager"**. Go back on the website where you generated your certificate request (generally the Default Web Site) and open the properties window. To do so, right click on the website and select "**Properties**" in the menu.

2. Go to the "**Directory Security tab**". Click on the "**Server Certificate"** button. This will start the certificate wizard. Click "**Next"**.

3. Select "**Process the pending request" and install the certificate** and click "**Next**".

4. Click "**Browse"** and find the SSL certificate file that you download from your certificate authority. If the file type is not a .cer, make sure to view all file types. Click "**Next**".

   Finish the rest of the wizard.

MICROSOFT IIS 7.0

Generate CSR

1. Under **Administrative Tools (**category view: click **Performance and Maintenance**), open the **Internet Services Manager**. In the IIS Manager, choose your server name. a pane displaying on the options available for the server will be displayed on the features pane.

2. In the **"Features"** pane (the middle pane), double-click the **"Server Certificates"** option located under the Security heading.

   Notes; two default certificate is defined for the chosen server.

3. In the "**Action**" pane, choose the "**Create Certificate Request**" option to request to create a new certificate.

4. Enter the required field on the screen. Click "**Next**" to continue after each fields required through each interface is filled.

   Common Name - should be the Fully Qualified Domain Name (FQDN) or the web address for which you plan to use your IIS SSL Certificate

   Organization Information

   Organization - The legally registered name of your organization/company.

   Organizational unit - The name of your department within the organization
   Notes; You should enter in these fields what appears on your official company registration documents.
   Geographical details

   City/locality - The city in which your organization is located.

   State/province - The state in which your organization is located.

   Country/region – MY (Malaysia).

5. Next is to choose on the cryptographic service provider and the bit length.

   On the "**Cryptographic Service Provider Properties"** list**,** select either "**Microsoft RSA SChannel Cryptographic Provider"** or "**Microsoft DH SChannel Cryptographic Provider"** from the drop-down list. By default, IIS 7 uses the "**Microsoft RSA SChannel Cryptographic Provider"**.

   On the "**Bit length"** drop-down list, select a bit length that can be used by the provider. By default, the **RSA**

SChannel provider uses a bit length of 1024. The **DH SChannel** provider uses a bit length of 512. A longer bit length is more secure, but it can affect performance.

Click Next to continue.

6. Choose a filename to save your CSR.

   Enter the file name for the certificate request (CSR) and the location of where you would like to save the file. (you can browse for file location). Click "**Next**".

   You will need this CSR to enroll for your IIS SSL Certificate so make sure you know where to find it.
   Click "**Finish**" to complete.

Installation

1. Under **Administrative Tools (**category view: click **Performance and Maintenance**), open the **Internet Services Manager**. In the IIS Manager, choose your server name. A pane displaying on the options available for the server will be displayed on the features pane.

2. In the **"Features"** pane (the middle pane), double-click the **"Server Certificates"** option located under the Security heading.

3. In the "**Action**" pane, choose the "**Complete Certificate Request**" option. This will open the Complete Certificate Request wizard.

4. Click the button to browse and select the server certificate that you received from the certificate authority. If the certificate doesn't have a .cer file extension, select to view all types. Enter any friendly name you want so you can keep track of the certificate on this server.
   Click "**OK"**.

   Notes; If successful, you will see your newly installed certificate in the list. If you receive an error stating that the request or private key cannot be found, make sure you are using the correct certificate and that you are installing it to the same server that you generated the CSR on. If you are sure of those two things, you may just need to create a new Certificate Request and reissue/replace the certificate. Contact your certificate authority if you have problems with this.

Binding the certificate to Website

1. From the "Connections" menu in the main Internet Information Services (IIS) Manager window, expand the sites folder and click on the website that you want to bind the certificate to.

2. Under "Sites", select the site to be secured with SSL.

3. In the "**Action**" pane, right click on "Bindings".
   The "Site Bindings" window will open.

4. Click on the **Add...** button.

5. Change the Type to **https**. The IP address should be the IP address of the site or All Unassigned, and the port over which traffic will be secured by SSL is usually 443.and then select the SSL certificate that you just installed. Click **OK**.
6. Restart the IIS to complete the operation.

TOMCAT

Generate CSR

Key Generation for Tomcat and SSL Web Server Certificate installation

Step 1: Create a Keystore and Private Key

1. Create a certificate keystore and private key by executing the following command:
   keytool -genkey -keyalg RSA -alias tomcat -keysize 2048 -keystore [keystore name]

2. This command will prompt for the following attributes of the certificate:

   Enter keystore password: Specify a password (must be at least 6 characters long) and enter it when promted to do so.

   Your first and last name: First name and last name must match exactly with the URL or domain name you plan to secure (e.g. www.mydomain.com)

   Name of your organizational unit: The name of your department within the organization (e.g. TAB IT)

   Name of your organization: The legal (officially registered) name of your organization/company (e.g. TABSB)

   Name of your city and locality: The city or town in which your organization is located (e.g. Taman Desa)

   Name of your state and province: The state in which your organization is located (e.g. Wilayah Persekutuan)

   T**he two-letter country code for this unit:** Enter official country codes for this field (e.g. MY)
   Is CN=www.mydomain.com, OU=TAB IT, O=TABSB, L=Taman Desa, ST=Wilayah Persekutuan, C=MY correct?: If the information is correct, type "Yes", otherwise "No"

   Enter key password for <tomcat>(RETURN if same as keystore password): Enter the keystore password (e.g. pswd)

   ****NOTE****
   Be sure to remember and specify the same password for the keystore and the keyEntry or else you will the following error message will occur when you restart the jakarta engine:
   java.security.UnrecoverableKeyException: Cannot recover key

   Noted that keystore was created.

   Please run the following: **keytool -list -keystore [keystorename]** to make sure the keystore file can be read.

   The keystore will be stored in your JDK/bin directory. Create a copy of the keystore file and store it on a removable disk for safe keeping in case of a server crash.

Step 2: Backup Keystore file

To backup the keystore file with the keyentry just created, please refer to the following solution: vs23585

Step 3: Create a CSR file with your newly created keystore

1. Create the Certificate Signing Request file with the following command:
   keytool -certreq -alias tomcat -keyalg RSA -file certreq.csr -keystore [keystorename]
   Enter keystore password: pswd

2. The CSR will be saved to your JDK/bin directory and can be entered into the website. Please include these tags:

   -----BEGIN NEW CERTIFICATE REQUEST-----

   -----END NEW CERTIFICATE REQUEST-----

Step 4: Submit the CSR

Please submit your CSR in our online TMCA enrollment process and fax the necessary documentation to your TMCA Representative.

****NOTE****
The above steps provides general instructions for key generating SSL Certificates. If you have any problem or encounter error regarding your server during the generation process, TABSB recommends that you contact either the vendor of your software or an organization that support Tomcat.

Installation

1. Install the root certificate file by executing the following command:
   keytool -import -trustcacerts -alias Digicert -file Digicert-class2.cer -keystore your_site_name.jks

2. Next, install the intermediate certificate file by executing the following command:
   keytool -import -trustcacerts -alias Digisign-2048 -file digisign-2048.cer -keystore your_site_name.jks

3. Install your server certificate file to your keystore executing the following command:
   keytool -import -trustcacerts -alias tomcat -file your_site_name.cer -keystore your_site_name.jks

If successful, a confirmation stating that the "**Certificate reply was installed in keystore**" can be seen.

If it asks if you want to trust the certificate, choose **y** or **yes**.

Your keystore file (your_site_name.jks) is now ready to use on your Tomcat Server and you just need to configure your server to use the keystore file.

Configuring your SSL Connector

Tomcat will first need a SSL Connector configured before it can accept secure connections.
By default Tomcat looks for your Keystore with the file name .keystore in the home directory with the default password "changeit". The home directory is generally /home/user_name/ on Unix and Linux systems, and C:\Documents and Settings\user_name\ on Microsoft Windows systems. You will be able to change the password and file location.

1. Open the Tomcat server.xml file in a text editor (this is usually located in the conf folder of your Tomcat's home directory).

2. Find the connector that will be secured with the new keystore and Uncomment the SSL Connector Configuration. Make sure that the Connector Port is 443 or 8443 like the example below

3. Specify the correct keystore filename and password in your connector configuration. When you are done your connector should look something like this:

<Connector **port="443"** maxHttpHeaderSize="8192" maxThreads="150" minSpareThreads="25" maxSpareThreads="75" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true" **SSLEnabled="true"** clientAuth="false" sslProtocol="TLS"**keyAlias="server" keystoreFile="/home/user_name/your_site_name.jks" keypass="your_keystore_password"** />

4. Save the changes to server.xml

5. Restart Tomcat

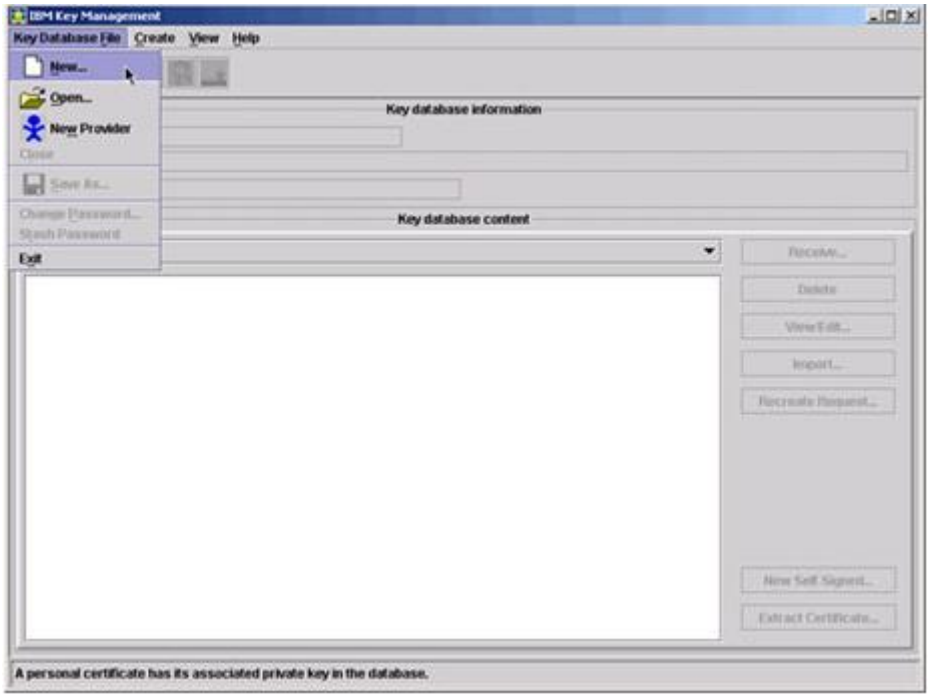
WEBSPHERE

Generate CSR

NOTE
The following instructions are for IBM Websphere 6.0x. The following steps can be used by using the older versions of Websphere but there are some small interface differences.

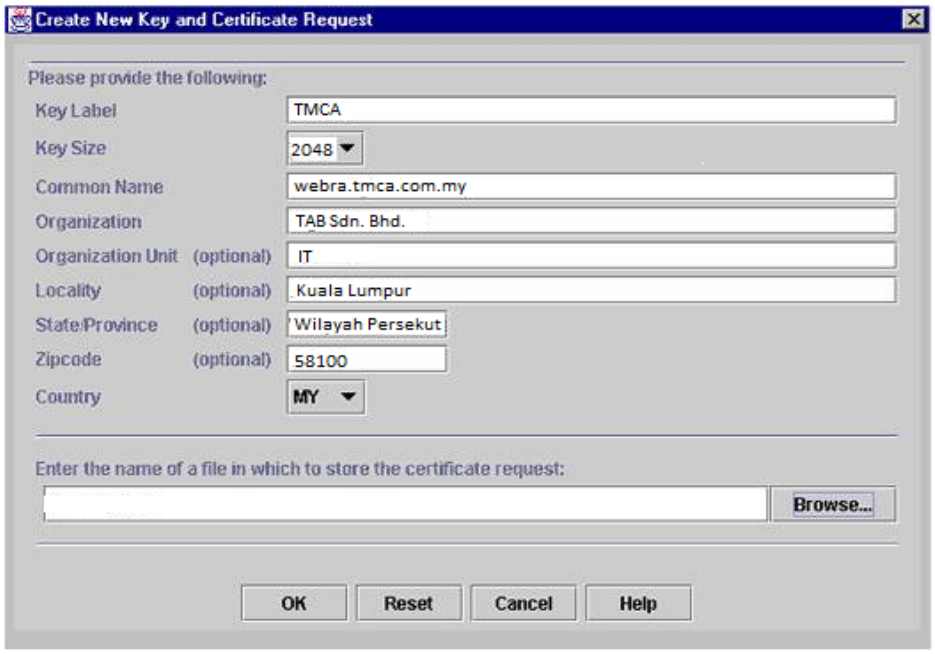
The first step is to create a **keystore**, a file that contains the certificates and private key. You will create the keystore with IBM's Key Management Utility, which comes installed with WebSphere:

1. Start the Key Management Utility (iKeyman).



2. In the IBM Key Management Utility, click on **Key Database File** and then **New**.
3. Choose **Key database** type and select **JKS**. Give the keystore a name such as your_domain.jks.
4. Click the **Browse** button. Go to C:\Program Files\IBM\WebSphere\AppServer\profiles\default\etc or to a different location where you want to store your keystore file.

5. Click **OK**. Enter a password and click **OK**.
6. Click **Create** then **New Certificate Request** to bring up the Create New Key and Certificate Request dialog.
7. Type a **Key Label**, **Common Name**, **Organization**, **Locality**, **State**, and select a **Country**. Select 2048 for **Key Size.** For common name enter the fully qualified domain name for the site you are securing (e.g. www.yourdomain.com).



Browse for a location and enter a name for the file such as your_domain.csr and click **OK**.

Installation

Installing the Intermediate and Root Certificates

1. Enter IKEYMAN in UNIX from the command prompt. In Windows, start the Key Management utility in the IBM HTTP Server folder.

2. In the main User Interface, choose Key Database File. Choose Open.

3. Select your key database and click on **OK**.

4. Next, enter your password and click **OK**.

5. Click on the link to Signer Certificates in the Key Database content frame. Click the Add button.

6. Choose the certificate you are adding (or browse to find the certificate), then select OK. Begin with the Class2root.cer. If you get a message that this file is already installed, select to continue.

7. Next, go ahead and upload the TMCA Server ID 2048.cer file in the same manner in which you installed the TrustedRoot.

Installing your Primary Server SSL Certificate (your_domain_name.cer)

1. In IKEYMAN, in your Key Database, click on Personal Certificates, then the "**Receive"** button.
2. Choose your DigiCert SSL Certificate (your_domain_name.cer) from the Receive Certificate from File Box. Then click on **OK**.

For further assistance, check with IBM as they have a helpful guide for SSL installation.
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/csec_ssl.html

WEBLOGIC

Generate CSR

CSR Creation With Java Keytool for WebLogic Servers

****NOTE****
We recommend that you generate a new keystore before creating your CSR to avoid errors during installation. This is even the case when reissuing or renewing your certificate.

Create a Keystore file

1. Using keytool, enter the following:
   keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore your_domain.jks
   'your_domain' in the command above should be the name of the domain you are securing.

2. Some information are prompted to be filled for your certificate.
   Please note: When prompted for the first and last name, DO NOT enter your first and last name. Instead, enter the name to which the certificate is being issued (e.g., www.yourdomain.com, mail.yourdomain.com, *.yourdomain.com)

3. When prompted, enter 'y' or 'yes' to confirm. You will next be asked for a password. You will need to use this same password when generating a CSR and importing your certificates.

Generate a CSR from your new keystore

1. Use keytool to create a Certificate Signing Request from your keystore:
   keytool -certreq -alias server -keyalg RSA -file your_domain.csr -keystore your_domain.jks

   Again, 'your_domain' is the name of the domain you are securing. (without the * character if you are ordering a Wildcard Certificate).

2. Enter the keystore password.

3. Your CSR file should now have been created.

Installation

WebLogic 8 and 9 SSL Certificate Installation

1. To install the root certificate file, you must execute the following command first to your keystore:
   keytool -import -trustcacerts -alias Digicert -file Digicert-class2.cer -keystore your_site_name.jk

2. Next, type the following command to install the intermediate certificate file to your keystore:
   keytool -import -trustcacerts -alias Digisign-2048 -file digisign-2048.cer -keystore your_site_name.jk

3. Type the following command to install your server certificate file to your keystore:
   keytool -import -trustcacerts -alias server -file your_site_name.cer -keystore your_site_name.jks

If successful, a confirmation stating that the "**Certificate reply was installed in keystore**" can be seen.

If it asks if you want to trust the certificate, choose **y** or **yes**.

Your keystore file (your_site_name.jks) is now ready to use on your Tomcat Server and you just need to configure your server to use the keystore file.

Configuring the Keystore for use in WebLogic

1. On your WebLogic server, expand the "Servers" node and choose the server you will be configuring.

2. Next, go to Configuration-->Keystores and SSL.
   Several default keystores or previously installed keystores may be displayed under "Keystore Configuration."

3. To enable your new keystore, click the "Change..." link under "Keystore Configuration."

4. Choose "Custom Identity and Java Standard Trust" as your keystore configuration type, then click Continue.

5. Under "Custom Identity Keystore File Name" enter the full path to the your_domain.jks file on your server.

6. "Custom Identity Keystore Type" select jks.

7. The "Custom Identity Keystore PassPhrase" should be the password you specified when the keystore was created.

   If you have forgotten that password, you will need to begin the process of creating your keystore from the beginning.

8. You will again be asked to enter your keystore password and confirm.

9. Click Continue, and then Finish.

10. You will now need to go back under the "Servers" node and select the server you are configuring.

11. Next, go to Configuration-->Keystores and SSL, then click the "Change..." link under "Keystore Configuration."

12. In the Configure SSL page, choose "Key Stores" as the method in which identity and trust is stored for the WebLogic server.

13. Specify the "Private Key Alias" and "Passphrase" that were used when creating your keystore. If you followed our instructions or used our command generator, "server" is your alias. The passphrase is the keystore password.

14. Click Continue, then Finish.

Reboot the WebLogic server. Your keystore should now be installed and enabled.