Contents

C2Net Stronghold

1. Open the Stronghold Configuration Manager.
2. Click **New Key Generation**.
3. Enter the key size (2048 bits) and follow the instructions for generating the random data.

   Note: *Do not use these characters: < > ~ ! @ # $ % ^ * / ( ) ?. &*

   The new key pair is located in:strongholdserverroot/private/your_domain_name.key. Where your_domain_name is the domain name and extension that you are securing (For example: yourcompany.com)

4. Open the file in a text editor. Copy the text, including the BEGIN and END tags.
5. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**
6. Paste the text from the CSR file into the field provided.

Cisco Adaptive Security Appliance (ASA) 5500

1. Open the Cisco Adaptive Security Device Manager (ASDM) and click **Configuration** > **Device Management**.
2. Expand **Certificate Management** and then click **Identity Certificates** > **Add**.
3. Select **Add a new identity certificate** and click **New** next to the **Key Pair** list.
4. Select **Enter new key pair name** and enter a name for the key pair. Set the **Size** to 2048 and set the **Usage** to General purpose.
5. Click **Generate Now**.
6. Click the **Select** button to the right of the **Certificate Subject DN** field. In the Certificate Subject DN window, configure the following DN attributes by selecting the attribute type from the **Attribute** list, entering an appropriate **Value**, and clicking **Add**:

    - **Common Name (CN):** Fully-qualified domain name (FQDN) for which you are requesting the SSL certificate. If you are generating a CSR for a wildcard certificate, the common name must begin with * (for example, *.yourcompany.com).
    - **Department (OU):** Branch of your company that is requesting the SSL certificate, such as “Finance”.
    - **Company Name (O):** Full legal name of your company.
    - **Country (C):** Two-letter ISO 3166 country code. For example, the code for the Japan is “JP”. For other countries, see the ISO list of country codes.
    - **State (St):** Full name of the state or province where your company is headquartered, such as “California”.
    - **Location (L):** Full name of the locality or city where your company is headquartered, such as “Los Angeles”.

    Note: *Each of the DN attributes has a 64-character limit.*

7. In the Add Identity Certificate window, click **Advanced**.
8. In the **FQDN** field, enter the fully-qualified domain name through which the device will be accessed externally (for example, vpn.domain.com).
   This value should match the Common Name specified in step 6.
9. Click **OK** and then **Add Certificate**.
   When prompted, save the CSR information as a .txt file.
10. Open the file in a text editor. Copy the text, including the BEGIN and END tags.
11. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

Cobalt RaQ4/XTR

To enable SSL on a virtual site:

Before creating the CSR, you must enable SSL on a virtual site.

1. Go to the Server Management screen.
2. Click the green wrench (RaQ4) or pencil (XTR) button next to the virtual site where you want to enable SSL. This displays the Site Management UI.
3. On the left side, click **Site Settings** (or **General**, if you are using XTR).
4. Select the **Enable SSL** option.
5. Click **Save Changes**.

To create a self-signed SSL certificate and submit the CSR:

After you have enabled SSL, generate a self-signed SSL certificate. The certificate will later be signed by AffirmTrust.

1. Go to the Server Management screen.
2. Click the green wrench (RaQ4) or pencil (XTR) button next to the virtual site where you want to enable SSL. This displays the Site Management UI.
3. On the left side, click **Site Settings** (or **General**, if you are using XTR).
4. In the Certificate Subject Information table, enter this information.

    - **Country:** Two-letter ISO 3166 country code. For example, the code for the Japan is “JP”. For other countries, see the ISO list of country codes.
    - **State:** Full name of the state or province where your company is headquartered, such as “California”.
    - **Locality:** Full name of the locality or city where your company is headquartered, such as “Los Angeles”.
    - **Organization:** Full legal name of your company.

5. In the list at the bottom of the screen, select **Generate self-signed certificate**.
6. Click **Save Changes**. The screen refreshes and displays your self-signed certificate in the **Certificate Request** and **Certificate** boxes.
7. Copy the contents of the **Certificate Request** box, including the BEGIN and END tags.
8. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

F5 BIG IP (version 9)

1. Launch the F5 BIG IP web UI.
2. Click **Local Traffic** > **SSL Certificates** > **Create**.
3. Under **General Properties**, specify a name for the certificate.
4. Under **Certificate Properties**, specify the following information:
    - **Issuer:** Certificate Authority (Trend Micro SSL)
    - **Common name:** Fully-qualified domain name of the server (for example, www.domain.com, mail.domain.com, or *.domain.com)
    - **Division:** Your department
    - **Organization:** The full legal name of your organization
    - **Locality, State or Province, Country:** City, state, and country where your organization is located
    - **E-mail Address:** Your email address
    - **Challenge Password, Confirm Password:** Your password
5. Set **Key Properties** to 2048.
6. Click **Finished**. You should be provided with the text of the CSR file. Copy the text, including the BEGIN and END tags.
7. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

F5 BIG IP (pre-version 9)

1. Log in to your BIG IP device as the root user and run this command:

   ```
   # /usr/local/bin/genconf
   ```

   You will be prompted to enter your company details, including the full legal company name and address.

2. Use the following command to create the CSR:

   ```
   # /usr/local/bin/genkey www.yoursite.com
   ```

   where www.yoursite.com is the fully qualified domain name of the site that you are securing.

3. When prompted, enter your company details.
4. Find the CSR file (www.yoursite.com.csr) located under /config/bigconfig/ssl.csr/. Transfer this file to a workstation and open it in a text editor. Copy the text, including the BEGIN and END tags.
5. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

F5 FirePass VPS

1. Log in to the FirePass web administration console.
2. In the Administration Console, click **Server** > **Security** > **Certificates**.
3. Click **Generate a New Certificate Request**.
4. Enter your company information in the CSR generation area and click **Generate Request**.
5. When you download the CSR, it is a ZIP file that contains both the CSR file and the private key. Save the private key in a secure location you will need it later to install your certificate.
6. Open your CSR file in a text editor. Copy the text, including the BEGIN and END tags.
7. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

HSphere Web Server

1. On the control panel home page, click **SSL** and then enable SSL for the domain you are securing.
2. Go to the next page, “SSL Certificate Signing Request Parameters”. Fill in any blanks and click **Submit**. Three files are generated: a CSR, a private key, and a temporary SSL certificate.
3. Save the private key and CSR and store them as text files in a safe place. You will need them to install your SSL certificates.
4. Open the CSR file in a text editor. Copy the text, including the BEGIN and END tags.
5. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

IBM HTTP Server

1. Open IKEYMAN to create a key pair and certificate request in the Key Database. You can make a new database for each key and request, or store them all in one database.
2. To create a new database, start IKEYMAN, select **Key Database File**, click **New**, and then enter your new database name.
3. Click **OK**. Enter and confirm your password, and then click **OK**.
4. To create the new key pair and CSR, open your database name in IKEYMAN.
5. Click **Create** and then **New Certificate Request**. Enter the information in the form. For key size, use the largest size available, ideally 2048-bit. Click **OK**.
6. Open the CSR file in a text editor. Copy the text, including the BEGIN and END tags.
7. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

Java-based web server (generic)

1. Back up and remove any old keystores from your Java-based web server. The CSR creation procedure requires that you generate a new keystore because your new SSL certificate will not function properly in an old keystore.
2. Create a new keystore. At a command prompt, enter:

   ```
   keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore
   your_domain_name.jks
   ```

   where your_domain_name is the name of the domain that you are securing. If you are requesting a wildcard certificate, do not include * at the beginning of the filename because it is not a valid filename character.

   - When prompted, enter your DN information. Set the first and last name to your domain name and extension (for example, www.yourcompany.com). If you are requesting a wildcard certificate, it must begin with * (for example, *.yourcompany.com)
   - When prompted, confirm that your information is correct and enter yes.
   - When prompted, confirm your password.

3. Generate a CSR with your new keystore. At a command prompt, enter:

   ```
   keytool -certreq -alias server -keyalg RSA -file your_domain.csr -
   keystore your_domain_name.jks
   ```

   where your_domain_name is the name of the domain that you are securing.

   When prompted, enter the keystore password that you specified when you created the keystore. The CSR file is created.

4. Using a text editor, open the CSR. Copy the text, including the BEGIN and END tags.
5. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

Lotus Domino 8.5

1. On the Server Certificate Admin page, click **Create Key Ring**.
2. Fill in the form. Set the Key Size to 2048.
3. Continue to the next page. You will get a confirmation that the key ring was created.
4. Click **OK** to return to the main page. Click **Create Certificate Request**.
5. Select **Paste into form on CA's site** and click **Create Certificate Request**.
   You will be presented with a confirmation screen that displays the CSR field properties and the text of the CSR.
6. Copy the certificate request (including the BEGIN and END tags) and click **OK**.
7. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

Mirapoint

1. On the Admin screen, click **Security and Certificates**.
2. Select **(CSR)**.
3. Enter the details that will appear in your SSL certificate, including the common name you want to secure (Example: www.yourdomain.com).
4. Click **Download** and save the file as a text file.
5. Open the CSR file in a text editor and copy the text, including the BEGIN and END tags.
6. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

Nginx

1. Use the terminal client (ssh) to log in to your server. At the prompt, enter the following command:

   ```
   openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
   ```

   where server is the name of your server.

   Two files will be generated: the CSR file and a private key file for the decryption of your SSL certificate.

2. Save the private .key file because you will need it when you install the SSL certificate.
3. When you are prompted for the Common Name (domain name), enter the fully qualified domain name for the site you are securing. If you are generating wildcard certificate, the common name must start with an asterisk (for example, *.yourcompany.com).
   You will then be prompted for your organizational information and your CSR file will be created.
4. Open the CSR file in a text editor and copy the text, including the BEGIN and END tags.
5. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.
6. Save the private .key file because you will need it when you install the SSL certificate.

Oracle Wallet Manager

1. In Oracle Wallet Manager click **Operations** in the menu. Select **Create Certificate Request** to open the Create Certificate dialog box.
2. Enter the following information in the required fields:

    - **Common Name:** Enter the fully qualified domain name that you need to secure (www.yourdomain.com).
    - **Organization:** Enter the full legal name of your organization.
    - **Locality/City:** Enter the city or locality where your organization is located.
    - **State/Province:** Enter the state or province where your organization is located.
    - **Country:** Select the country where your organization is located.
    - **Key Size:** Select a key size to use when creating the public/private key pair. 2048 is recommended.
    - **Advanced:** Do not make any changes to the Advanced settings.

3. Click **OK**. A dialog box will tell you that a certificate request was created successfully. Click **OK** again to return to the main window.
4. In Oracle Wallet Manager, click **Operations** in the menu. Select **Export Certificate Request**.
5. Enter the directory where you want to save the CSR. Enter a file name in the **Enter File Name** box.
6. Click **OK**.
7. Open the CSR file in a text editor and copy the text, including the BEGIN and END tags.
8. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

Oracle WebLogic Server 8 or 9

To create a keystore:

To avoid errors during installation, generate a new keystore before creating your CSR. You should generate a new keystore even when reissuing or renewing your certificate.

1. At a command prompt, enter this command:

   ```
   keytool -genkey -alias server -keyalg RSA -keystore
   your_domain_name.jks
   ```

   where *your_domain_name* is the name of the domain you are securing. If you are requesting a wildcard certificate, omit the * in the filename because it is not a valid filename character.

2. When prompted, enter the information for your certificate.

   Note: *Set the first and last name to the name to which the certificate is being issued (for example, www.yourdomain.com, mail.yourdomain.com, *.yourdomain.com).*

3. When prompted, enter “yes” to confirm. Next, you will be asked for a password. You will need to use this password later, when generating a CSR and importing your certificates.

To create a CSR:

1. At a command prompt, enter the following command:

   ```
   keytool -certreq -alias server -keyalg RSA -file your_domain.csr
   -keystore your_domain_name.jks
   ```

   where *your_domain_name* is the name of the domain you are securing. If you are requesting a wildcard certificate, omit the * in the filename because it is not a valid filename character.

2. Enter the keystore password.
3. Open the your_domain_name.csr file in a text editor and copy the text, including the BEGIN and END tags.
4. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

Plesk 10

1. Log in to the Plesk Control Panel.
2. Click **Tools & Utilities**. This option may be located on the **Server** tab or in the left column.
3. Click **SSL Certificates**.
4. Click **Add SSL certificate**.
5. Fill in settings on the Add SSL Certificate page and click **Request**.

   Note: *All fields marked with * must be completed. Set* ***Bits*** *to 2048.*

   The CSR will be available from the certificate list. Plesk will also email your CSR to the email address provided when you signed up.

6. Open the CSR file in a text editor and copy the text, including the BEGIN and END tags.
7. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

Plesk 9

1. Log in to the Plesk 9 Control Panel.
2. In the left menu, click **Settings**.
3. Under **Security**, click **SSL Certificate**.
4. In the SSL Certificates menu, click **SSL Certificate**.
5. Enter the relevant information in the certificate information (CSR) section and then click **Request**.
6. When returned to the **SSL Certificate** section, select the new certificate request

   name. The CSR is available from that screen.

7. Copy the text of the CSR, including the BEGIN and END tags.
8. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

Plesk 8

1. Log in to the Plesk Control Panel.
2. Clicking the **Domains** button. The Domain List page appears.
3. Click the domain name that you want to secure with SSL.
4. Click the **Certificate** button.
5. Click the **Add** button. The SSL Certificate setup page appears.

6. Enter the relevant information in the **Certificate Information** section.

   Note: *All fields marked with * must be completed. Set Bits to 2048.*

7. Click the **Request** button displayed to the right of your details.

   Plesk will email your CSR to the email address provided when you signed up. The email contains two sections: the private key and the CSR. Do not lose the private because you will need it later to install the certificate.

8. Open the CSR file in a text editor and copy the text, including the BEGIN and END tags.
9. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

SAP Web Application Server 6.10 or higher

You must generate an individual certificate request for each application server that uses a server-specific PSE. If you use a system-wide SSL server PSE, then you only need to generate a single certificate request.

To determine each unique SSL server PSE, expand the SSL server PSE node in the Trust Manager and double-click each application server to display details about the server. The server's Distinguished Name appears in the **Own certificate** field. You must generate a certificate request for each application server with a unique Distinguished Name.

1. On the Trust Manager screen, expand the SSL server PSE node.
2. Perform this procedure for each server-specific PSE or for a single system-wide PSE:

    a. Select the application server.
    The application server's certificate appears in the **PSE maintenance** section in the Own certificate field.
    b. In the **PSE maintenance** section, click **Create Certificate Request**.
    A dialog box displays the certificate request.
    c. Copy the certificate request, including the BEGIN and END tags.
    d. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.

Zeus Web Server

1. Log in to the web server.
2. Select **SSL Certificates**.
3. Click the **Create** button to create a new certificate set.
4. Select **Buy a certificate from another certifying authority** and click **OK**.
5. Fill in the appropriate fields with your DN information and then click **OK**.
6. Copy the CSR, including the BEGIN and END tags.
7. Open the AffirmTrust console and click **Certificates** > **Certificates** > **Add**. Paste the text from the CSR file into the field provided.