Contents

C2Net Stronghold

To install the server certificate:

1. If there is a temporary SSL certificate in your /ServerRoot/ssl/certs/ directory, move or delete it.
2. Run the following command:

```
getca your_domain_name
```

   Where your_domain_name is the same name you specified when creating the CSR

3. Open your server certificate in a text editor. Copy the text, including the BEGIN and END tags.
4. Paste the contents of your certificate into the getca terminal window and enter **Control-D** or the appropriate EOF character.

To install the CA certificate bundle certificates:

1. Copy the CA certificate bundle to your server in the /ssl/certs/ directory.
2. Using a text editor, open the httpd.conf file (typically located in the /conf/ directory).
3. Edit the SSLCACertificateFile entry so that it points to the CA certificate bundle file as follows:

```
SSLCACertificateFile ssl/certs/cabundle.crt
```

3. Restart your server.

Cisco Adaptive Security Appliance (ASA) 5500

To install the SSL certificate in the Adaptive Security Device Manager (ASDM):

1. Download your CA certificate bundle and server certificate files to the directory where you will store your certificate files.
2. In ADSM, click **Configuration** > **Device Management**.
3. Expand **Certificate Management** and select **CA Certificate**. Click **Add**.
4. Select the **Install from a file** option, browse to the CA certificate bundle file, and then click the **Install Certificate** button at the bottom of the Install Certificate window. Your intermediate certificates are now installed.
5. In ASDM, click **Configuration** > **Device Management**.
6. Expand **Certificate Management** and select **Identity Certificates**.
7. Select the appropriate identity certificate from when your CSR was generated and click the **Install** button.
8. Browse to the appropriate identity and click **Install Certificate**.
   Your certificate is now configured for use with the specified type of WebVPN session.

Cobalt RaQ4/XTR

To install the server certificate:

1. Go to the Server Management screen.
2. Click the green wrench (RaQ4) or pencil (XTR) button next to the site you are securing.
3. Click **SSL settings**.
4. Copy your server certificate (your_domain_name.crt), including the BEGIN and END tags, into the form.
5. In the list at the bottom of the screen, select **Use manually entered certificate** and then click **Save Changes**.

To install the CA certificate bundle:

1. Copy the CA certificate bundle file to your server.
2. Open your httpd.conf file and add this line to the SSL section:

```
SSLCACertificateFile /your_directory_path/cabundle.crt
```

3. Save the file, and then restart Apache.

F5 BIG IP (version 9)

To install the server certificate:

1. Launch the F5 BIG IP web UI.
2. Click **Local Traffic** > **SSL Certificates**.
3. Click the name you assigned to the certificate while creating the CSR.
4. Browse to the your_domain_name.crt file that you received from Trend Micro.
5. Click **Open** > **Import**.

   Your SSL Certificate file is now installed.

To enable your intermediate certificates:

1. Download the cabundle.crt file from the AffirmTrust console.
2. In the console, click **Local Traffic** > **SSL Certificates** > **Import**.
3. Click **Import Type** > **Certificate** > **Create New**.
4. Specify the certificate name.
5. Browse to the cabundle.crt file and click **Open** > **Import**.

To configure your server for SSL:

1. Create or open the SSL Profile that you will be using with this certificate.
2. In the SSL menu, log in to the Configuration Utility and click **Local Traffic** > **Profiles** > **Client**. Select the client to configure and on the **Configuration** menu, click **Advanced**.
3. Select the SSL certificate (public/private key pair) that you installed at the beginning of these instructions.
4. In the Chain section, browse to the certificate file that you imported in the previous step, then save and exit the configuration.

   Your SSL Certificate has now been installed and enabled for use on your server.

F5 BIG IP (pre-version 9)

1. Use FTP to move your server and intermediate certificates to the BIG-IP device.
2. Rename your server certificate from your_domain_name.crt to your.domain.name.crt and copy it to the /config/bigconfig/ssl.crt/ folder.
3. Copy the intermediate certificates to the /config/bigconfig/ssl.crt/ folder.
4. To restart the proxy, run the following commands:

   ```
   # bigpipe proxy <IP Address>:443 disable
   # bigpipe proxy <IP Address>:443 enable
   ```

   The certificates are now installed.

F5 FirePass VPS

1. In the Administration console, click **Server** > **Security** > **Certificates**.
2. Click **Install**.
3. Click **Add New Certificate** located near the bottom of the screen.
4. Copy and paste the certificate and key files into their corresponding fields.
5. Click **Go!** to install the certificate and key files.

HSphere Web Server

To install the server certificate:

1. Download your CA certificate bundle and server certificate files to the directory where you saved your certificate and key files.
2. On the control panel home page, click **SSL**.
3. In the W eb Service area, click the **Edit** button under **SSL**. An upload form opens.
4. In the box labeled **Install Certificate based on previously**, paste the contents of your server certificate file, including the BEGIN and END tags. You can open the certificate in a text editor.
5. Click **Upload**.

To install the CA certificate bundle:

Note: This is similar to the procedure for installing the server SSL certificate

1. Paste the contents of the CA certificate bundle file into the **Certificate Chain File** box. In some versions of HSphere, this box is labelled **Certificate Authority File**.
2. Click **Install**.
   Your certificates are now properly installed.
3. Keep backup copies of all your key and certificate files in a secure place. This enables you to easily re-secure your server if it crashes.
4. To test the secure connection, open a web browser and visit your site using https.
   You should not receive any browser errors or warnings. Test with both Internet Explorer and Firefox, because Firefox will display a warning if the Intermediate certificate is not installed. If you receive a browser message saying that the site is not available, the server may not yet be listening on port 443. If your web request times out, a firewall may be blocking traffic to the web server on TCP port 443.

IBM HTTP Server

To install the intermediate and root certificates:

1. Download the root and intermediate certificates, as well as your server certificate.
2. Do the following:

   UNIX: At the command prompt, enter “IKEYMAN”.
   Windows: Start the Key Management utility, located in the IBM HTTP Server folder.

3. In the main user interface, click **Key Database File,** and then **Open**.
4. Select your key database and click **OK**.
5. Enter your password and click **OK**.
6. In the Key Database pane, click **Signer Certificates** and then **Add**.
7. Browse to find the root certificate and click **OK**.
   If you get a message stating that this file is already installed, opt to continue. Repeat with the intermediate certificates.

To install your server certificate:

1. In IKEYMAN, in your Key Database, click **Personal Certificates** and then **Receive**.
2. In the Receive Certificate from a File dialog box, choose your server certificate and then click **OK**. Refer to documentation on the IBM web site for additional information on configuring SSL.

Java-based web server (generic)

1. Download your server certificate in .p7b format into the folder where the keystore (domain.jks) is located.

   Note: You must install the certificate to the same keystore that you used to generate the CSR.

2. At a command prompt, enter the following:

   ```
   keytool -import -trustcacerts -alias server -
   file your_domain_name.p7b -keystore filename.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 the certificate is installed correctly, you will receive a “Certificate reply was installed in keystore” message.

   If you are prompted whether you want to trust the certificate, enter “Yes”.

3. To configure your server to use SSL, refer to your web server’s documentation for instructions.

Lotus Domino 8.5

1. On the Server Certificate Admin page, click **Install Trusted Root Certificate into Key Ring**.
2. Click **Merge Trusted Root Certificate into Key Ring**. A summary of the certificate you are importing is displayed. Click **OK**.

   A confirmation of successful import is displayed.
3. Click **OK**.
4. Repeat this process for each certificate in the chain, in this order:

   - Root certificate
   - Intermediate certificates
   - Server certificate

5. Click **Install Certificate into Key Ring**.
6. Click **Merge Certificate into Key Ring**.

   You will get a confirmation of successful import.

To install the intermediate certificates:

1. Download the intermediate certificates and save them on your server.
2. From the Admin screen on your web server, click **Security** > **Certificates** > **Intermediate CA Certificate**.
3. Click **Browse** and locate one of the intermediate certificates that you saved to your server. Click **OK** and then **Install**. Repeat for the next certificate.

To install the server certificate:

1. Copy and paste the text of your server certificate and save it as a .crt file (for example, ssl_cert.crt).
2. From the Admin screen on your web server, click **Security** > **Certificates**.
3. Click **Browse**, locate the SSL certificate that you saved, and click **OK**.
4. Click **Install**. This installed the certificate on your web server.

To select SSL connections:

1. Click **Security** > **SSL**.
2. Use the check boxes to select which connections you want configure to use SSL and then click **Apply**.

To select the certificate interface:

1. From the Admin screen on your web server, click **Security** > **Certificates** > **Interfaces**.
2. In the **Interface** box, enter the interface on which you want to use the SSL certificate. This can a fully-qualified domain name (FQDN) or an IP address. If you leave it blank, the certificate will operate on the primary system interface.
3. Click **Set**.

Nginx

1. Download your server SSL certificate and the certificate bundle file to the Nginx server.
   Your Nginx server also has a key file that was created when you generated the certificate request.
2. Edit your Nginx configuration to reference certificate and key files.
   The exact configuration file you edit depends on your version of Nginx, your operating system, and the method used to install Nginx.

For more information on how to configure your Nginx server, refer to the following topic: Configuring HTTPS server.

Oracle Wallet Manager

1. Copy the SSL certificate that you received from AffirmTrust.
2. Open the Oracle Wallet Manager and go to the main panel.
3. In the menu bar, click **Operations** > **Import Trusted Certificate**. The Import Trusted Certificate dialog panel appears.
4. Choose **Paste the Certificate**, and click **OK**.
   Another Import Trusted Certificate dialog panel appears with the following message:

   Please provide a base64 format certificate and paste it below.

5. Paste the certificate into the window, and click **OK**.
   A message at the bottom of the window informs you that the trusted certificate was successfully installed.

6. Click **OK**.
   You are returned to the Oracle W allet Manager main panel, and the trusted certificate appears at the bottom of the **Trusted Certificates** tree.

Oracle WebLogic Server 8 or 9

To install your server certificate in WebLogic

This procedure loads all the necessary certificates to your keystore.

1. Download the your_domain_com.p7b certificate file from AffirmTrust.
2. Run this command to install the certificate to your keystore:

```
keytool -import -trustcacerts -alias server -file
      your_domain_com.p7b -keystore your_domain_name.jks
```

You should get a confirmation stating that the “Certificate reply was installed in keystore”.

If you are prompted to trust the certificate, choose “yes”. Next, you must configure your server to use the keystore.

To configure the keystore for use in WebLogic:

1. On your WebLogic server, expand the **Servers** node and choose the server you will be configuring.
2. Click **Configuration** > **Keystores and SSL**.

   Several default keystores or previously installed keystores may be displayed under **Keystore Configuration**.

3. To enable your new keystore, click **Change** under **Keystore Configuration**.
4. Choose **Custom Identity and Java Standard Trust** as your keystore configuration type, and then click **Continue**.
5. Under **Custom Identity Keystore File Name**, enter the full path to the your_domain_name.jks file on your server.
6. Set **Custom Identity Keystore Type** to jks.
7. Set **Custom Identity Keystore PassPhrase** to the password you specified when the keystore was created.

If you have forgotten the password, you will need to repeat the entire process, beginning with creating the keystore.

8. When prompted, re-enter your keystore password and confirm.
9. Click **Continue**, and then **Finish**.
10. Return to the **Servers** node and select the server you are configuring.
11. Click **Configuration** > **Keystores and SSL**, then click **Change** under **Keystore Configuration**.
12. On 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. The alias is “server” and the passphrase is the keystore password.
14. Click **Continue**, and then **Finish**.
15. Reboot the WebLogic server. Your keystore should now be installed and enabled.

Plesk 10

1. Download your server certificate, intermediate certificates, and the CA certificate bundle.
2. Log in to Parallels Plesk Panel.
3. On the **Hosting Services** menu, click **Domains**.
4. Next to the domain name you want to use, click **Open in Control Panel**.
5. Open the **Websites & Domains** tab and click **Secure Your Site with SSL Certificates**.
6. Under **Certificate name**, click the certificate you want to use.
7. Next to the **Certificate** field, click **Browse**.
8. Locate your server certificate file and click **Open**.
9. Next to the **CA certificate** field, click **Browse**.
10. Locate the certificate bundle file and click **Open**.
11. Click **Send File**.
12. If your server is running Linux, stop and start the Apache process. If your server is running Windows, stop and start the DNS service.

Plesk 9

1. Download your server certificate, intermediate certificates, and the CA certificate bundle.
2. Log in to Parallels Plesk Panel.
3. In the menu on the left, select **Domains**.
4. Click the domain name that the certificate is issued for.
5. Click the **Certificates** menu item.
6. Click **Browse** and locate your signed SSL certificate.
7. Select the certificate file and then click **Send File**.
8. Navigate to the location of your server SSL certificate. Select it, and then click **Send File.** This will upload and install the certificate against the corresponding private key.
9. On the list that is displayed, click the name of the certificate.
10. Open the certificate bundle file in a text editor and copy and paste its contents into the box labeled **CA Certificate**.
11. Click **Send Text**.
12. Click **Up Level** and then click **Up Level** again.
13. Select **Web Hosting Settings**.
14. At the top of the page, change the **SSL Certificate field** to the certificate you just installed and then click **OK**.
15. Click **Home** and then click **Service Management**.
16. If your server is running Linux, stop and start the Apache process. If your server is running Windows, start and stop the DNS service.

Plesk 8

1. Download your server certificate, intermediate certificates, and the CA certificate bundle.
2. Log in to Parallels Plesk Panel.
3. In the menu on the left, click **Domains**.
4. Click the domain name that the certificate is issued for.
5. Click the **SSL Certificates** menu item.
6. Click **Browse** and locate your server SSL certificate.
7. Select the certificate file, and then click **Send File**.
   This uploads and installs the certificate against the corresponding private key.
8. In the displayed list, click the name of the certificate.
9. Open the certificate bundle file in a text editor, copy its contents, and paste the contents the box labeled **CA Certificate**.
10. Click **Send Text**.
11. Click **Up Level** and then **Setup**.
12. At the top of the page, change the **SSL Certificate** drop-down menu to the certificate that you just installed.
13. In the menu on the left, click the **Server** item.
14. Click **Service Management**.
15. If your server is running Linux, stop and start the Apache process. If your server is running Windows, start and stop the DNS service.
    Note: *Restarting Apache will not work. Stop the service and start the service again to complete the installation.*

SAP Web Application Server 6.10 or higher

To install the server certificate:

1. On the Trust Manager screen, expand the SSL server PSE node.
2. Perform this procedure for each application server that will have a signed certificate:

    a. Double-click the appropriate application server to select it. The application server's SSL server PSE is displayed in the **PSE maintenance** section.
    b. In the **PSE maintenance** section, choose **Import Cert. Response**. A dialog box displays the certificate request. Copy the certificate request response.
    c. Paste the certificate request response into the dialog box's text box. The signed public-key certificate is imported into the server's SSL server PSE, which is displayed in the PSE maintenance section. You can double-click the certificate to view information about it.
    d. Save the data.

Next, you must import the CA's root certificates. The procedure varies depending on where the certificates are located.

To import root certificates that are located in the certificate database:

1. In the certificate section, click **Import certificate**.
2. The Import Certificate dialog appears. Select the **Database** tabstrip.
3. Select the certificate from the certificate database and choose **Enter**. The certificate appears in the certificate section.
4. Click **Add to Certificate List**. The certificate is added to the certificate list for the PSE displayed in the PSE maintenance section.
5. Save the data.

To import CA root certificates that are located in the file system:

1. In the certificate section, choose **Import certificate**. The Import Certificate dialog appears.

2. Enter the corresponding file name from the file system.
3. Select the certificate's file format (Base64).

   Choose **Enter.** The certificate appears in the certificate maintenance section.
4. Choose **Add to Certificate List**.

   The certificate is added to the certificate list for the PSE displayed in the PSE maintenance section.
5. Save the data.

To import CA root certificates that are located in a different PSE:

1. Expand the node for the PSE that contains the certificates and double-click one of the application servers to select it.
2. The PSE and its certificate list appear in the PSE maintenance section.
3. Double-click the certificate to select it.

   The certificate appears in the certificate maintenance section.
4. Double-click one of the application servers under the **SSL server PSE** node to select it.
5. Click **Add to Certificate List**.

   The certificate is added to the certificate list for the PSE displayed in the PSE maintenance section.
6. Save the data.
7. Repeat for all certificates.

1. Open your SSL certificate files in a text editor and paste the contents of each certificate one after the other, in this order:
   a. Server certificate (your_domain_name.crt)
   b. Intermediate certificates
   c. Root certificate

   Include the beginning and end tags on each certificate. The result should look like this:

```
--BEGIN CERTIFICATE--
(Your Primary SSL certificate:
your_domain_name.crt) --END CERTIFICATE--
--BEGIN CERTIFICATE--
(Your Intermediate certificate:
Trend_Micro_CA.crt) --END CERTIFICATE--
--BEGIN CERTIFICATE--
(Your Root certificate:
root_certificate.crt) --END CERTIFICATE-
-
```

2. In the web server, select **SSL certificates**.
3. Click **Generate CSR** (or, possibly, **Replace Certificate**) for this certificate.
4. Paste your new combined certificate into the **Signed Certificate** box and click **OK**.
5. Accept this certificate.
6. Click **Home**, and check the box next to the domain you are securing. Click **Configure**.
7. Go to **SSL enabled**. Click **SSL is enabled**, and select your certificate.
8. Save the changes, and restart the server.