### HOSTING WARRIORS



Christian Web Hosting for Warriors on a Mission"

#### SSL/TLS

The SSL and TLS features are intended to make your website more secure. These features generate and manage SSL certificates, signing requests, and keys. This is useful for websites that will use logins and credit card numbers, since information will be sent to and from your website over the Internet as encrypted data versus plain text. This makes it difficult for malicious users to intercept communications between visitors and your website.

To begin, select a link underneath 1 of the 3 headings:

- Private Keys (KEY)
- Certificate Signing Requests (CSR)
- Certificates (CRT)

These links provide access points that generate, view, or delete keys, requests, and certificates.

**Note:** Adding a private key is the first step in setting up an SSL certificate for your site. It is highly recommended that SSL certificates be used if your visitors will be submitting sensitive information to your website.

# Add a Private Key

A new key can be added manually or uploaded using a \*.key file.

### **Upload an Existing Key**

To upload a key, begin under the Upload a New Key heading:

1. Enter your domain name in the *Domain the key is for* field.

- 2. Paste a key below or click the *Choose File* button to upload a \*.key file.
- 3. Click the *Install* button to properly install the private key to the server.

#### **Generate a New Key**

If an entirely new key is needed:

- 1. Select the desired domain name from the pull-down menu, or type it into the *Host* field.
- 2. Select the desired key size from the pull-down menu.
- 3. Click the *Generate* button to generate the new key.

The key will automatically be installed on the server and will appear in the list under the *Keys on Server* heading once it has been generated.

#### **Remove a Key on Server**

Click *Remove* to the right of the appropriate domain in the *Keys on Server* table. Then, click *Yes* to confirm.

### Show Details about a Key on Server

Click Show Details to the right of the appropriate domain in the Keys on Server table.

# Add a Certificate Signing Request (CSR)

The signing request form is required for obtaining a certificate from an SSL provider. The SSL provider may require information in a specific way. If this is true for your SSL provider, take the steps to make sure the information is presented in the required way.

## Generate a New Certificate Signing Request (CSR)

To generate a CSR:

- 1. Select the host from the *Host* pull-down menu.
- 2. Fill in the rest of the appropriate information in the fields below the menu.

3. Click the *Generate* button.

**Remember:** You must have a key prior to generating a signing request.

#### **Remove a Certificate Signing Request (CSR)**

To remove a CSR:

- 1. Click *Remove* to the right of the appropriate domain in the *Certificate Signing Requests on Server* table.
- 2. Click Yes to confirm.

#### Show Details about a Certificate Signing Request (CSR)

To show details about a CSR, click *Show Details* to the right of the appropriate domain in the \_Certificate Signing Requests on Server table.

## Add a Certificate

When installing a trusted certificate obtained through an SSL provider, use the features beneath the *Upload a New Certificate* heading.

### **Upload an Existing Certificate**

To upload the certificate:

- 1. Paste the certificate into the text box, or upload a \*.crt file using the *Choose File* button.
- 2. Click the *Upload* button to install the certificate onto the server.

#### **Generate a New Certificate**

If the SSL certificate is self-signed, it can be generated under *Generate a New Certificate*:

- 1. Select the host from the pull-down menu.
- 2. Key-in the remaining information.
- 3. Click Generate.

When the certificate is generated and self-signed, it will automatically be installed on the server.

**Note:** Self-signed certificates are generally reserved for intranet uses. To use a certificate on the Internet, you should use a third-party service. Consult your favorite search engine to shop for SSL providers.

#### **Remove a Certificate**

To remove a certificate:

- 1. Click *Remove* to the right of the appropriate host in the *Certificates on Server* table.
- 2. Click Yes to confirm.

#### Show Details about a Certificate

Click *Show Details* to the right of the appropriate host in the *Certificates on Server* table.

## Manage Certificate Sharing

If you are the server administrator, you can choose to allow your customers to share your SSL certificate.

- 1. Click Change Certificate Sharing Permissions to begin.
- 2. On the Manage SSL Certificate Sharing screen, click Enable Sharing.
  - Click *Disable Sharing* if you want to disallow users from sharing your certificate.
- 3. Under the *Certificate Linking* heading, select a domain to see an accurate link example.
  - Your customers can share your SSL certificate at this URL, if you enabled sharing. However, before you eagerly enable hotlink protection in a bid to stop the evil bandwidth thieves, you need to be aware of the limitations and potential problems that might come with enabling the feature.