Manage Service SSL Certificates

This documentation is for a previous release of cPanel & WHM. To view our latest documentation, visit our Home page.

For cPanel & WHM 54

(Home >> Service Configuration >> Manage Service SSL Certificates)

Overview

This interface allows you to manage certificates for your server's services, such as:

- Exim (SMTP).
- POP3 and IMAP.
- The cPanel services (cPanel & WHM and Webmail).
- Your FTP server.

SSL certificates allow your web server to identify itself to the computers that access it.

You can use either a certificate that you purchased from a certificate authority or a self-signed certificate.

Important:
If you use a self-signed certificate for a service, the system will automatically reset that self-signed certificate when it expires.

Warning:
We recommend that you **do not use** self-signed certificates. They are not as secure as certificates from a certificate authority. Any server could claim to be your server with a self-signed certificate because they do not use a third-party verification system. To remedy this, use certificates from a certificate authority (CA), which verifies that users are securely connected to your server.

For more information about how to generate or purchase a certificate, read our Generate an SSL Certificate and Signing Request documentation.

Service SSL Certificates

At the top of the interface, you will see a table that contains the services on your server and the certificates for each service:

Column	Description
Service	The service that the certificate secures.
Certificate Domains	The domain of the service that the certificate secures.

Certificate Expiration	The date on which the certificate expires. **Note:** Before the certificate expires, WHM will send a warning to the system administrator's email address to reset or replace the certificates. A warning will also appear in WHM's *Home* interface. **Remember:** If you use a self-signed certificate for a service, the system will automatically reset that self-signed certificate when it expires.
Certificate Key Size	The size of the key, in bits, that the system used to generate the certificate. Larger numbers result in certificates that are more secure.
Actions	(See below)

Reset a Certificate

This option uninstalls the current certificate for the service and replaces it with a new self-signed certificate.

To reset a certificate, perform the following steps:

1. Click *Reset Certificate* next to the service for which you wish to reset the certificate.
2. Click *Generate a New Certificate* to generate and automatically install the certificate.

> **Warning**
> This option automatically erases an existing certificate from the service. If you replace a certificate from a certificate authority with a self-signed certificate, users may see warnings because their client applications do not trust self-signed certificates.

Certificate Details

This option displays details about the installed certificate for the service:

Column	Description
Domains	The domain of the service that the certificate secures.
Issuer	Information about the certificate authority that issued the certificate. **Note:** This column displays a warning message for self-signed certificates.
Key Size	The size of the key, in bits, that the system used to generate the certificate. Larger numbers result in certificates that are more secure.
Expiration	The date on which the certificate expires. **Note:** Before the certificate expires, WHM will send a warning to the system administrator's email address to reset or replace the certificates. A warning will also appear in WHM's *Home* interface.

Apply Certificate to Another Service

This option allows you to apply a certificate to multiple services. This is useful, for example, when you have a signed certificate for your server's main domain that you wish to apply to other services on your server.

To apply a certificate to another service, perform the following steps:

1. Click the appropriate *Apply Certificate to Another Service* link.
2. The interface will scroll down to the *Install a New Certificate* section. Select the checkboxes for the services for which you wish to apply this certificate.

   > **Note:**
   > WHM automatically enters the details of the *Install a New Certificate* text boxes with the certificate's information.

3. Click *Install* to install the certificate to the selected services, or click *Cancel* to cancel the operation.

   > **Warning:**
   > If you replace a certificate from a certificate authority with a self-signed one, users may see warnings because their client applications do not trust self-signed certificates.

Install a New Certificate

This form allows you to install a new certificate that you can use to secure the services on your server.

To install a new certificate on your server, perform the following steps:

1. To use a certificate that already exists on your server, click *Browse Certificates*. Select the services that you wish for the certificate to secure.
   a. Click *Browse Account* and select the username from the menu, or click *Browse Apache.*
   b. Select the certificate that you wish to use from the menu.
   c. Click *Use Certificate* to use the certificate, or click *Cancel* to cancel the operation.

      > **Note:**
      > WHM automatically enters the certificate's information into the *Install a New Certificate* form.

2. Paste the contents of the Certificate file (`.crt`) into the *Certificate* text box.

   > **Note:**
   > Click *Autofill by certificate* to search for the appropriate private key and CA bundle from cPanel's public CA bundle repository.

3. Paste the contents of the Private Key file (`.key`) into the *Private Key* text box.
4. If you have a CA bundle, paste the contents of that bundle (`.cab`) into the *Certificate Authority Bundle* text box.
5. Click *Install* to install the certificate, or click *Cancel* to cancel the operation.
6. If you selected the `cpsrvd` daemon, and the certificate has installed correctly, the interface will prompt you to restart the `cpsrvd` daemon. Click *Restart cpsrvd* to restart the cPanel service daemon.

   > **Important:**
   > You **must** restart the `cpsrvd` daemon each time that you install a new SSL certificate for a service.