Manage Service SSL Certificates

For cPanel & WHM version 64

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

- Overview
  - Free cPanel-signed certificate
- Service SSL Certificates
  - Reset a Certificate
  - Certificate Details
  - Apply Certificate to Another Service
- Install a New Certificate
- iOS Mail push notifications
- Additional documentation

Overview

This interface allows you to manage certificates for your server's services. For example, you can manage certificates for the following services:

- Exim (SMTP).
- POP3 and IMAP.
- The cPanel services (cPanel & WHM and Webmail).
- Your FTP server.
- iOS Mail Push Notifications (APNs).

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

You can use any of the following types of certificates to secure your server's services:

- A free cPanel-signed hostname certificate.
- A certificate that you obtained from a certificate authority (CA).
- A self-signed certificate.

> **Warning:**
> We recommend that you **do not use** self-signed certificates. They are **not** as secure as certificates from a CA. 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 CA, which verifies that users are securely connected to your server.

- PKCS #12 (iOS APNs **only**).

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

> **Note:**
> In cPanel & WHM version 64, we will attempt to automatically replace the default SSL certificate for any service besides Apache if that certificate does not match the server’s hostname. However, we will **only** automatically replace the certificate if that certificate is a one-year, cPanel-signed single domain, domain-validated (DV) certificate.

Free cPanel-signed certificate

cPanel, Inc. offers valid cPanel & WHM license holders a free signed certificate for the services on your server's hostname. This replaces the certificates for these services that meet any of the following conditions:

- Maintains a weak signature algorithm.
- Revoked.
- Self-signed.
- Invalid (For example, your server's hostname must be valid and resolve in DNS).
- Expires in less than 25 days.

Your server automatically orders the certificate when the server runs the `upcp` maintenance script, and then downloads and installs it when it becomes available.

When that signed certificate is less than 25 days from expiration, your server automatically orders a replacement free signed certificate. The server downloads and installs the certificate when it becomes available. Otherwise, if the signed certificate expires, the server installs a self-signed certificate, and then replaces that certificate with the free signed certificate when it is ready.

Notes:

- If you create the `/var/cpanel/ssl/disable_auto_hostname_certificate` touch file, the system will no longer order, download, and install a free cPanel-signed hostname certificate.
- If you create the `/var/cpanel/ssl/disable_service_certificate_management` touch file, the system disables all automatic replacement of expired service certificates. The system also disables notifications about expired or expiring service certificates.

Important:

- Your server **must** possess a valid hostname and resolve in DNS.
- Your server **must** possess a valid cPanel & WHM license.
- This system **only** replaces self-signed or expired certificates. It does **not** replace an existing certificate from a valid CA.
- cPanel, Inc. does **not** offer free cPanel-signed hostname certificates for cPanel DNSONLY servers.

Service SSL Certificates

The interface displays the following table, which lists 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. **Notes:** • Before the certificate expires, WHM sends 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. • When a certificate expires, your server installs a self-signed certificate. If your server meets the requirements to obtain a free cPanel-signed certificate, the server automatically orders one the next time that the `upcp` maintenance script runs. When the signed certificate becomes available, the server downloads and installs it.
Certificate Key Size	The size of the key, in bits, that the system used to generate the certificate. Larger numbers result in more secure certificates.
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 to reset the certificate.
2. Click *Proceed* to generate and automatically install the certificate.

Warnings:

- This option automatically erases an existing certificate from the service. If you replace a certificate from a CA with a self-signed certificate, users may see warnings because their client applications do **not** trust self-signed certificates.
- If your server meets the requirements to obtain a free cPanel-signed certificate, the server automatically orders one the next time that the `upcp` maintenance script runs. When the signed certificate becomes available, the server downloads and installs it.

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 CA 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. **Notes:** • Before the certificate expires, WHM sends a warning to the system administrator's email address to reset or replace the certificates. A warning also appears in WHM's *Home* interface. • If your server meets the requirements to obtain a free cPanel-signed certificate, the server automatically orders one the next time that the `upcp` maintenance script runs. When the signed certificate becomes available, the server downloads and installs it.

Apply Certificate to Another Service

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

iOS Mail push notifications

In cPanel & WHM version 64, we introduced support for the iOS Apple® Push Notification service (APNs). Use this interface to manage the certificate and key that your server uses to communicate with APNs. For more information about how to install this certificate, read our How to Set Up iOS Push Notifications documentation.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- Manage SSL Hosts
- Manage Service SSL Certificates
- Security FAQ
- Purchase and Install an SSL Certificate
- Generate an SSL Certificate and Signing Request

- SSL TLS Wizard
- SSL TLS
- Manage Certificate Sharing
- Install and Manage SSL for your site HTTPS
- Security Policy

- Manage SSL Hosts
- Manage Service SSL Certificates
- Security FAQ
- Purchase and Install an SSL Certificate
- Generate an SSL Certificate and Signing Request

- WHM API 1 Functions - get_autossl_check_schedule
- WHM API 1 Functions - disable_autossl
- WHM API 1 Functions - get_autossl_pending_queue
- WHM API 1 Functions - get_autossl_providers

- WHM API 1 Functions - get_autossl_log