SSL TLS Status

(*cPanel >> Home >> Security >> SSL/TLS Status*)

Overview

This interface allows you to view, upgrade, or renew your Secure Sockets Layer (SSL) certificates. You can also view useful information about each domain's SSL certificate, for example:

- The type of certificate that secures the domain.
- When the certificate expires or expired.
- Graphical representation of all certificates for quick reference.
- Options such as *View Certificate* or *Upgrade Certificate* for applicable domains.
- AutoSSL Domain Control Validation (DCV) error messages for applicable domains.
- The last time that AutoSSL ran for applicable domains.

Warning:
As of cPanel & WHM version 68, we only support Transport Layer Security (TLS) protocol version 1.2.

- We will only support applications that use TLSv1.2.
- We **strongly** recommend that your hosting provider enable TLSv1.2 for your account.

Note:

CAA (Certificate Authority Authentication) records in the domain's zone file restrict which CAs (Certificate Authority) may issue certificates for that domain.

- If no CAA records exist for a domain, all CAs can issue certificates for that domain.
- If conflicting CAA records already exist, remove the existing CAA records or add one for the desired CA.

For example, a CAA record for Comodo would resemble the following example, where e `xample.com` represents the domain name:

```
example.com. 86400 IN CAA 0 issue
"comodoca.com"
```

You can manage CAA records through cPanel's *Zone Editor* interface (*cPanel >> Home >> Domains >> Zone Editor*). For more information about a CA's requirements, read their documentation.

Purchase certificates banner

The banner at the top of the interface allows you to perform the following actions:

- View a list of unsecured domains.
- Purchase certificates for all unsecured domains.
- Select which domains to secure.

When you click *Purchase Certificates*, cPanel's *SSL TLS Wizard* interface (*cPanel >> Home >> Security >> SSL/TLS Wizard*) will appear, which displays the unsecured domains and available certificates. When you click *Show Unsecured Domains*, the *Domain* list will display only unsecured domains.

In This Document

Related Documentation

- SSL TLS Status
- Install and Manage SSL for your site HTTPS
- Manage Certificate Sharing
- SSL TLS
- Private Keys - KEY

For Hosting Providers

- More about TLS and SSL
- What is Domain TLS
- Tweak Settings - Redirection —

Search bar and filter

The *Search* text box allows you to filter by domain name. Enter all or part of the domain name to update the domain list. For filter options, click the filter icon (

).

Click the tab below to view each filter option.

Note: When a user accesses cPanel, WHM, or Webmail on an SSL/TLS port with the HTTP protocol, the web server redirects the user to the URL of the server's hostname with the HTTPS protocol. For example, if the server's hostname is `host.exampleshost.com`, `http://www.example.com:2083` will direct the user to the `https://host.examplehost.com:2083` location.

Choose the closest matched domain for which that the system has a valid certificate when redirecting from non-SSL to SSL URLs. Formerly known as “Always redirect to SSL/TLS”

This setting allows you
to redirect users to the proper SSL/TLS ports when they visit specific URLs. This setting defaults to *On*.

When you enable this setting, the system will attempt to redirect in the following order:

1. Redirect to the *Origin Domain Name* if an installed certificate secures that domain an installed certificate.
2. Redirect to a wildcard domain that matches the name on the main service certificate.
3. If no domain matches the domains on any certificate, then redirect to `https://` protocol for the domain.

Warnings:

- If you disable this option, users may see

d t h e i r p a s s w o r d s t o t h e s e l i n k s **w i t h o u t** e n c r y p t i o n . W e **s t r o n g l y** r e c o m m e n d t h a t y o u d

o **n o t** d i s a b l e t h i s o p t i

on.

- The *RequireSSL* option in the *Security* section of the *TweakSettings* interfa

ce (*WHM >> Home >> Server Configuration >> Tweak Settings*) forces SSL direction by def

ault. We recommend that you do **not** change this setti

ng.

- The system will redirect users who navigate to the /cpanel, /webmail, or /whmpat

hs of their domain to a respective port, but will not be redirected if they enter the cor

responding subdomain. For examp

le:

- As of cPanel & WHM version 68, we **only** support Transpo
- Whe
  www
  ,
  www
  , or
  www
  , the
  www
  ,
  www
  , or
  www
  208

  resp
- This
  cpa
  ,
  web
  , or
  whm
  .

rtLayerSecurity(TLS)protocol version1.

2
.

- We
  sup
  TLS
- We
  stro
  rec
  TLS
  on

Note:
The *Calendars and Contacts* interface (*cPanel >> Home >> Email >> Calendars and Contacts*) **requires** that your third-party client supports redirection.

Non-SSL redirect destination

Note:
If you enable *Always redirect to SSL/TLS*, the system ignores this setting.

This setting allows you to specify how to redirect users who access cPanel & WHM via the `/cpanel`, `/webmail`, or `/whm` paths without SSL. Select one of the following options:

- *Hostname* — Redirects users to the server's hostname (for example, `host.example.com:2082`, where `host.example.com` represents the server's hostname).
- *Origin Domain Name* — Redirects a user to their main domain (for example, `example.com:2082`, where `example.com` represents the user's domain).

This setting defaults to *Origin Domain Name* .

SSL redirect destination

> **Note:**
> If you enable *Always redirect to SSL/TLS*, the system ignores this setting.

This setting allows you to specify how to redirect users who access cPanel & WHM via the `/cpanel`, `/webmail`, or `/whm` paths with SSL. Select one of the following options:

- *SSL Certificate Name* — Redirects users to the domain that the website's SSL certificate secures. You can view this certificate in the *Manage Service SSL Certificates* interface (*WHM >> Home >> Service Configuration >> Manage Service SSL Certificates*).
- *Hostname* — Redirects users to the server's hostname (for example, `host.example.com:2083`, where `host.example.com` represents the server's hostname).
- *Origin Domain Name* — Redirects a user to their main domain (for example, `example.com:2083`, where `example.com` represents the user's domain).

This setting defaults to *SSL Certificate Name*.

Logout redirection URL

This setting allows you to redirect users to a specific URL after they log out of cPanel.

This setting defaults to *No redirection*.

- cPanel Web Disk Configuration
- cPanel Web Services Configuration

Domain TypesSSL TypesSSL StatusesAutoSSL Statuses

Type	Description
All	Select all of the domains, regardless of type.
Main	Select only the main domains. For example: • `example.com` • `www.example.com`
Subdomain	Select only the subdomains. For example: • `store.example.com` • `www.store.example.com`
Addon Domains	Select only the addon domains. For example: • `addon.com` • `www.addon.com`
Parked Domains	Select only the parked domains. For example: • `parked.com` • `www.parked.com`
www and mail domain	Select only the `www` and `mail` subdomains. For example: • `www.example.com` • `mail.example.com`

Proxy subdomains	Select only the proxy subdomains. For example: • `cpanel.example.com` • `whm.example.com` • `webmail.example.com` • `webdisk.example.com`

Type	Description
All	Select all of the domains, regardless of certificate type.
Unsecured	Select only the unsecured domains. No certificates secure these domains. **Warning:** We **strongly** recommend that you secure all of the domains that you visitors may view.
Self-Signed	Select only the domains that a self-signed certificate secures.
AutoSSL DV Certificate	Select only the domains that an AutoSSL-issued domain validated (DV) certificate secures.
DV Certificate	Select only the domains that a DV certificate secures.
OV Certificate	Select only the domains that a organization validated (OV) certificate secures.
EV Certificate	Select only the domains that a Extended Validation (EV) certificate secures.

Status	Description
All	Select all of the domains, regardless of certificate status.
Active	Select only the domains that active certificates secure.
Expired	Select only the domains with an expired certificate.
Expiring Soon	Select only the domains secured by certificates that expire soon.
Unsecured	Select only the domains that no certificate secures.
Has AutoSSL Problems	Select only the domains with AutoSSL problems. For example: `This domain does not resolve to an IPv4 address on the internet.`

Status	Description
All	Select all of the domains, regardless of AutoSSL status.
Included	Select only the domains that AutoSSL includes.
Excluded	Select only the domains that AutoSSL does **not** include.

AutoSSL selection

To control whether AutoSSL includes an individual domain, select one of the following options:

- *Include during AutoSSL* — Select the checkbox of each domain to include when AutoSSL runs, then click *Include during AutoSSL*.
- *Exclude during AutoSSL* — Select the checkbox of each domain to exclude when AutoSSL runs, then click *Exclude during AutoSSL*.
- *Run AutoSSL* — Force AutoSSL to run immediately. The *AutoSSL is in progress …* message displays for the duration of the AutoSSL operation. The page will refresh when the operation completes.

> **Note:**
> The *AutoSSL is in progress...* message may display when you load this interface if the AutoSSL operation is already in progress.

The Domains table

The *Domains* table displays each domain's certificate and provides options to view or upgrade the certificate.

- *Domain* — This column displays a complete or filtered list of all domains on the cPanel account. The following certificates display in this column:
  - *Unsecured*
  - *Self-Signed certificate*
  - *Domain validated*
  - *AutoSSL Domain Validated*
  - *Organization validated*
  - *Extended validation*
- *Certificate Status* — This column displays domain specific certificate information. If an error exists for the domain in the `/var/cpanel/logs/autossl/` directory, that error will display in this column. This column also displays the time AutoSSL last ran for applicable domains. The following options display in this column:
  - *View Certificate* — View the certificate of the domain if the certificate exists. The *Manage SSL Hosts* section of cPanel's *SSL/TLS* interface (*cPanel >> Home >> Security >> SSL/TLS*) will appear in a new window.
  - *Upgrade Certificate* or *Purchase Certificate* — Upgrade or purchase a certificate for the domain. cPanel's *SSL/TLS Wizard* interface (*cPanel >> Home >> Security >> SSL/TLS Wizard)* will appear, which will display the specified domain and available certificates.

    > **Note:**
    > The *View Certificate*, *Upgrade Certificate*, and *Purchase Certificate* options only appear for applicable domains.

  - *Include during AutoSSL* or *Exclude from AutoSSL* — Apply or remove AutoSSL for this domain. For more information about AutoSSL, read our Manage AutoSSL documentation.

    > **Note:**
    > To select multiple domains, perform the following steps:
    >
    > 1. Select or deselect the checkboxes to add or remove the applicable domains.
    > 2. Click *Include Domains during AutoSSL* or *Exclude Domains during AutoSSL* at the top-left of the interface. For example, click *Include 5 Domains during AutoSSL*.