Manage AutoSSL

(*WHM >> Home >> SSL/TLS >> Manage AutoSSL*)

Overview
Providers
Options
Logs
Manage Users
Pending Queue
Additional documentation

Overview

This interface allows you to manage the AutoSSL feature, which automatically installs domain-validated SSL certificates for the Apache®, Dovecot®, Exim, Web Disk, and cPanel Server services for users' domains. It also allows you to review the feature's log files and select which users receive AutoSSL certificates.

Notes:

- The cPanel AutoSSL provider requires outbound access to the `store.cpanel.net` server over port 443. For more information, read our How to Configure Your Firewall for cPanel Services documentation.
- While the cPanel AutoSSL provider generally only requires a short amount of time to complete the installation process, certain factors may cause longer wait times. Under some conditions, certificates may require up to 48 hours to process.

Run AutoSSL for All Users

Click *Run AutoSSL for All Users* at the top of the interface to run the AutoSSL feature for all users for whom you enabled the feature.

Notes:

- The system runs the AutoSSL feature for all users when it performs nightly system updates via the `/usr/local/cpanel/scripts/upcp` script. AutoSSL examines the system's SSL coverage and requests certificates from the configured provider to improve the system's SSL coverage.
- To run the AutoSSL feature for all users via the command line, run the `/usr/local/cpanel/bin/autossl_check --all` command.

cPanel AutoSSL certificates

The system automatically polls the cPanel AutoSSL certificate provider to determine each pending certificate's status:

Note:
The cPanel (powered by Sectigo®) provider does **not** request additional certificates for a web virtual host if the provider already possesses a pending certificate request for that web virtual host.

Age of certificate request	Polling frequency
Less than one day.	Once per five minutes.
Between one and two days.	Once per hour.
More than two days.	Once per day.

CAA Records preflight check

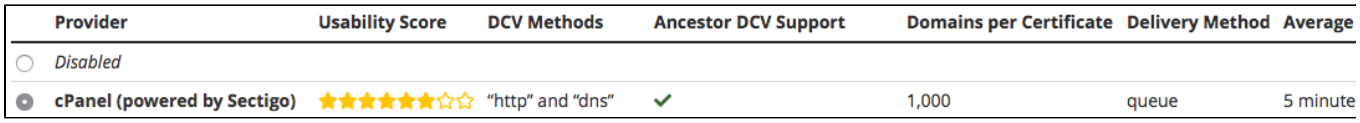
When AutoSSL runs, the system performs a preflight check. This check adds a Certificate Authority Authentication (CAA) record in the domain's zone file before AutoSSL orders a new certificate for that domain.

Providers

The AutoSSL *Providers* tab allows you to select which provider you want to handle your AutoSSL management. For more information about each provider, their services, and general usability, click *Show/Hide Details*. This action displays a table that scores each provider by their AutoSSL services and capabilities. These usability scores are measured with a star (

) icon. Certain provider capabilities and features affect and contribute to their overall usability score.

For example, an AutoSSL provider with an six-star score may look like the following:



Provider	Usability Score	DCV Methods	Ancestor DCV Support	Domains per Certificate	Delivery Method	Average
Disabled						
cPanel (powered by Sectigo)	★★★★★★☆☆	"http" and "dns"	✔	1,000	queue	5 minute

The system calculates the *cPanel (powered by Sectigo)* provider's usability score by its ability to:

- Support the *"http"* and *"dns"* Domain Control Validation (DCV) method (two stars for each Ancestor DCV-supported DCV method, for a total of four stars).
- Provide 1,000 domains per certificate (one star).
- The ability to provide an *unlimited* number of certificates per registered domain per week (one star).

The provider details table contains the following information:

Category	Description
Provider	The AutoSSL provider. Select *Disabled* to disable the AutoSSL feature.
Usability Score	The total score of a provider, which its AutoSSL capabilities determine. This score is the sum of each provider's *DCV Methods*, *Ancestor DCV Support*, *Domains per Certificate*, *Average Delivery Time*, *Maximum Number of Redirects*, and *Rate Limit* capabilities. A provider can attain a rating up to eight stars.
DCV Methods	The DCV methods that the provider offers. A provider can receive a total of two stars per DCV method if they support Ancestor DCV. If they do **not** support Ancestor DCV, the provider receives one star per DCV method.
Ancestor DCV Support	Whether the successful DCV of a parent domain implies success of a subdomain. For example, if the `example.com` succeeds, then the DCV for the `store.example.com` subdomain is unnecessary.
Domains per Certificate	The number of unique domains per certificate. A provider can receive a total of one star.
Delivery Method	The means through which the provider issues a certificate, via the *api*, *queue*, or *Unspecified* method.
Average Delivery Time	The amount of time the provider requires to issue a certificate, if specified. A provider can receive a total of one star.
Validity Period	The period of time before the certificate expires, or *Unspecified*.
Maximum Number of Redirects	The maximum number of redirects a domain can use and still pass an HTTP-based DCV. A provider can receive a total of one star.
Rate Limit	The number of certificates the provider registers per domain per week, or *Unspecified*. A provider can receive a total of one star.

Terms of Service

If the AutoSSL provider requires a Terms of Service or other similar agreement, review it and select the appropriate checkbox to agree to those terms.

> **Note:**
> If a provider updates their Terms of Service, you may need to return to this interface to agree to them.

Options

The *Options* tab allows you to configure various options for AutoSSL.

Notifications

The notification options allow you to select the frequency at which your users receive AutoSSL-related notifications.

> **Notes:**
> - Some of these options remove the corresponding notification option in cPanel's *Contact Information* interface (*Home >> cPanel >> Preferences >> Contact Information*). For example, if you disable the *Notify the user for **all** AutoSSL events and normal successes* user notification setting, this option is unavailable to your cPanel users.
> - These options override the user's current settings.

User Notifications

You can select from the following notification options for your cPanel users:

- *Notify the user for **all** AutoSSL events and normal successes.*
- *Notify the user for AutoSSL certificate request failures, warnings, and deferrals.*
- *Notify the user for AutoSSL certificate request failures **only**.*
- *Disable AutoSSL user notifications.*

This setting defaults to *Notify the user for AutoSSL certificate request failures, warnings, and deferrals.*

Administrator Notifications

You can select from the following notification options for your reseller and WHM users:

- *Notify the administrator for **all** AutoSSL events and normal successes.*
- *Notify the administrator for AutoSSL certificate request failures, warnings, and deferrals.*
- *Notify the administrator for AutoSSL certificate request failures **only**.*
- *Disable AutoSSL administrator notifications.*

This setting defaults to *Notify the user for AutoSSL certificate request failures, warnings, and deferrals.*

Allow AutoSSL to replace invalid or expiring non-AutoSSL certificates.

This option allows AutoSSL to replace certificates that the AutoSSL system did **not** issue. When you enable this option, AutoSSL will install certificates that replace users' non-AutoSSL certificates if they are invalid or expire within 3 days.

> **Important:**
> - Unless you fully understand this option, do **not** enable it, because the system may unexpectedly replace an expiring or invalid Extended Validation (EV) or Organization Validated (OV) certificate with a Domain Validated (DV) certificate.
> - Users' non-AutoSSL certificates are paid, and should be replaced by another paid certificate.

Logs

Use the *Logs* tab to review the system's AutoSSL log files. To view a specific log, select it from the menu and click *View Log* to display the its information.

> **Note:**
> The system stores the log files in both text and JSON format in the `/var/cpanel/logs/autossl` directory.

Manage Users

The *Manage Users* tab allows you to override your server's feature list settings and control whether AutoSSL is enabled for your users. Use the search text box to locate specific users, or use the check box and menu to select all users or clear your current selections.

Note:
User feature lists may differ, based on the user's assigned package. For more information, read our Feature Manager documentation.

You can select from the following *Toggle AutoSSL* options for individual users and select users:

- *Enable AutoSSL on selected users* — Override the feature list setting and force AutoSSL to be enabled.
- *Disable AutoSSL on select users* — Override the feature list setting and force AutoSSL to be disabled.
- *Reset AutoSSL on selected users* — Use setting established by the feature list's *default* setting. For more information, read our Feature Manager documentation.

Run AutoSSL Check

You can use the *Check* button to perform a domain check for a specific user.

Pending Queue

The *Pending Queue* section of the interface lists the status and the details of the pending AutoSSL jobs on your server.

Use the navigation controls at the top of the table to sort and search through the list.

Additional documentation

Suggested documentationFor cPanel usersFor WHM usersFor developers

- Manage AutoSSL
- The is_script_stuck Script
- Service Manager
- Service Status
- WHM Scripts

- Server Information for cPanel
- SSL TLS Wizard
- Install and Manage SSL for your site HTTPS
- SSL TLS Status
- Private Keys - KEY

- Manage AutoSSL
- How to Restart Services
- The cPanel Service Daemons
- The is_script_stuck Script
- Service Manager

- WHM API 1 Functions - fetch_service_ssl_components
- WHM API 1 Functions - install_service_ssl_certificate
- WHM API 1 Functions - reset_service_ssl_certificate
- WHM API 1 Functions - configureservice
- cPanel API 1 Modules - Serverinfo