Manage AutoSSL

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

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:

- In cPanel and WHM version 60 and later, the system modifies the `.htaccess` file with the following rules:

```
RewriteCond %{REQUEST_URI} !^/[0-9]+\..+\.cpaneldcv$
RewriteCond %{REQUEST_URI} !^/[A-F0-9]{32}\.txt(?:\ Comodo\
DCV)?$
RewriteCond %{REQUEST_URI}
!^/\.well-known/acme-challenge/[0-9a-zA-Z_-]+$
```

- 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:

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.

Note:
The cPanel (powered by Comodo®) 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.

Providers

Warning:
Let's Encrypt™ imposes significant rate limits. For more information, read our SSL FAQ and Troubleshooting documentation.

To select an AutoSSL provider, perform the following steps:

1. Select the desired AutoSSL provider or select *Disabled* to disable this feature.
2. 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 the provider updates their Terms of Service, you may need to return to this interface to agree to them.

3. Click *Save.*

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 documentation For cPanel users For WHM users For developers

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

- Server Information for cPanel
- Install and Manage SSL for your site HTTPS
- SSL TLS Status

- Manage Certificate Sharing
- Certificate Signing Requests - CSR

- Manage AutoSSL
- System User Accounts
- WHM Scripts
- The find_outdated_services Script
- The cPanel Service Daemons

- 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 - servicestatus
- WHM API 1 Functions - configureservice