

Manage AutoSSL

For cPanel & WHM version 58

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

Overview

Domain and rate limits

Select an AutoSSL provider

Enable AutoSSL

Feature list override

Run AutoSSL

Review log files

Frequently Asked Questions

How do I revoke a certificate?

Let's Encrypt won't issue a certificate for a virtual host list (website).

Is Manage AutoSSL available for cPanel & WHM version 56?

Overview

This interface allows you to manage the AutoSSL feature, which automatically installs domain-validated SSL certificates on users' domains for the Apache and Dovecot services. It also allows you to review the feature's log files and select which users to secure with AutoSSL.

Notes:

- cPanel & WHM ships with the cPanel (powered by Comodo) provider. To install the Let's Encrypt AutoSSL provider plugin, read our [The Let's Encrypt Plugin](#) documentation.

Warnings:

- Certificates that Let's Encrypt provides through AutoSSL can secure a **maximum** of 100 domains per *virtual host*.
 - Let's Encrypt will issue a maximum of 20 certificates per week that contain a domain or its subdomains. If you include subdomains of a domain on more than 20 certificates, Let's Encrypt will issue those during the next window, up to the limit for that week.
 - Let's Encrypt uses the domain's alias (parked domain), **not** the main domain, as the common name for AutoSSL. To use the main domain as the common name for AutoSSL, you must use cPanel or another AutoSSL provider. For more information, consult the [Let's Encrypt Community Support](#) page.
- The AutoSSL feature 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](#) knowledgebase article.

Domain and rate limits

The AutoSSL feature includes the following limitations and conditions:

- Each AutoSSL provider may have a specific domain rate limit. For example:
 - Certificates that cPanel, Inc. provides through AutoSSL can secure a **maximum** of 200 domains per virtual host.
 - Certificates that Let's Encrypt™ provides can secure a **maximum** of 100 domains per virtual host.
- AutoSSL will **only** include domains and subdomains that pass a Domain Control Validation (DCV) test, which proves ownership of the domain.
- AutoSSL includes corresponding `www.` domains for each domain and subdomain in the certificate, and those `www.` domains count towards any domain or rate limits.
 - For example, if your domain is `example.com`, AutoSSL will automatically include `www.example.com` in the certificate.
 - If the corresponding `www.` domain does not pass a DCV test, AutoSSL will not attempt to secure that `www.` domain.
 - This affects Let's Encrypt's limit of 20 certificates per week that may contain a domain or its subdomains.
- AutoSSL does **not** secure proxy subdomains or wildcard domains.
- Each AutoSSL provider may wait for a specific amount of time to replace an AutoSSL-provided certificate before it expires. For example:
 - AutoSSL will attempt to renew certificates that cPanel, Inc. provides when they expire within 15 days.
 - AutoSSL will attempt to renew certificates that Let's Encrypt provides when they expire within 29 days.
 - Due to rate limits, AutoSSL prioritizes new certificates over the renewal of existing certificates.
- AutoSSL will **not** attempt to replace pre-existing valid certificates that expire in more than three days.
- AutoSSL will replace certificates with overly-weak security settings (for example, RSA modulus of 512-bit or less).
- If a virtual host contains more than the provider's limit of domain names, AutoSSL uses the following conditions to determine the priority of domains to secure:

1. Whether the domains are currently secured.
2. Shortest domain name length.
3. Domain name alphabetical order.

For example, the following table demonstrates these limitations for the cPanel AutoSSL provider:

Virtual Host 1	Virtual Host 2	Result
200 domains		AutoSSL will generate one certificate for the account which secures all 200 domains.
202 domains		AutoSSL will generate one certificate for the account which secures the 200 domains with the shortest names.
100 domains	100 domains	AutoSSL will generate a certificate for each virtual host that secures all of its domains.
100 domains	102 domains	AutoSSL will generate a certificate for each virtual host that secures all of its domains.
100 domains	202 domains	AutoSSL will generate two certificates: <ul style="list-style-type: none"> • Virtual Host 1 — Secures all of its domains. • Virtual Host 2 — Secures its 200 domains with the shortest names.

Select an AutoSSL provider

To select an AutoSSL provider, perform the following steps:

1. Select the desired AutoSSL provider.
 - Select *disabled* to disable this feature.
2. If the AutoSSL provider requires that you accept their Terms of Service or other similar agreement, read the document and select the appropriate checkbox to agree to those terms.
3. If you need to reset your registration with the AutoSSL provider due to security issues, select the appropriate checkbox to agree to those terms and click *Reset Registration*.
4. Click *Submit*.

Note:

If the provider updates their Terms of Service, you may need to return to this interface to agree to them.

Enable AutoSSL

Users **must** use a package that includes the `autossl` feature to receive the free certificates. For more information about feature lists, read our [Feature Manager](#) documentation.

Feature list override

To override the feature settings and control whether AutoSSL is enabled for a user or users, perform the following steps:

1. Click the *Manage Users* tab to display a table of users on the server.
 - You can search and navigate the list of users with the navigation controls.
 - To set the feature on all domains, click *Enable AutoSSL on all users*, *Disable AutoSSL on all users*, or *Use Feature List for all users*.
 - To set the feature on multiple domains, select the appropriate checkboxes and click *Enable AutoSSL on selected users*, *Disable AutoSSL on selected users*, or *Reset AutoSSL for selected users*.
2. To enable or disable AutoSSL on a single domain, select the appropriate option:
 - *Enable AutoSSL* — Override the user's Feature List settings to enable AutoSSL.
 - *Disable AutoSSL* — Override the user's Feature List settings to disable AutoSSL.
 - *Reset to Feature List Setting* — Allow the user's Feature List settings to determine whether AutoSSL is enabled or disabled.

Notes:

- Because the system adds the `/etc/cron.d/cpanel_autoss1` cron daemon task to schedule the automatic provisioning of certificates, you may experience a delay between when you enable the feature and the installation of certificates. The interface displays the next time that the script will run.
- The system restarts Apache after AutoSSL provisions and installs certificates for all accounts during a nightly run.

Run AutoSSL

Click *Run AutoSSL for all users* at the top of the interface to run the AutoSSL feature for all users with the feature enabled.

To run the AutoSSL feature for a single user, click the user's *Check* button in the *Run AutoSSL Check* column of the table.

Review log files

To review AutoSSL log files, perform the following steps:

1. Click the *Logs* tab.
2. Select the log that you wish to view from the menu, and click *View Selected Log*.
3. Click *Refresh Logs List* to refresh the list of log files.

The system stores the log files in both text and JSON format in the `/var/cpanel/logs/autoss1` directory.

Frequently Asked Questions

How do I revoke a certificate?

We do not support the revocation of certificates through cPanel & WHM at this time.

Let's Encrypt won't issue a certificate for a virtual host list (website).

Let's Encrypt will only issue a certificate five times per week to a specific set of domains before it blocks any further certificates for that set of domains.

To work around this rate limitation, [create an alias to a domain](#) in the virtual host list (website) so that Let's Encrypt interprets the virtual host as a new set of domains.

Is Manage AutoSSL available for cPanel & WHM version 56?

That version of cPanel & WHM does not support deferred Apache and Dovecot configuration restarts, which results in unacceptable downtime and a poor customer experience. As such, we will not make the plugin available for version 56.