

HTTPS and Certificates

Version 1.0.0 | Updated 2026-09-05 | 1 min read

Existing service guidance

In this guide: [Before you start](#) | [Steps](#) | [Verify the result](#) | [Help and related information](#)

A valid certificate must cover the exact hostname visitors use. Never resolve a warning by disabling certificate verification.

Before you start

Use the access and features actually assigned to your account. Keep a rollback or recovery route before changing existing service settings.

Steps

1. Confirm DNS points to the correct approved host.
2. Use the existing certificate or AutoSSL controls available for the account; a paid certificate purchase is not assumed.
3. Check HTTPS for every intended hostname and ensure page resources also use HTTPS.
4. Verify renewal status and monitor expiry. Ask support if validation or renewal fails.

Verify the result

The browser accepts the certificate without exceptions and no required page content is loaded insecurely.

Help and related information

Contact support, service status, and Customer Access. Never send passwords or recovery codes.

Official cPanel documentation. Account features vary by hosting package.