




Track SSL Certificate Expirations Easily

mySites.guru checks every site's SSL certificate issuer, expiry date and full chain validity on every snapshot, alerting you before they expire.

Phil E. Taylor | 16 March 2026

 The screenshots below are from an older version of the interface. We've since redesigned the dashboard, but the process works the same way.

mySites.guru has checked SSL certificates on every site snapshot since 2012. It's one of those features that runs quietly in the background - you only notice it when something goes wrong and it catches the problem before your clients do.

When we snapshot your Joomla or WordPress site as part of our security audit, we download the active SSL certificate the same way a browser would. We check the SSL issuer, expiration date, and the full certificate validation chain to make sure all intermediate certificates are also valid.

SSL has a lot going on under the hood. We check the ciphers in use and the minimum encryption level your server accepts. If your site allows insecure encryption methods, we'll alert you by email.

We also distinguish cPanel and Let's Encrypt SSL Certificates as these are normally web host provided and auto-renewed without user intervention, these are shown with custom icons on your dashboard.



Let's Encrypt SSL Certificate

This site is using Let's Encrypt SSL Certificate, you need to ensure it is set for auto-renew as we dont alert because of the short issue periods

The background shows a dashboard with several site cards. Each card has a circular icon on the left and a refresh button on the right. The refresh buttons are orange with a white circular arrow and a number. The cards are: 1. cPanel icon, refresh 13. 2. Let's Encrypt icon (sun and padlock), refresh 9. 3. Let's Encrypt icon (sun and padlock), refresh 14. 4. PHP 7.3 icon (green), refresh 1.

Why are short expiration dates now standard?

Certificate lifetimes have been shrinking for years. What used to be a 2-5 year certificate is now often 90 days with Let's Encrypt. Auto-renewal handles this most of the time, but when it fails, browsers block your site for visitors entirely.

That's why mySites.guru shows you an overview of all your SSL certificates sorted by expiration date.

SSL Expiration Dates

[Export CSV](#)

Here are all your sites in our database with a https:// prefix to their urls, listed and ordered by the expiration date of their SSL Certificate. Sites at the top will expire first.

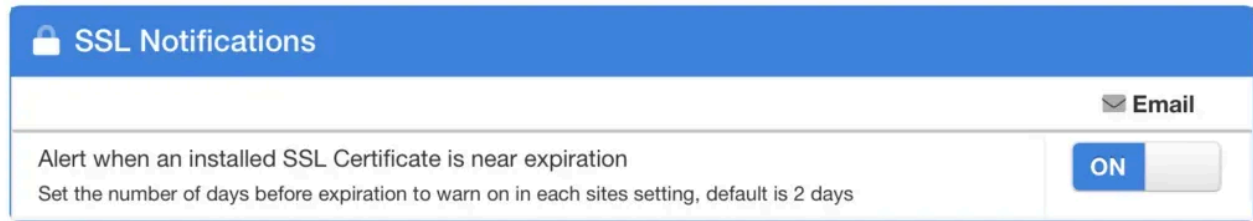
This information is updated during the daily snapshot.

 watchnotful.io		Issued By cPanel, Inc. Certification Authority - Expires: May 18 2020	Manage Site →
 example-tinytiger.com		Issued By cPanel, Inc. Certification Authority - Expires: May 18 2020	Manage Site →
 example-brownmouse.com		Issued By Let's Encrypt Authority X3 - Expires: Jun 01 2020	Manage Site →
 example-whitepanda.com		Issued By Let's Encrypt Authority X3 - Expires: Jun 01 2020	Manage Site →
 example-greenfish.com		Issued By Let's Encrypt Authority X3 - Expires: Jun 03 2020	Manage Site →

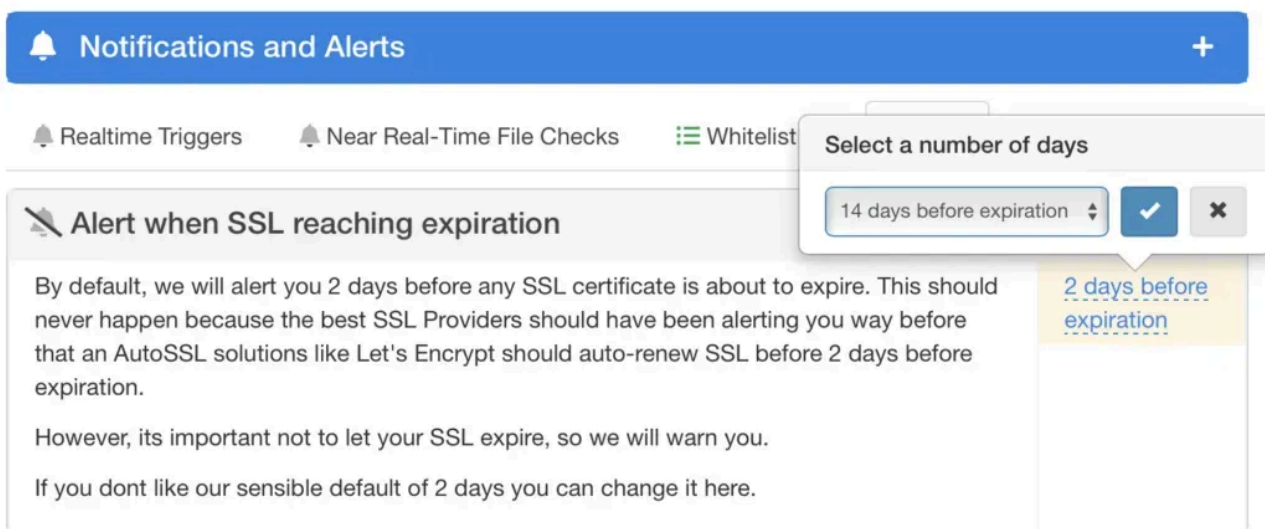
On this screen you can also export the list to CSV file for further offline processing should you wish.

How do expiry alerts work?

By default, mySites.guru alerts you when a certificate gets within 2 days of expiry. For most sites with auto-renewal that threshold should never trigger - but it's there as a safety net.



If your renewal process requires more lead time, you can configure how many days in advance you want the alert.



What about Qualys SSL Labs integration?

[Qualys SSL Labs](#) is the standard tool for testing SSL implementation in depth. mySites.guru links directly to it from the Learn More page in the [SSL Snapshot tool](#).

😊 Our Recommendation

We highly recommend that you install, and keep current, a valid SSL certificate and serve all assets over a `https://` prefixed connection

There has been a huge push recently to secure the web, and its now expected by Google and your customers that all sites should be secured with an SSL Certificate

Although this tool doesnt check the validity of your installed certificate, the fact that you can connect from our service to your site over `https://` prefixed domain name, indicates your certificate is installed correctly as we refuse to connect to a site with an invalid, expired or badly installed certificate.

If you would like to test your installation you can use the awesome tool at Qualys for this purpose.

[Test SSL Connection with Qualys Tool](#)

The most common issue with SSL Certificates is either expired and not renewed certificates, or incorrectly installing the complete chain (bundle) of certificates, or including the root certificate (which you should never do). The tool at Qualys will tell you if any of these apply to you.

It gives you detailed technical information about your SSL configuration and your web server's security posture.

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1



Subject	withlovemelissax.com Fingerprint SHA256: bb9e5d1ecca63b14f3ea8398a3572f640d39546e5529b952278cb9c5c8053f72 Pin SHA256: LcdQT1evRMx5Ewqj0dSlcUWghN5Yv03g9FYCpTC0hc=
Common names	withlovemelissax.com
Alternative names	withlovemelissax.com cpanel.withlovemelissax.com cp calendars.withlovemelissax.com cpcontacts.withlovemelissax.com mail.withlovemelissax.com webdisk.withlovemelissax.com webmail.withlovemelissax.com www.withlovemelissax.com
Serial Number	00b40b2622785a7bab061ef48822e87545
Valid from	Tue, 18 Feb 2020 00:00:00 UTC
Valid until	Mon, 18 May 2020 23:59:59 UTC (expires in 1 month and 4 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	cPanel, Inc. Certification Authority AIA: http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Revocation information	CRL, OCSP CRL: http://crt.comodoca.com/cPanelIncCertificationAuthority.crl OCSP: http://ocsp.comodoca.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)



Certificates provided	3 (4646 bytes)
Chain issues	None
#2	
Subject	cPanel, Inc. Certification Authority Fingerprint SHA256: 821cc55ce7ec5c74febb42f624eb6a36c478215a31ed67e3cf723a67e8c75eba Pin SHA256: hOF1upiO+xevnDEQ13g3aY3M3Uqa44RN5rVlvwU2WC8=
Valid until	Sat, 17 May 2025 23:59:59 UTC (expires in 5 years and 1 month)
Key	RSA 2048 bits (e 65537)
Issuer	COMODO RSA Certification Authority
Signature algorithm	SHA384withRSA
#3	
Subject	COMODO RSA Certification Authority Fingerprint SHA256: 4f32d5dc00f715250abcc488511e37f501a899deb3b77ea8adbbd3aef1c412da Pin SHA256: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvpLg5yRME=
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 1 month and 16 days)
Key	RSA 4096 bits (e 65537)
Issuer	AddTrust External CA Root
Signature algorithm	SHA384withRSA

SSL tracking is covered in our [monitoring and alerting guide](#).

Frequently Asked Questions

How does mySites.guru monitor SSL certificates?

On every site snapshot, mySites.guru downloads the active SSL certificate and checks the issuer, expiration date, and the full certificate chain for validity.

How far in advance will mySites.guru alert me before an SSL certificate expires?

By default you're alerted 2 days before expiry, but this threshold is configurable so you can get earlier warnings if your renewal process requires more lead time.

Can I see all my SSL certificate expiry dates in one place?

Yes - mySites.guru provides an overview screen listing all connected sites sorted by certificate expiration date, with an option to export the list to CSV.


Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.
No credit card required.

<https://manage.mysites.guru/en/register>

Get in touch

Phil E. Taylor
phil@phil-taylor.com



mySites.guru

© 2026 Blue Flame Digital Solutions Limited. All rights reserved.

mysites.guru

