

Recent change Root Certificate from Sectigo CA (June 2025)

This documentation is to inform about a recent change made by our SSL certificate supplier Sectigo that may be causing issues with your SSL certificates.

Sectigo is currently migrating to **new public root Certificate Authorities (CAs)** as part of a global infrastructure upgrade. This change aims to improve longterm compatibility and security but may temporarily affect some systems that do not yet recognize the new root certificates.

What does this mean for you?

Some SSL-secured services may experience trust warnings certificate errors or unexpected behavior especially on older devices, systems, or applications that have not updated their root certificate store.

You can read more about the migration directly on Sectigo's official page:

☐ [Sectigo Public Root CAs](#) Migration

You can find additional root and intermediate certificates to install [via this link](#):

We're on it!

Our team is actively working with Sectigo to ensure a smooth transition and to minimize any disruptions. We're also updating relevant systems and providing necessary documentation to help affected customers resolve issues as quickly as possible.

What you can do:

Ensure your servers and clients are using up-to-date operating systems and trust stores.

If you are seeing issues, add the new intermediate certificate.

- Domain Validated (DV) - [new_intermediate_DV.crt](#)
- Extended Validation (EV) - [new_intermediate_EV.crt](#)

- Organization Validated (OV) - [new_intermediate_OV.crt](#)

Use intermediate certificate based on "[Type of certificate](#)" you have selected you have. For example, if you have a Domain Validated (DV) certificate, use [new_intermediate_DV.crt](#).

We appreciate your patience and understanding during this transition.

Revision #2

Created 2026-08-07 14:51:03 UTC by Sarath

Updated 2026-08-07 16:00:24 UTC by Sarath