My domain certificate is untrusted after the May 30th

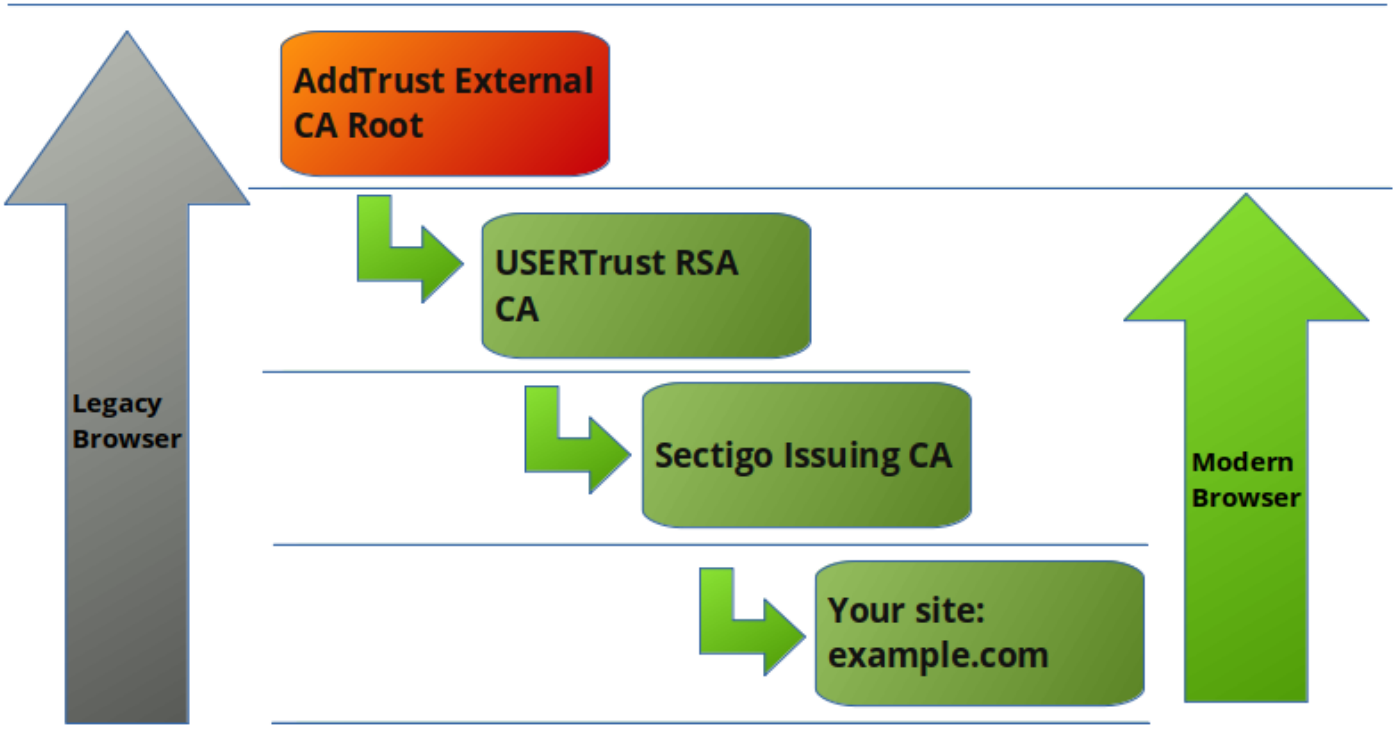
Question:

After the 30th of May 2020, my website certificate becomes untrusted. Why and how to fix that?

Answer:

On May 30, 2020, 10:48:38 +0000 root certificate "**AddTrust External CA Root**" and intermediate certificate "**USERTrust RSA Certification Authority**" expired.
That could impact leaf certificates validation on outdated systems.

Modern browsers are not affected by the expiration since they automatically switch to the new SHA-2 root (Comodo or USERTrust).



If your service meets one of the following conditions, it may be affected:

- Your application is set up to explicitly trust **Addtrust External CA Root** ;
- Your service is using the expired Root certificate and is being accessed by applications other than browsers (e.g. API, cURL, OpenSSL, etc.) ;
- Your service is using an application that has not received security updates since mid-2015 ;
- Your service is using an application with broken certificate path validation (e.g. OpenSSL, OpenLDAP, Postfix) ;

If your service uses one of the affected applications regardless of the Root certificate installed, you should update the settings of the affected application.

Follow this guide to check if your service is using the expired Root:

- Start **OpenSSL**

  ```
  openssl s_client -connect remote.host:443
  ```

  where "**remote.host**" equals your domain name ;
- If you see**AddTrust External CA Root**as**CN**, please follow the next steps.
  Otherwise, the service is not affected by the issue.

```
sserdyuk@thinkpad:~$ openssl s_client -connect [redacted]:443
CONNECTED(00000005)
depth=2 C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Certification Authority
verify return:1
depth=1 C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Domain Validation Secure Server CA
verify return:1
depth=0 OU = Domain Control Validated, OU = PositiveSSL Wildcard, CN = [redacted]
verify return:1
---
Certificate chain
 0 s:OU = Domain Control Validated, OU = PositiveSSL Wildcard, CN = [redacted]
   i:C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Domain Validation Secure Server CA
 1 s:C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Domain Validation Secure Server CA
   i:C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Certification Authority
 2 s:C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Certification Authority
   i:C = SE, O = AddTrust AB, OU = AddTrust External TTP Network, CN = AddTrust External CA Root
---
```

To fix any issue reinstall root and intermediate certificates bundle.
Check your "**Issuer Common Name**" using OpenSSL

```
OH6x1Yk1+9GiV8axQbUdawjFANw8/SSN3qxon0U+2orrXybO1Cl3/Mn2256JDOrq
TJPKA9NlMXZwlou20udCD4Ue+TsD5/7PdRxORqIH2zSglHN7ULYbpTSbLVRuDoht
fzsiJ0gJbfXHgPwDZTYZ5etWk8tkk6j1s3M6JeXp84o=
-----END CERTIFICATE-----
subject=OU = Domain Control Validated, OU = EssentialSSL, CN = hatsuseno.org

issuer=C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Domain Validation Secure Server CA

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: ECDH, P-384, 384 bits
---
SSL handshake has read 6631 bytes and written 775 bytes
```

Depending on your current vendor use following root and intermediates (updated 03.06.2020):

Product	Domain Validation	Organization Validation	Extended Validation
Comodo	root | int	root | int	root | int
Sectigo	root | int	root | int	root | int
Sectigo with AAA root (for legacy devices)	root | int	root | int	root | int

Revision #2
Created 2026-08-07 14:40:33 UTC by Sarath
Updated 2026-08-07 15:55:22 UTC by Sarath