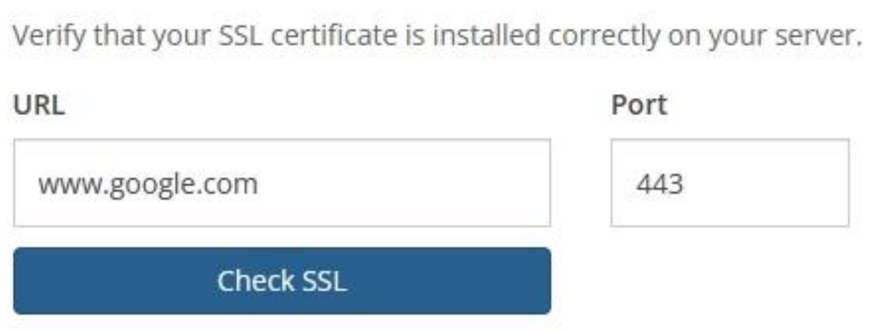
How can we check for validation of a SSL Certificate also check validity of Chain of Trust between the Intermediate Certification Authorities and the Certificate of the website or web server.

Following is the website that will do the above job.



Verify that your SSL certificate is installed correctly on your server.

URL: www.google.com

Port: 443

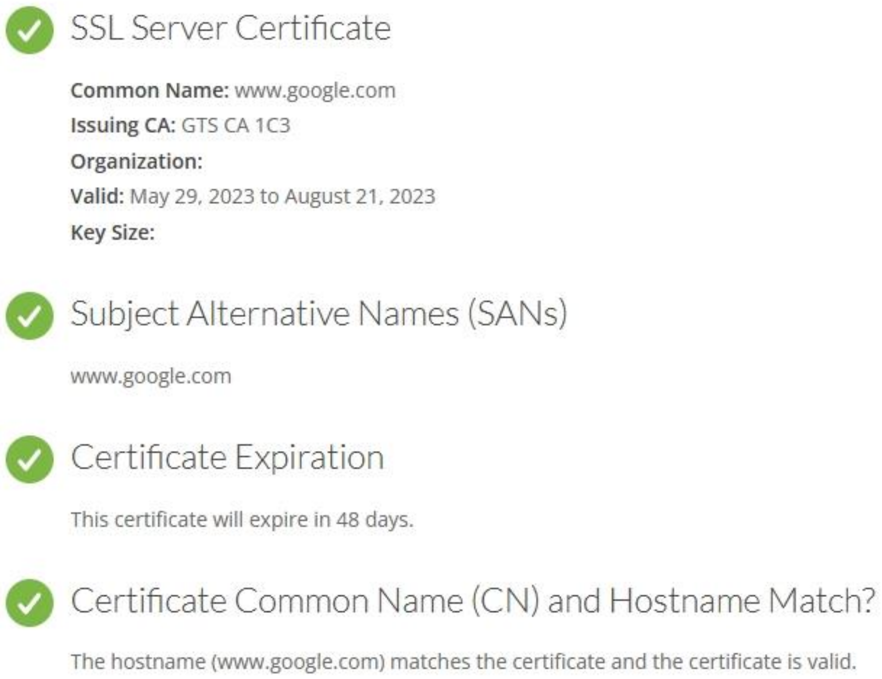
Now Click on Check SSL

If the web server will be having a valid SSL Certificate you will get details about the certificate

like

- Certificate Issuing Root Authority
- Intermediate Chain of Trust
- Certificate details of web server
- Encryption Algorithms used
- Expiration Date Details of the Certificate

Following are some screenshots of the Output



✓ SSL Server Certificate

Common Name: www.google.com
Issuing CA: GTS CA 1C3
Organization:
Valid: May 29, 2023 to August 21, 2023
Key Size:

✓ Subject Alternative Names (SANs)

www.google.com

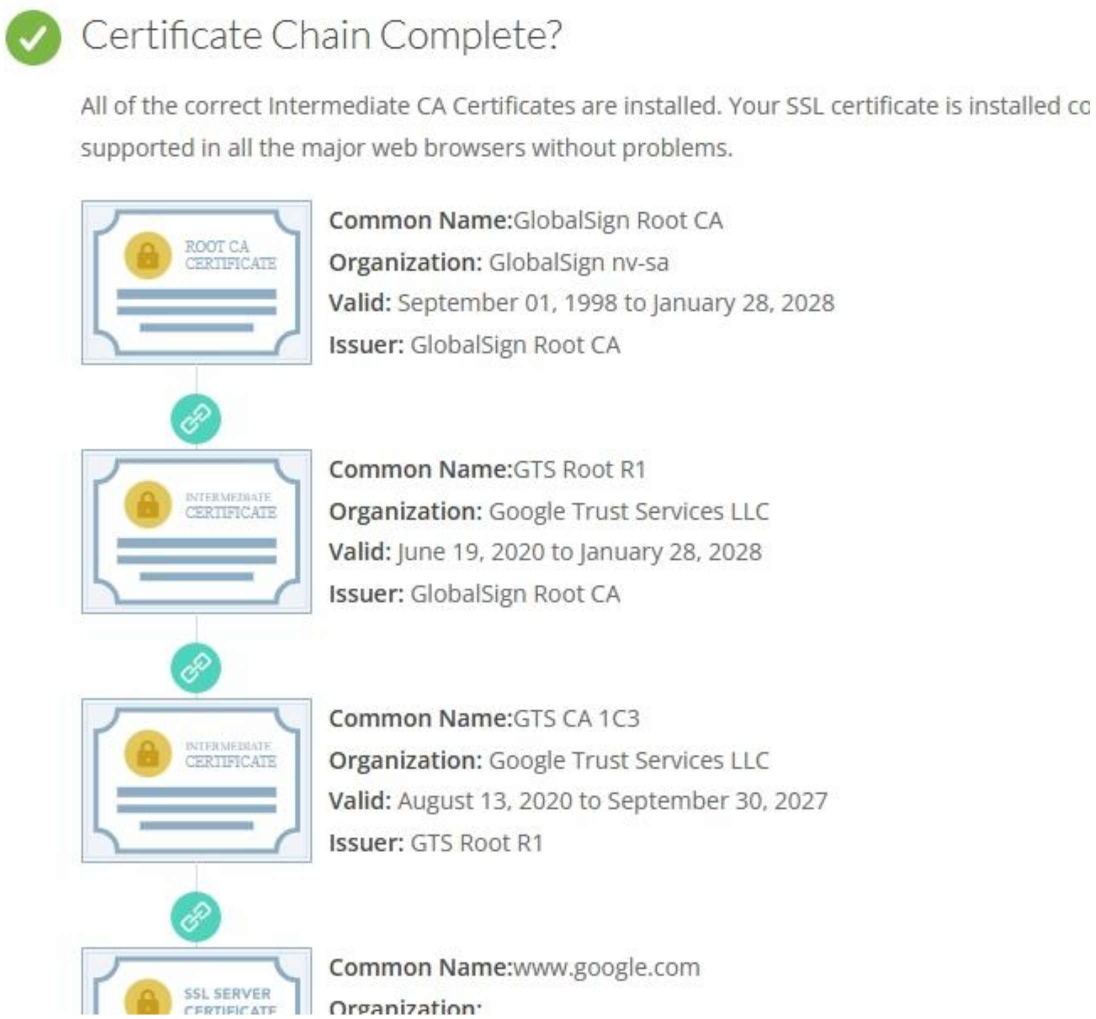
✓ Certificate Expiration

This certificate will expire in 48 days.

✓ Certificate Common Name (CN) and Hostname Match?

The hostname (www.google.com) matches the certificate and the certificate is valid.

Following are the details about validity of Chain of Trust



Certificate Chain Complete?

All of the correct Intermediate CA Certificates are installed. Your SSL certificate is installed co supported in all the major web browsers without problems.

Common Name: GlobalSign Root CA
Organization: GlobalSign nv-sa
Valid: September 01, 1998 to January 28, 2028
Issuer: GlobalSign Root CA

Common Name:GTS Root R1
Organization: Google Trust Services LLC
Valid: June 19, 2020 to January 28, 2028
Issuer: GlobalSign Root CA

Common Name:GTS CA 1C3
Organization: Google Trust Services LLC
Valid: August 13, 2020 to September 30, 2027
Issuer: GTS Root R1

Common Name:www.google.com
Organization: