Steps to Verify Certificate Installation

To determine whether you need to import the new intermediate or root certificate, you can list the existing certificate in your truststore or keystore. If you are using Linux servers, follow these steps:

1) Navigate to your keystore / truststore location in your application server
2) Enter command: keytool -list -v -keystore **your_keystore_name** > /tmp/certificates_list.txt (Enter your password when prompted)
3) Open /tmp/certificates_list.txt and validate if below certificate details are already present.

   GS_Chain.cer which is intermediate certificate , serial number : 01ee5f221dfc623bd4333a8557 , valid from : Wednesday, November 21, 2018 8:00:00 AM , valid to : Tuesday, November 21, 2028 8:00:00 AM ,
   CN = GlobalSign RSA OV SSL CA 2018
   GS_Root.cer which is root certificate , serial number : 040000000001215853 08a2, valid from Wednesday, March 18, 2009 6:00:00 PM, valid to : Sunday, March 18, 2029 6:00:00 PM, CN = GlobalSign

Alternatively, you may use GUI-based tools such as Keystore Explorer to inspect your truststore or keystore.

PS: If the certificates are already present then you do not need to import them to your truststore or keystore.