Configuring Certificate Revocation Validation

A certificate that is issued by a Certificate Authority (CA) is expected to be in use for its entire validity period. However, certain circumstances may cause a certificate to become invalid prior to the expiration of the validity period, e.g., a compromise or suspected compromise of the corresponding private key. Under such circumstances, the issuing CA needs to revoke the certificate prior to the scheduled expiry date so that the certificate would longer be trusted.

Certificate Revocation List (CRL) and OCSP (Online Certificate Status Protocol) are two protocols that are used to check whether a given X509 certificate is revoked by its issuer.

- **CRL** is a list of digital certificates that have been revoked by the issuing CA.
- **OCSP** is an internet protocol that is used for obtaining the revocation status of an X509 digital certificate using the certificate serial number.

WSO2 X509 authenticator, which perms client X509 certificate authentication supports certificate validation with CRL and OCSP. At the verification phase of the SSL handshake, OSCP/CRL certificate verification process is used to contact the relevant CA to verify the validity of the given certificate. If the response states that the certificate is revoked, it indicates that the certificate is no longer trusted by the CA, i.e., the SSL connection to the peer is terminated.

To learn about configuring the X509 certificate authenticator, see Configuring X509Certificate Authenticator.

Explore the following sections below to configure CRL and OCCP for certificate validation.

**Before you begin**

Locate the `<IS_HOME>/repository/conf/security/certificate-validation.xml` file and open in a text editor.

Example: