Certificate Monitoring and Revocation with OCSP

First Published: January 8, 2020

It's important to manage certificate requirements by keeping track of certificates that are approaching expiry, and by revoking expired certificates. Cisco Collaboration Systems offers tools to confirm certificate validity so that your security cannot be compromised due to trust established by invalid certificates:

- Certificate expiration monitoring – Cisco Unified Communications Manager and the IM and Presence Service can be configured to check certificates periodically and email you when a certificate is approaching expiry. This helps you to replace certificates proactively before they expire.
- Certificate revocation via the Online Certificate Status Protocol (OCSP)–OCSP provides an online method for checking certificate validity and revoking certificates automatically as they expire. This ensures that invalid certificates cannot be used to establish trust.

NOTE: Certificate expiration checking is not a substitute for revocation checks. A certificate that has not expired can become revoked. For example, this could happen if a certificate were issued in error and then later cancelled. Certificate revocation checks would catch this, but certificate expiration checks would not.

Certificate Revocation Checking with OCSP

The Online Certificate Status Protocol (OCSP) is an online mechanism for checking certificate validity and revoking expired certificates. An OCSP request that includes the certificate serial number, is sent to an OCSP responder, whom responds with the certificate status (good, revoked, or unknown).

- OCSP provides an alternative to Certificate Revocation Lists (CRLs) with the following benefits over CRLs:
- Less bandwidth and network resources required than CRLs
- Allows the network administrator to specify a central OCSP server, which can service all devices within a network.
- Allows the network administrator the flexibility to specify multiple OCSP servers, either per client certificate or per group of client certificates.
- OCSP server validation is usually based on the root CA certificate or a valid subordinate CA certificate, but may also be configured so that external CA certificates or self-signed certificates may be used. Using external CA certificates or self-signed certificates allows the OCSP servers certificate to be issued and validated from an alternative PKI hierarchy.

A network administrator can configure an OCSP server to collect and update CRLs from different CA servers. The devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every peer. When peers have to check the revocation status of a certificate, they send a query to the OCSP server that includes the serial number of the certificate in question and an optional unique identifier for the OCSP request, or a nonce. The OCSP server holds a copy of the CRL to determine if the CA has listed the certificate as being revoked; the server then responds to the peer including the nonce. If the nonce in the response from the OCSP server does not match the original nonce sent by the peer, the response is considered invalid and certificate verification fails. The dialog between the OCSP server and the peer consumes less bandwidth than most CRL downloads.

If the OCSP server is using a CRL, CRL time limitations will be applicable; that is, a CRL that is still valid might be used by the OCSP server although a new CRL has been issued by the CRL containing additional certificate revocation information. Because fewer devices are downloading the CRL information on a regular basis, you can decrease the CRL lifetime value or configure the OCSP server not to cache the CRL. For more information, check your OCSP server documentation.

Certificate Monitoring and Revocation Tasks

The following table outlines how to configure your Cisco Collaboration products for TLS 1.2.

Table 1. Certificate Monitoring and Revocation Tasks

	Task	Description
Step 1	Configure Certificate Monitor Notifications for Unified CM	Configure Cisco Unified Communications Manager and the IM and Presence Service to monitor certificate expiry dates and to email the administrator when certificates are close to expiry.
Step 2	Configure OCSP Revocation Checks for Unified CM	Configure Cisco Unified Communications Manager and the IM and Presence Service to use OCSP to check certificate validity, and to revoke expired certificates.
Step 3	Configure OCSP Revocation Checks for Expressway	Configure Expressway to use OCSP for certificate checking and revocation.
Step 4	Configure OCSP Revocation Checks for Cisco Meeting Server	Configure Cisco Meeting Server to use OCSP for certificate checking and revocation.
Step 5	Configure OCSP Revocation Checks for CUBE	Configure a Cisco Unified Border Element (CUBE) to use OCSP for certificate checking and revocation.
Step 6	Configure OCSP Revocation Checks for IOS Infrastructure	Configure the IOS network infrastructure to use OCSP to monitor and revoke expired certificate

Configure Certificate Monitor Notifications for Unified CM

Configure Cisco Unified Communications Manager and the IM and Presence Service to use automated certificate monitoring for Unified Communications Manager or the IM and Presence Service. The system monitors certificate expiry and emails you when a certificate is approaching expiration.

NOTE: Certificate expiry notifications are not a replacement for revocation checking. A certificate can be revoked prior to its expiry date such as might occur when a certificate is issued in error and then voided prior to the expiration date.

NOTE: The Cisco Certificate Expiry Monitor network service must be running. This service is enabled by default, but you can confirm the service is running in Cisco Unified Serviceability by choosing Tools > Control Center – Network Services and verifying that the Cisco Certificate Expiry Monitor Service status is Running.

1. Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate monitoring) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate monitoring).
2. Choose **Security > Certificate Monitor**.

3. In the **Notification Start Time** field, enter a numeric value. This value represents the number of days before certificate expiration where the system starts to notify you of the upcoming expiration.
4. In the **Notification Frequency** fields, enter the frequency of notifications.
5. Optional. Check the **Enable E-mail notification** check box to have the system send email alerts of upcoming certificate expirations.
6. Check the **Enable LSC Monitoring** check box to include LSC certificates in the certificate status checks.
7. In the **E-mail IDs** field, enter the email addresses where you want the system to send notifications. You can enter multiple email addresses separated by a semicolon.
8. Click **Save**.

NOTE: The certificate monitor service runs once every 24 hours by default. When you restart the certificate monitor service, it starts the service and then calculates the next schedule to run only after 24 hours. The interval does not change even when the certificate is close to the expiry date of seven days. It runs every 1 hour when the c

Configure OCSP Revocation Checks for Unified CM

Configure Cisco Unified Communications Manager and the IM and Presence Service to use the Online Certificate Status Protocol (OCSP) to check certificate status regularly and to revoke expired certificates automatically

Before you begin

Make sure that your system has the certificates that are required for OCSP checks. You can use Root or Intermediate CA certificates that are configured with the OCSP response attribute or you can use a designated OCSP signing certificate that has been uploaded to the tomcat-trust.

1. Log in to Cisco Unified OS Administration (for Unified CM certificate revocation) or Cisco Unified CM IM and Presence Administration (for IM and Presence Service certificate revocation).
2. Choose **Security > Certificate Revocation**.
3. Check the **Enable OCSP** check box, and perform one of the following tasks:
   - If you want to specify an OCSP responder for OCSP checks, select the Use configured OCSP URI button and enter the URI of the responder in the OCSP Configured URI field.
   - If the certificate is configured with an OCSP responder URI, select the Use OCSP URI from Certificate button.
4. Check the **Enable Revocation Check** check box.
5. Complete the **Check Every** field with the interval period for revocation checks.
6. Click **Save**.
7. Optional. If you have CTI, IPsec or LDAP links, you must also complete these steps in addition to the above steps to enable OCSP revocation support for those long-lived connections:
   a. From Cisco Unified CM Administration, choose **System > Enterprise Parameters.**
   b. Under **Certificate Revocation and Expiry**, set the **Certificate Validity Check** parameter to **True**.
   c. Configure a value for the **Validity Check Frequency** parameter.

      NOTE: The interval value of the **Enable Revocation Check** parameter in the Certificate Revocation window takes precedence over the value of the **Validity Check Frequency** enterprise parameter.

   d. Click **Save**.

Configure OCSP Revocation Checks for Expressway

Cisco Expressway can be configured to use OCSP to complete revocation checks for SIP TLS certificates. Expressway-E sends and receives OCSP responses on ports 80 and 443. Expressway sends the request to the responder URI as specified by the certificate to be checked.

Supported for SIP TLS only. No need to download Certificate Revocation Lists

1. In Cisco Expressway, go to **Configuration > SIP**.
2. Select the **Use OCSP** option.
3. In **Fallback behavior**, configure the behavior if the OCSP response is Unknown. For example, *Treat as revoked* or *Treat as not revoked*.

NOTE: You can also configure OCSP checks via the following xConfiguration commands:

- Run the following command: **xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: On**
- Run the following command: **xConfiguration XCP TLS Certificate CVS UseOcsp: On**

TIP: Consider increasing the TLS handshake timeout to mitigate the effects of slow OCSP responses.

Configure OCSP Revocation Checks for Cisco Meeting Server

You can configure a Cisco Meeting Server to use OCSP for certificate revocation checking. There are two separate configuration process: one for SIP and LDAP TLS connections and a second process for Common Access Card (CAC) certificate checking.

For SIP and TLS connections, you can configure OCSP via the **tls <sip|ldap> verify enable|disable oscp** command

1. Log in to the MMP interface.
2. To enable OCSP for SIP connections, run the **tls sip verify ocsp** command
3. To enable OCSP for LDAP connections, run the **tls ldap verify ocsp** command.

To configure OCSP for Common Access Card (CAC):

1. Log in to the MMP interface
2. Run the **cac ocsp enable** command
3. Optional. Configure a specific OCSP responder with the **cac ocsp responder <URL>** command. This command overrides any OCSP responder designated within the certificate.
4. Refer to the following table for additional optional commands:

MMP Command	Description
cac enable|disable [strict]	Enables/disables CAC mode with optional strict mode removing all password-based logins
cac issuer <ca-cert-bundle>	Identifies trusted certificate bundle to verify CAC certificates
cac ocsp certs <keyfile> <certificatefile>	Identifies certificate and private key for TLS communications with OCSP server, if used

cac ocsp responder <URL>	Identifies the URL of the OCSP server
cac ocsp enable|disable	Turns OCSP checks Ton or off

Configure OCSP Revocation Checks for CUBE

A Cisco Unified Border Element (CUBE) can be configured to use OCSP revocation checking for TLS connections. When configuring TLS on CUBE, run the following command:

revocation-check ocsp

For additional details on configuring TLS connections on CUBE, refer to "How to Configure SIP TLS Support on CUBE" in the *Cisco Unified Border Element Configuration Guide*

Configure OCSP Revocation Checks for IOS Infrastructure

When configuring PKI Integration for IOS Network Infrastructure, you can configure OCSP revocation checks for IPSec network connections (Cisco IOS XE).

NOTE: OCSP requests and the corresponding OCSP response by default include a unique identifier (a nonce). The use of a nonce offers a more secure and reliable communication channel between the peer and OCSP server. However, you can disable the usage of a nonce with the ocsp disable-nonce command.

In your IOS configuration, run the following commands:

1. Router(config)# crypto pki trustpoint mytp – specifies the name of the trustpoint
2. Router(ca-trustpoint)# ocsp url http://myocspserver:81 – specifies the URL of the OCSP server
3. Router(ca-trustpoint)# revocation-check ocsp –specifies OCSP as the prime revocation method.
4. Router(ca-trustpoint)# ocsp disable-nonce – Optional. This command disables the usage of a nonce for revocation checking.

Example:

The following example shows an IOS configuration for trustpoint mytp. OCSP is used with CRLs as a backup method if OCSP checks return an unknown status. This configuration includes the optional disablement of a nonce between the OCSP request and response.

1. enable
2. configure terminal
3. crypto pki trustpoint mytp
4. ocsp url http://myocspserver:81
5. revocation-check ocsp crl none
6. ocsp disable-nonce
7. exit
8. exit
9. show crypto pki certificates
10. show crypto pki trustpoints [status | label [status]]

NOTE: With the revocation-check command, you can configure OCSP along with two backup methods that can be used if the OCSP check returns an unknown response. The above command specifies CRLs as the first backup method. If CRL checks fail to return the status, the none option is used, which ignores revocation checks and assumes the certificate is valid. If you wanted the fallback method to assume the certificate is invalid, do not include the none method.

For detailed information on how to configure PKI Integration with a AAA Server, refer to the "Configuring Authorization and Revocation of Certificates in a PKI" chapter of the *Cisco IOS XE Security Configuration Guide*.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.