CRL Monitor

Table of Contents

Why ADSS CRL Monitor may not start?

By default, CRL Monitor remains stopped when there are no registered CAs in Trust Manager OR if one or more CAs are registered but none of them have enabled the option to "Enable automated polling".
To start CRL Monitor,

1. Register at least one CA within Trust Manager.
2. In at least one CA tick the "Enable automated polling" check box from Trust Manager > CRL Settings.
3. Start the CRL Monitor > Service Manager.

How to configure a new CA in CRL Monitor?

These are the high level steps required to configure a new CA for CRL monitoring:

- Register the CA certificate in the Trust Manager module with the purpose "CA (will be used to verify other certificates and CRLs)".
- Configure the appropriate CRL resource addresses using HTTP(S) or LDAP(S) protocols (these addresses can be automatically read from an issued certificate) and also enable polling for this CA, see **Trust Manager** for details.
- Restart the CRL Monitor service from **CRL Monitor > Service Manager** if this is the first CA being registered in Trust Manager; or you can go to the **CRL Monitor > CRL Monitoring** page and start polling for the new CA if the CRL Monitoring service is already running and polling for CRLs for some of the configured CA(s).

Why might ADSS CRL Monitor not download CRLs for a configured CA?

ADSS CRL Monitor can only fetch CRLs when the configuration details are correct. Check the following configurations:

1. Test the connection using internet/ LDAP browser to ensure configured HTTP(S)/ LDAP(S) address is working properly, see Trust Manager > CRL Settings.
2. If ADSS CRL Monitor is running behind a proxy server, then configure an appropriate proxy settings, see Global Settings > Miscellaneous .
3. Ensure that the SSL Server certificate issuer (for the server where the CRL is published) is registered in Trust Manager with the purpose "CA (will be used to verify other certificates and CRLs)".
4. Browse CRL Monitor > CRL Details to see whether a new CRL was received or not?
5. Browse CRL Monitor > CRL Logs to see the processing of ADSS CRL Monitor for the relevant CA.
6. View the log file from "Help > Debug Logs > service > crlmanager > crlmanager.log" to get an idea of the problem being encountered.

If you have made any configuration changes then ensure the Windows services/ Unix daemons are restarted after registering the issuer of an SSL Server authentication certificate in Trust Manager.

However, if you still face any problem, then contact support with the following information:

- Version of ADSS Server being used in your environment.
- A description of what action was performed, what was expected and what was experienced.
- The log files within "[ADSS-Server-Installation-Directory/logs/service/crlmanager]".
- A screenshot of the CRL polling configurations in Trust Manager > CRL Settings.
- Details of the CA for which CRL polling is unsuccessful (including the CA's certificate, CRL address and information like whether the CRL is publicly available).

What is meant by CRL Monitor High Availability?

In a load-balanced configuration there are two or more server instances handling front-end services such as the OCSP Service. The background task of CRL polling, i.e. retrieving CRLs from online repositories should be performed by only one instance of CRL Monitor. This is because if several CRL Monitor instances were polling for CRLs they would simultaneously download and attempt to process the same CRL, which is obviously pointless. However this leads to a potential situation where the CRL Monitor instance which is retrieving CRLs (referred to as the "*Master*") can become a single point of failure. If this instance fails then polling for CRLs will not be conducted by any other instance. To overcome this issue, the CRL Monitor implements a high availability option such that if the master instance fails (e.g. the server fails), then another CRL Monitor can automatically promote itself to *Master* and take over the responsibility for CRL polling. See CRL Monitor > High Availability for more details.

How to run CRL Monitor in a High Availability configuration?

In order to run more than one CRL Monitor instances in a high availability configuration, install them using the load-balance installation type and during the installation provide the database information for the same database which is already configured with a CRL Monitor instance. During the load-balanced installation, CRL Monitor is automatically configured in high availability mode. See CRL Monitor > High Availability for more details.

Are very large CRLs (e.g. 10MB or more) supported by ADSS Server?

Yes large CRLs of 10MB or more are supported by ADSS Server. Your should ensure that sufficient memory and disk space are available on both the ADSS Server machine and the database system. 1GB of Java memory is adequate to handle 10MB CRLs. Within ADSS Server there is a maximum limit of 1 MB for PEM encoded CRLs and any that exceed this limit are rejected. This is because PEM encoded CRLs consume a lot of system memory, however CRLs are rarely encoded in PEM format because they are much larger in size than normal DER format.

Does ADSS Server support X.509 v1 and v2 CRLs, PEM encoded CRLs or indirect CRLs?

Yes all of these CRL formats are supported.

What is the difference between Logs Archiving settings provided in Trust Manager and CRL Logs?

Logs archiving settings provided in Trust Manager are used for archiving the old CRLs downloaded for the configured CAs. See **Trust Manager** f or more details. The Logs Archiving page within the CRL Monitor module is used to archive the CRL Monitoring Logs. See **CRL Monitor > Logs Archiving** for more details.

Does ADSS Server support segmented CRLs? How can these be imported?

Reason based segmented CRLs are supported by the ADSS CRL Monitor module. Like normal (full) CRLs the segmented CRLs can also be imported either using automatic CRL Monitoring or through manual import. See **Trust Manager > Configure CRL Settings** for details on configuring polling of segmented CRLs. See **CRL Monitor > CRL Details** to learn how to manually import the segmented CRLs for a CA.

How to implement real time revocation?

When a certificate status is updated (revoked, suspended or reinstated), the CA does not publish the CRL right away. The publishing of CRL is

usually scheduled after defined (configurable) intervals, according to the CA's CRL publishing policy. This means that there could be a possible time delay between a certificate being revoked, and the availability of revocation information to the relying parties (unless the CRLs are issued immediately upon every revocation, which is not a common practice).

In the up-mentioned scenario, when a certificate revocation status is updated right after the publication of the CRL, its information will not be updated in the ADSS Server database, until the next CRL is successfully processed by ADSS Server. This implies, if ADSS Server receives a signature/ certification/ OCSP request within that time period, the revocation status will be determined on the basis of the current valid CRL, however, the actual status could be different.

To cope with this potential scenario, ADSS Server provides the real-time revocation information feature within ADSS CRL Monitor, i.e. Revocation Publishing Utility (RPU). This utility can work in two different ways:

1. **For UniCERT CAs:** The UniCERT CA generates a (.rev) file upon performing any change activity in the certificate status, and saves this file on a shared location. The RPU is configured to monitor the shared location, and immediately process the (.rev) file on arrival, and save the processed information in the RPU database.
2. **For other CAs:** The CA does not generate (.rev) file for each change in certificate status, but directly triggers this information in the RPU database.

Now when ADSS Server receives a signature/ certification/ OCSP request, it will first check the current valid CRL (in ADSS database) and will then look into the RPU database (if certificate status is good or on hold), before determining the certificate status. This configuration can be set from Global Settings> Real Time Revocation

How to change the CRL polling schedule from polling on nextUpdate to polling at a configurable period?

Whenever the CRL polling schedule is changed for an existing CA, such that the polling should be performed at configured intervals instead of the CRL nextUpdate, then the time for the CRL Next Fetch does not automatically change. This happens because the value for the Next Fetch field was previously set to be same as the CRL nextUpdate every time a new CRL arrived. Upon performing the above mentioned update operation the value for NextFetch is already set to the CRL nextUpdate for the current CRL and polling will be performed at that time for the first time after the update has been performed. To overcome this situation, it is required to manually alter the Next Fetch value along with the actual update operation. CRL polling for this CA should then be restarted from the CRL Monitor > CRL Monitoring page. Click here for details of CRL Polling configurations.

How to reset the CRL information for a CA before moving from a pre-production environment into production?

Whenever a CA is registered in a pre-production environment, it may be required to remove any CRLs which were downloaded before moving into the production environment. This can be achieved by going to the CRL Monitor module > CRL Details > View CRLs for a specific CA > and on the View CRLs page click the "Remove All CRLs" button. This button will not be available in a case when CRL polling is turned on for a registered CA. Therefore it is necessary to turn off CRL polling from the Trust Manager > Configure CRL Settings page before resetting CRLs for a registered CA.

How to configure ADSS Server to only retain the latest CRL and drop old CRLs for the registered CAs?

By default ADSS Server keeps a history of all the CRLs downloaded for a registered CA. The historic CRLs are sometimes required for historical digital signature verification or historical validation of the digital certificates. If historical validation is not required in an ADSS Server environment then storage of the historic CRLs is an unnecessary load on the ADSS Server database. You can turn off the option "Keep Old CRLs" on the Trust Manager > Configure CRL Settings page in the CRL Handling area. Find more details on the CRL configurations here.

How are segmented CRLs different from partitioned CRLs?

Segmented CRLs and partitioned CRLs are technically the same and the names are interchangeably used. However within ADSS Server these are differently interpreted based on how the CRLs are being segmented. If the CA has issued segmented CRLs based on different revocation reasons e.g. unspecified, certificateHold etc. then these CRLs are treated as segmented CRLs within the ADSS Server and multiple CRL resource addresses need to be configured within ADSS Server Trust Manger > Configured CRL Settings page. On the other hand if a CA issues CRLs divided based on the range of certificate serial numbers then ADSS Server handles such CRLs as partitioned CRLs and an LDAP repository containing all the partitioned CRLs needs to be configured within ADSS Server Trust Manager > Configure CRL Settings page.

How to configure and manage partitioned CRLs in ADSS Server?

The following link in the online ADSS Server admin guide explains how a CA can be configured to download certificate serial number based partitioned CRLs: http://manuals.ascertia.com/ADSS-Admin-Guide/default.aspx?pageid=Step_3___Configuring_CRL_Settings.

I can not download the Delta CRL for Microsoft CA

It is a known limitation in the ADSS Server that it fails to download the CRLs when the CRL file name contains a + sign. You can tune the MS CA configurations so that it doesn't include the + sign in the delta CRL file name. Follow these instructions to make the required configurations in the MS CA:

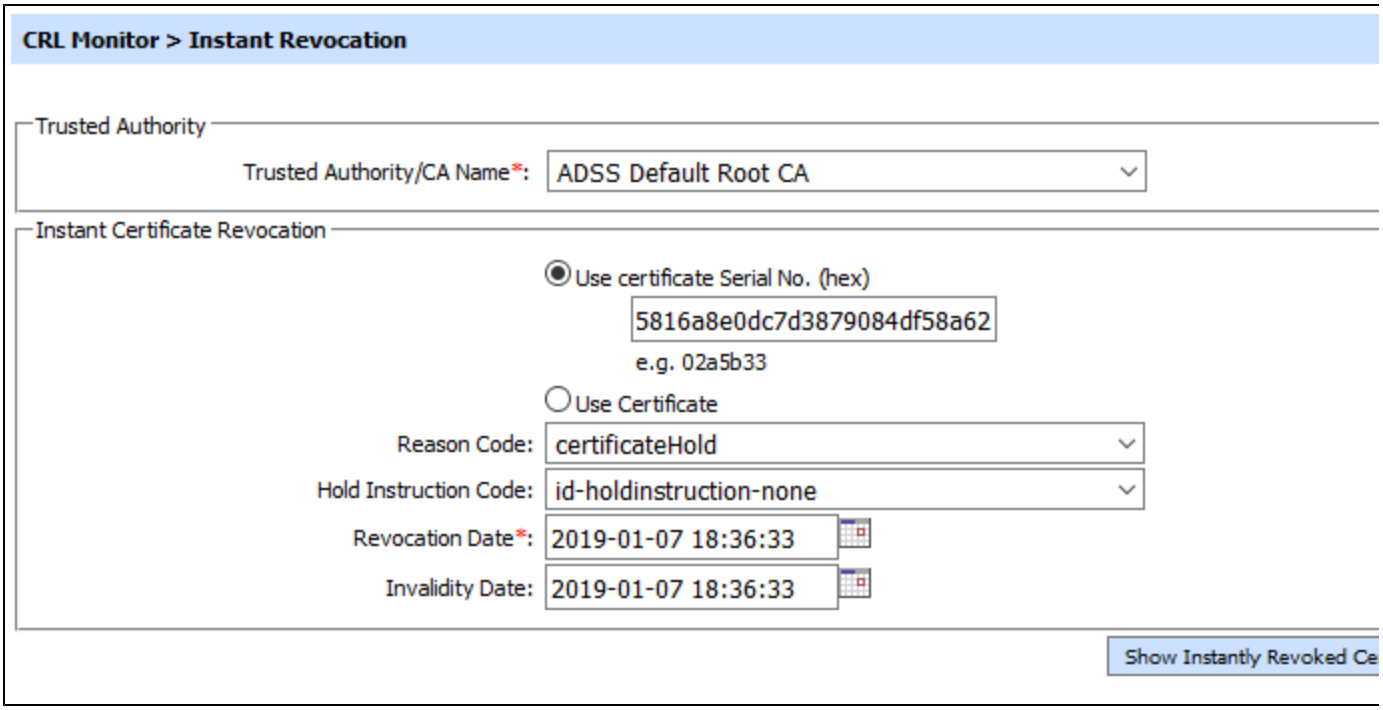
1. Go to the Start Menu > Control Panel > Administrative Tools and launch the **Certification Authority**
2. Right click on the CA certificate node and click on the **Properties**
3. In the Properties dialog, go to the **Extensions** tab
4. For the CRL Distribution Point (CDP) extension, by default a CRL file publishing address is configured like this: **C:\WINDOWS\system32\CertSrv\CertEnroll\.crl**
5. By default the options to publish both the CRL and the delta CRL to above location are selected. Note the variable is the reason why MS CA adds a + sign in the delta CRL file name while it doesn't add any such character in the full CRL file name.
6. Remove the default address and add two separate addresses out of which one is for publishing the full CRL and the other is for publishing for Delta CRL. The example addresses are listed below:
   C:\WINDOWS\system32\CertSrv\CertEnroll\.crl
   C:\WINDOWS\system32\CertSrv\CertEnroll_DELTA.crl
7. As in the second address listed above, the fixed string "_DELTA" is used instead of the variable "" to avoid inclusion of + sign in the CRL file name as well as CDP URL.
8. Apart from the CRL publishing path currently there is a default CRL Distribution Point configured for both the full and delta CRLs like **http:///CertEnroll/.crl**
9. It should also be removed and two new CRL addresses should be added likewise:
   http:///CertEnroll/.crl (used as the CDP Extension within issued certificates)
   http:///CertEnroll/_DELTA.crl (used as Freshest CRL Extension within the issued CRLs)
10. Configure the new CRL URL in the ADSS Server Trust Manager for the respective CA, it will successfully download the Delta CRL.

How to Instantly Revoke a certificate for Business Continuity Management?

If a CA goes out of operation due to some reason, its key will be destroyed and no CRL could be published after that. The BCM Server will take the charge to continue the business for non-revoked certificates of this CA. But at some point in future, a certificate issued by the same CA would need to be revoked and since no CRL could be published, the BCM Server will use the “Instant Revocation” feature of ADSS Server to revoke such a certificate.

Note that the ADSS Server keeps the CRL of a particular CA in a database table by retrieving all the CRL entries and adding to the table making an exact replica of the CRL. The OCSP Service checks the status of a certificate from this table as querying a database table is faster than parsing a CRL and searching for an entry. When we instantly revoke a certificate, its entry is added into the same database table that can be seen as revoking a certificate and adding to the CRL and the BCM Server will be able to provide its current revocation status as the OCSP Service will check its status by looking into the database and return “Revoked” status in response.

To instantly revoke a certificate, navigate to (ADSS Console > CRL Manager > Instant Revocation), the following screen will be displayed:



Follow these steps to revoke a certificate:

1. Select a CA that issued the certificate from the **Trusted Authorities/CA Name** drop down.
2. Now provide the certificate information, either certificate serial number or certificate can be provided by using the relevant controls on the screen.
3. Select a revocation reason from the **Reason Code** drop down. If reason code is **certificateHold**, then a hold instruction code should also be selected from the **Hold Instruction Code** drop down.
4. Provide a revocation date in the **Revocation Date** field.
5. An invalidity date can also be provided in the **Invalidity Date** field.
6. Once all the required information is provided, click on the **Revoke Certificate** button to instantly revoke this certificate.

Note: If **CRL Caching** is enabled in **Trust Manager** for high speed OCSP, then upon instantly revoking a certificate, ADSS Server will prompt to restart the OCSP Service so that the latest revocation information could be loaded into the cache.