

## Re: Certificates trouble: CRL not available(?) and "revocation server offline" error

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-04/msg00130.html>

---

- *From:* Brian Komar <[bkomarr@xxxxxxxxxxxxxxxxxxxx](mailto:bkomarr@xxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 30 Apr 2007 09:02:55 -0500
- 

First thing that I would do is validate the CDP and AIA extensions.  
Run pkiview.msc (from the resource kit tools) and verify that \*all\* CDP and AIA points are considered Valid (expiring is OK too).

Brian

On Sun, 29 Apr 2007 23:35:24 +0530, camexan wrote:

Hello to all!!!

I had installed EntRoot and EntIssuing CAs for my test environment (they are both online), and after that configured them like this:

EntRoot

- CDP and AIA locations left on default.
- Base CRL publication is 1 week, no Delta CRLs.
- Deleted all cert tmpls from CA>Certificate Templates except Subordinate Certification Authority.

EntIssuing

- CDP and AIA locations left on default
- Base CRL publication is 1 Days, Delta CRL publication is 6 hours, and AD replication is 2 hours (as this is my test environment)
- Created new FirmaEFS cert tmpl upon the Basic EFS, on its Properties>Superceded Templates tab add Basic EFS, and after that deleted Basic EFS from CA>Certificate Templates.

Trouble is: I obtained some certificates based upon the FirmaEFS cert tmpl on my client computer for two different users, by using Certificates snap-in console. However, when I try to use them for encryption of files I get some errors:

- When I try to encrypt files, a new local certificate is self-issued to the user and used for encryption (that is not part of the CA hierarchy), and not that obtained for EntIssuing CA. Is it possible to force user cert obtained from EntIssuing CA to be used for encryption

Re: Certificates trouble: CRL not available(?) and "revocation server offline" error

(i.e. to manually select certificate that will be used)?

– When I try to add certificate of users issued by EntIssuing CA, on the Encryption Details dialog of the file, I receive "revocation server offline" error. Then I manually checked that CDP and AIA locations are available, and they are, but it seems that clients cannot access them.

How can I troubleshoot whether clients have the access to the CRLs?

– Furthermore, in Certificates snap-in console on client, in Intermediate Certification Authority>Certificate Revocation List node, there's no EntIssuing CRL. I imported it manually, restarted the client, but I have the same error symptoms as previously. How can I see that client is consulting this CRL for revocation, and does it use some other ones from its cached locations?

I would appreciate if you can help me with this!

Camil.