Windows Server®
Active Directory

Zertifikatssperrliste(n) in Active Directory veröffentlichen

Zertifikatssperrliste(n) in Active Directory veröffentlichen

Inhalt

Zertifikatssperrliste(n) in Active Directory veröffentlichen

Hier in diesen Howto möchte ich euch zeigen, wie man die Zertifikatssperrliste(n) in Active Directory veröffentlicht. Das ganze wurde wieder in einer Virtuellen Umgebung mit Oracle - VirtualBox nachgestellt.

Die erste Frage die sich stellt ist was ist eigentliche eine Zertifikatssperrliste?

- Eine Zertifikatsperrliste **(certificate revocation list, CRL)** ist eine Liste, die die Ungültigkeit von Zertifikaten beschreibt. Sie ermöglicht es, festzustellen, ob ein Zertifikat gesperrt oder widerrufen wurde und warum.

- Zertifikate werden gesperrt oder widerrufen, wenn deren zugehöriger Schlüssel z. B. nicht mehr sicher ist, weil sie in die falsche Hände geraten sind oder kompromittiert wurden – in solchen Fällen muss das Zertifikat noch vor dem eigentlichen Ablaufdatum gesperrt werden.

Eine **CDP (CRL Distribution Point)** = Zertifikatsperrlisten-Verteilungspunkt ist eine Verzeichnisfreigabe in dem man die Zertifikatsperrliste(n) einer Firma findet und öffentlich für das Netzwerk zugänglich macht.

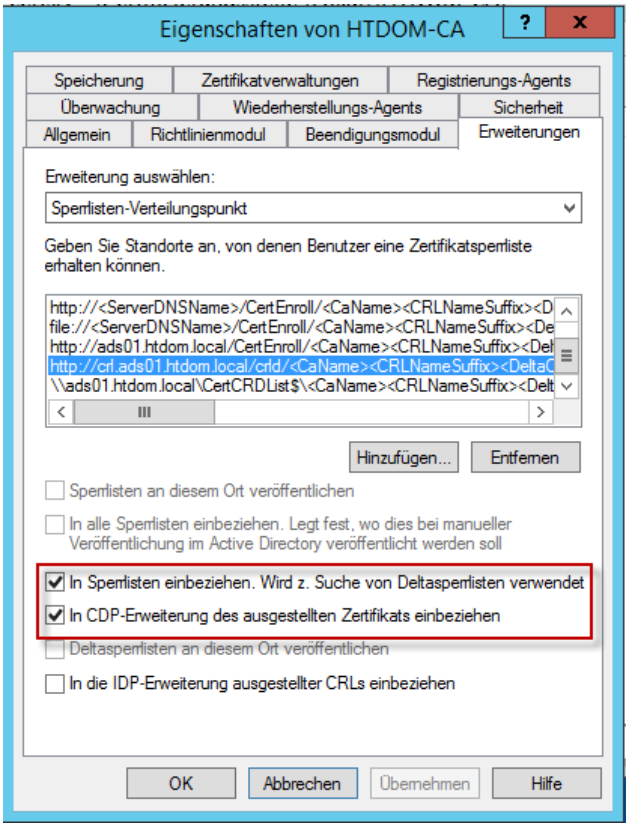
Die Standardangaben einer sogenannten CDP (CRL Distribution Point) sind wie folgt:

- Lokaler Pfad - Zertifikatsserver – **C:\Windows\system32\CertSrv\CertEnroll\<CDP variables>**
- LDAP – **ldap://CN=<CDP CA Name>,CN=<CDP server><other CDP variables>**
- HTTP/HTTPS – **http://<CA server name>\CertEnroll\<CDP variables>**
- Dateipfad – **file://<CDP variables>**
- Dateifreigabe – **\\<server name>\<share>\<CDP variables>**

Da nicht alle Firmen Benutzer auf das Hauptverzeichnis vom Domänencontroller zugreifen sollen, werden die Zertifikatssperrliste(n) in eine neue Freigabe um konfiguriert.

Erweiterung in der Zertifizierungsstelle konfigurieren

Als erstes wird die Verwaltungskonsole der Zertifizierungsstelle geöffnet, mit der rechten Maustaste klickt man auf den Servernamen und ruft die Eigenschaften auf.

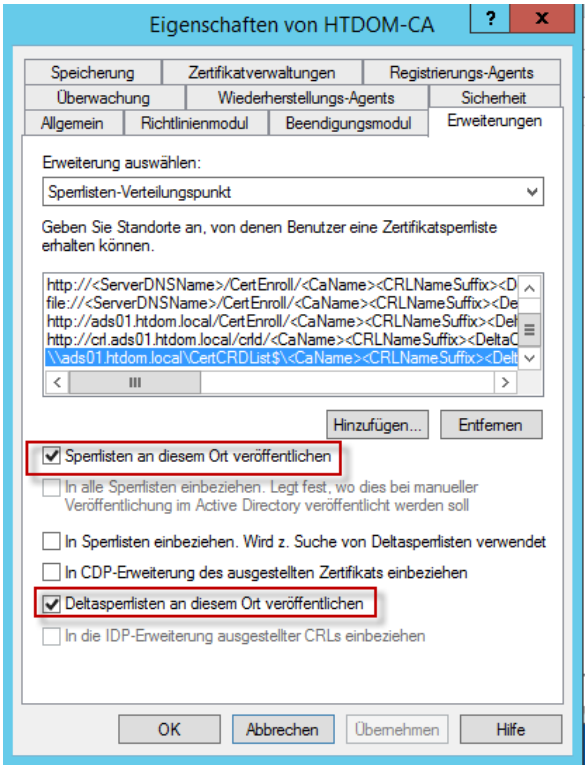


In der Erweiterung wählt man die **Sperrlisten-Verteilungspunkt** aus und fügt insgesamt zwei neue Einträge hinzu.

Erster Eintrag enthält die URL die man später über den Browser aufrufen kann.

http://crl.server.domain.local/crld/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

- In Sperrliste einbeziehen. Wird z. suchen von Deltasperrlisten verwendet
- In CDP-Erweiterungen des ausgestellten Zertifikats einbeziehen



Zweiter Eintrag beinhaltet die Serverfreigabe die im Anschluss angelegt wird.

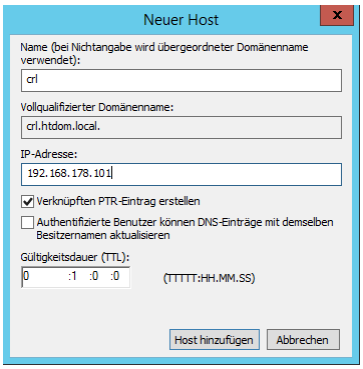
\\server.domain.local\<Freigabe$>\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

- Sperrlisten an diesen Ort veröffentlichen
- Deltasperrlisten an diesen Ort veröffentlichen

DNS Host Eintrag konfigurieren

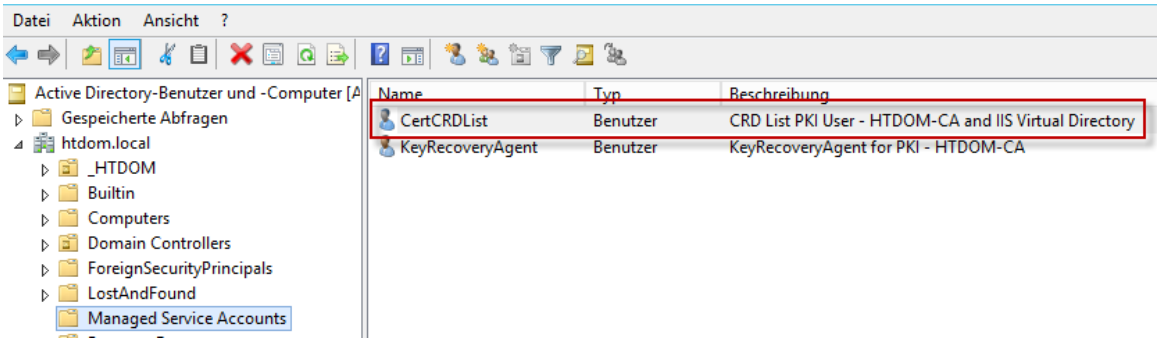
Damit wir die URL später im Browser aufrufen können legen wir einen neuen A/AAAA Host Eintrag im DNS Server an

In diesem Beispiel - **crl** - IP-Adresse Zertifikatserver



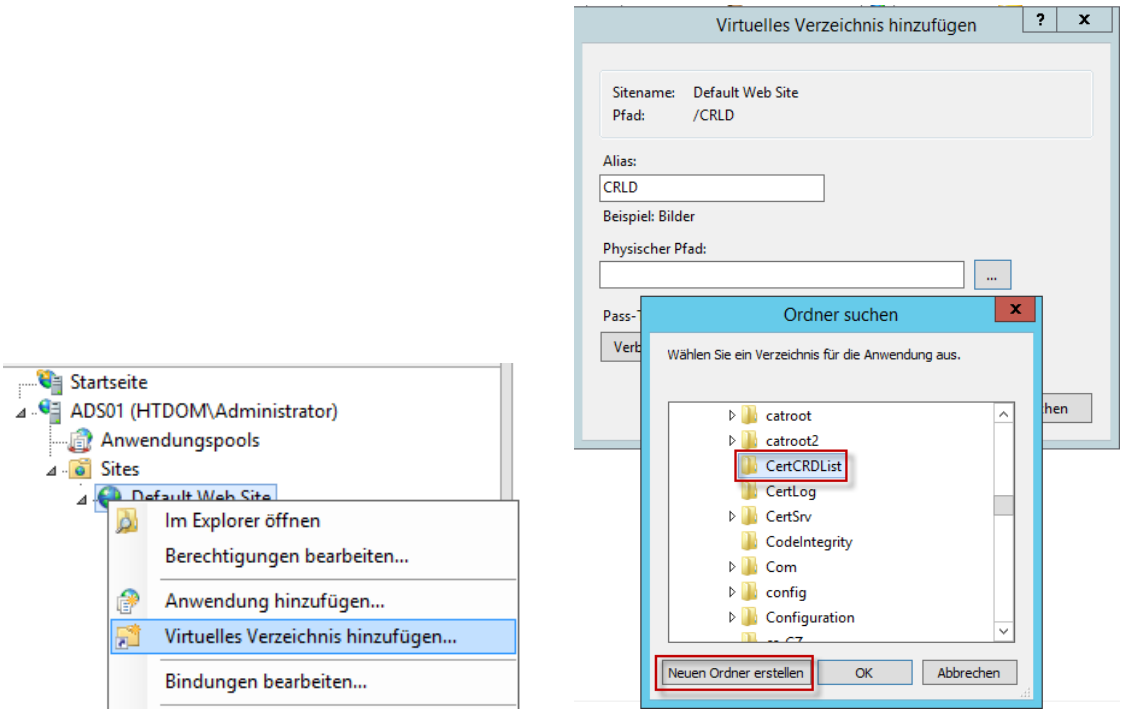
Managed Service Account im AD anlegen

Im Active Directory wird ein neuer Managed Service Account anlegen, der später Vollzugriff auf das Virtuelle Verzeichnis im IIS bekommt.

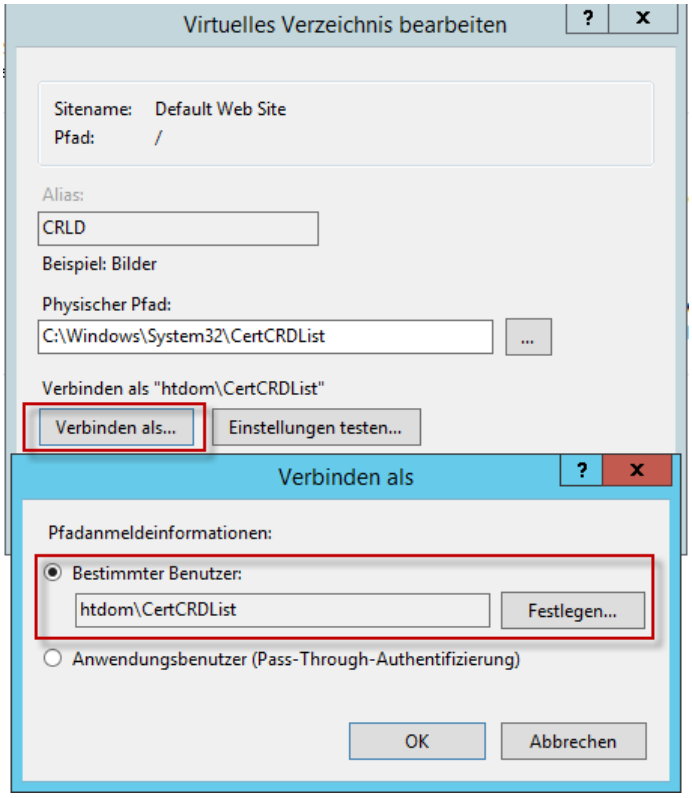


Virtuelles Verzeichnis im IIS konfigurieren

Im IIS-Servermanager legen wir für die **Default Web Site** ein neues Virtuelles Verzeichnis an

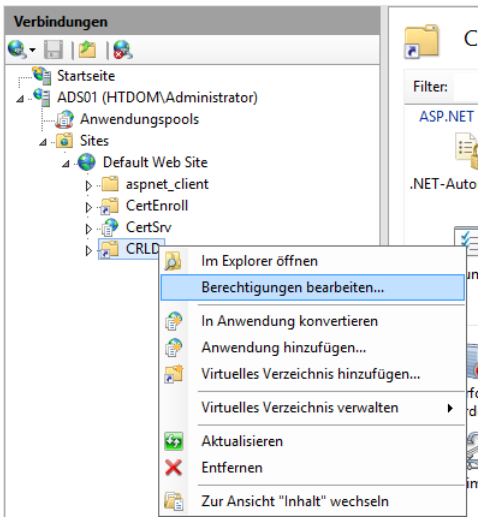


Das Virtuelle Verzeichnis bekommt einen Aliasname **CRLD** und im Physikalischen Pfad **C:\Windows\system32** wird ein neuer Ordner mit dem Namen **CertCRDList** angelegt. Der Ordner kann theoretisch angelegt werden wo man möchte.

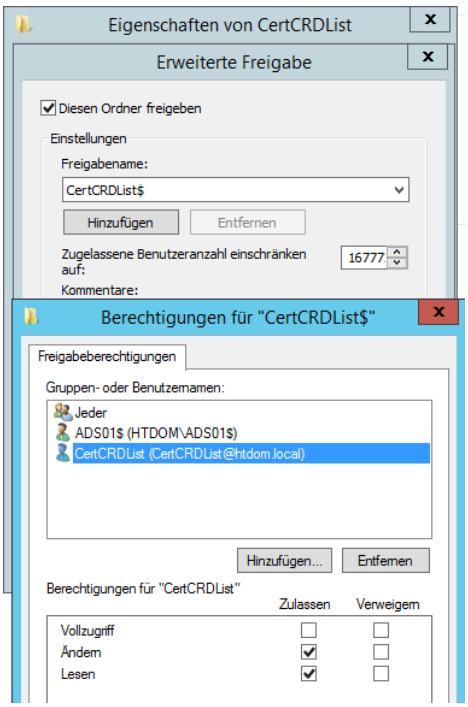


Bei **Verbinden als…** konfigurieren wir nun den neu erstellten Managed Service Account.

Bitte noch nicht auf **Einstellung testen**… klicken, hier würde man eine Fehlermeldung angezeigt bekommen, da der Managed Service Account noch nicht auf das Verzeichnis berechtigt ist.

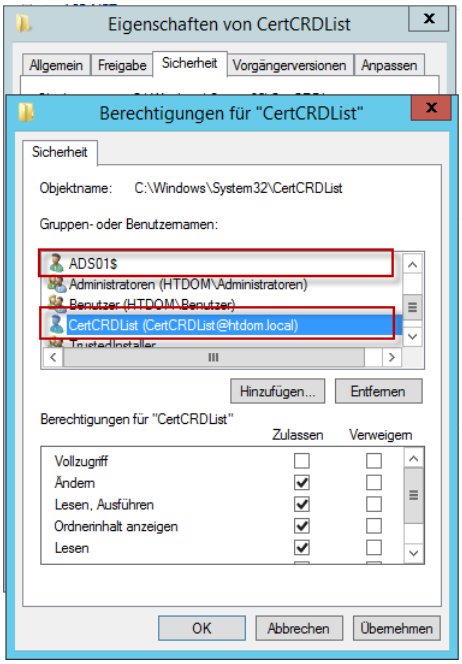


Im nächsten Schritt berechtigen wir jetzt das Virtuelle Verzeichnis für die Veröffentlichung der Zertifikatssperrliste(n), hierzu klickt man auf das Virtuelle Verzeichnis und bearbeite die Berechtigungen.



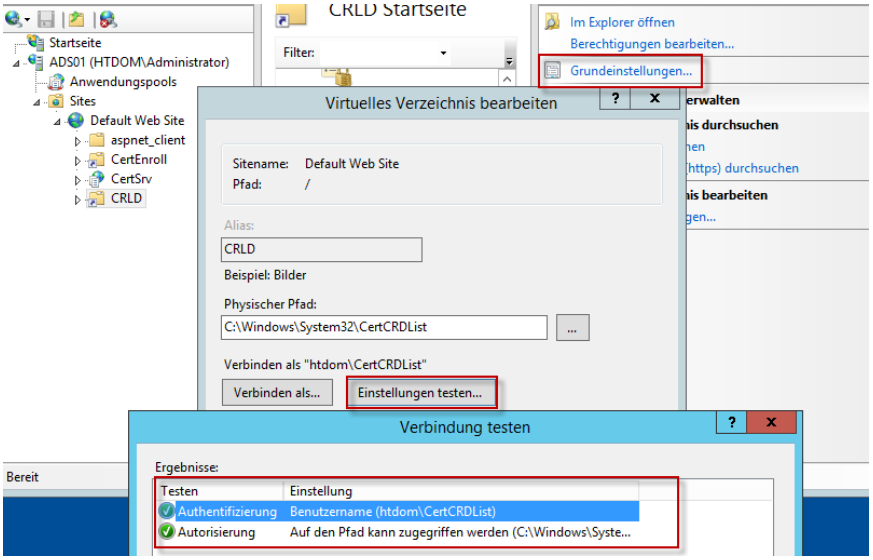
Das Verzeichnis wird nun Freigegeben mit dem Namen **CertCRDList$**

Berechtige den Domänencontroller mit Vollzugriff und den Managed Service Account mit Ändern Rechte, Jeder hat lese Zugriff.



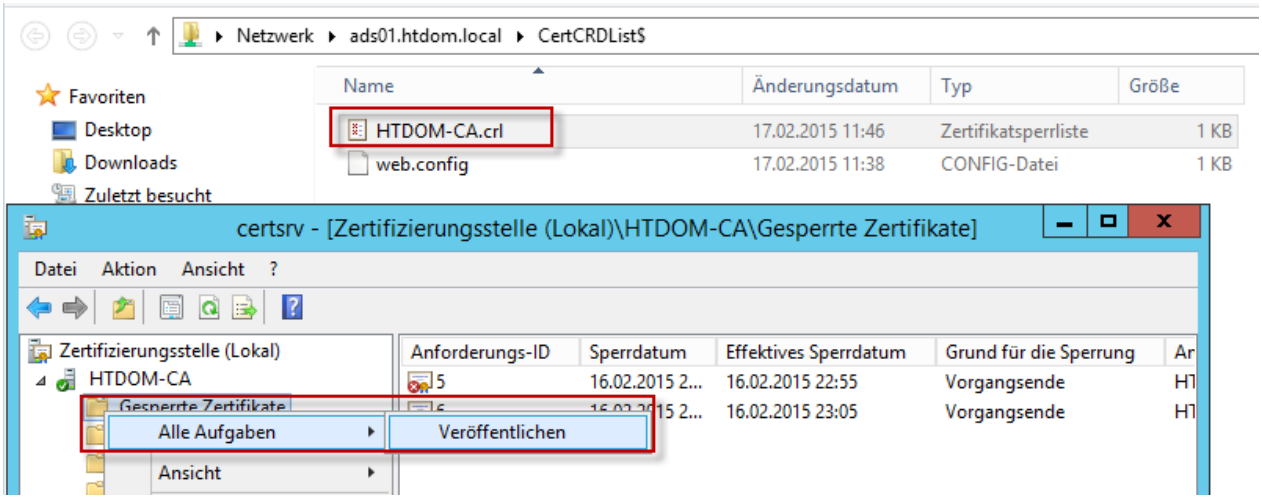
In dem Reiter Sicherheit berechtige ich ebenfalls den Domaincontroller mit Vollzugriff und den Managed Service Account mit Ändern Rechte, alles anderen Einträge bleiben unverändert.

Im Anschluss kann man das Virtuelle Verzeichnis auf den Zugriff testen.

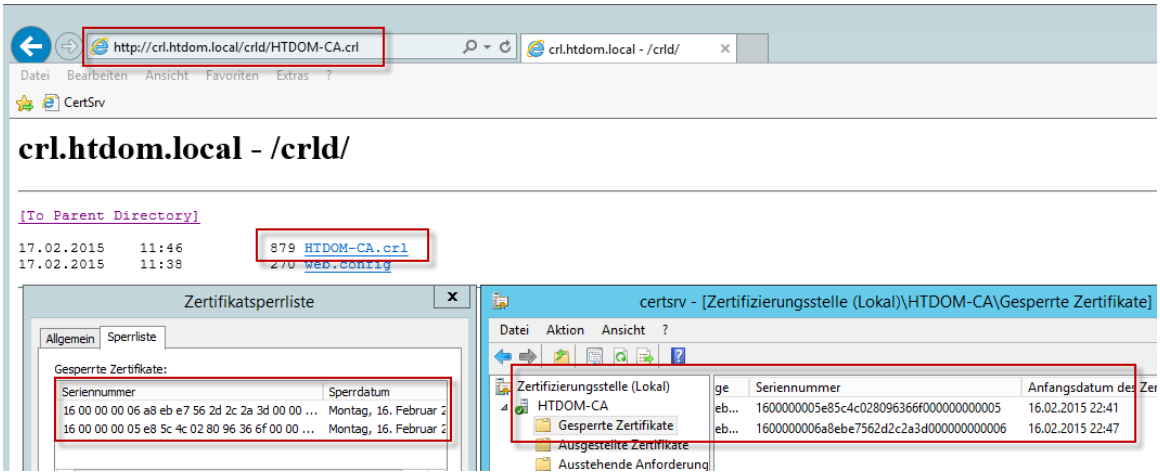


Zertifikatssperrliste veröffentlichen

Um nun die Zertifikatssperrliste(n) im neuen Verzeichnis zu veröffentlichen, öffnet man die Verwaltungskonsole der Zertifizierungsstelle, klickt auf **Gesperrte Zertifikate → Alle Aufgaben → Veröffentlichen**.



Zertifikatssperrliste im Browser überprüfen



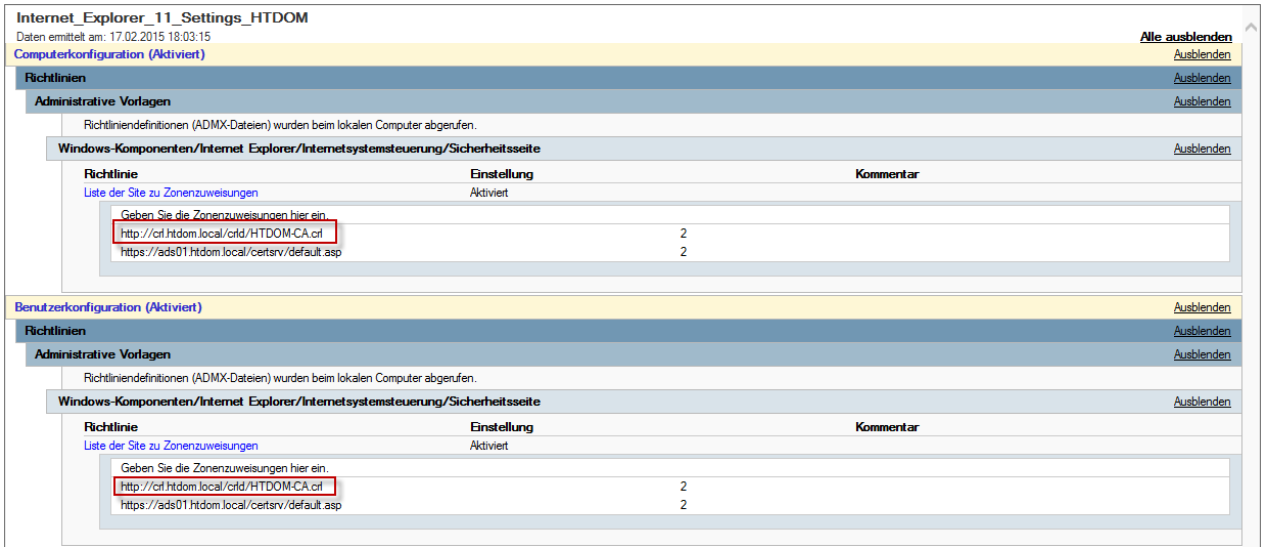
Um das Ganze zu kontrollieren kann man im Webbrowser die URL zu dem Sperrlistenzertifikat aufrufen.

http://crl.<domain.de>/crld/<ZertifizierungsStellenName>.crl

Sollte die URL nicht aufgerufen werden können, kann es daran liegen dass die Webseite noch zu den Vertrauenswürdigen Webseiten hinzugefügt werden muss.

Gruppenrichtlinie für Vertrauenswürdige Webseiten konfigurieren

Dies kann man recht einfach per Gruppenrichtlinie erledigen.



Download [Administrative Templates for Internet Explorer]

Richtlinie

Computerkonfiguration --> Administrative Vorlagen --> Windows Komponenten --> Internet Explorer --> Internetsystemsteuerung --> Sicherheitsseite --> Liste der Site zu Zonenzuweisung

http://crl.<domain.de>/crld/<ZertifizierungsStellenName>.crl

Benutzerkonfiguration --> Administrative Vorlagen --> Windows Komponenten --> Internet Explorer --> Internetsystemsteuerung --> Sicherheitsseite --> Liste der Site zu Zonenzuweisung

http://crl.<domain.de>/crld/<ZertifizierungsStellenName>.crl

So das war es erstmal wieder von mir.

Viele Grüße
Helmut Thurnhofer