Inhalt

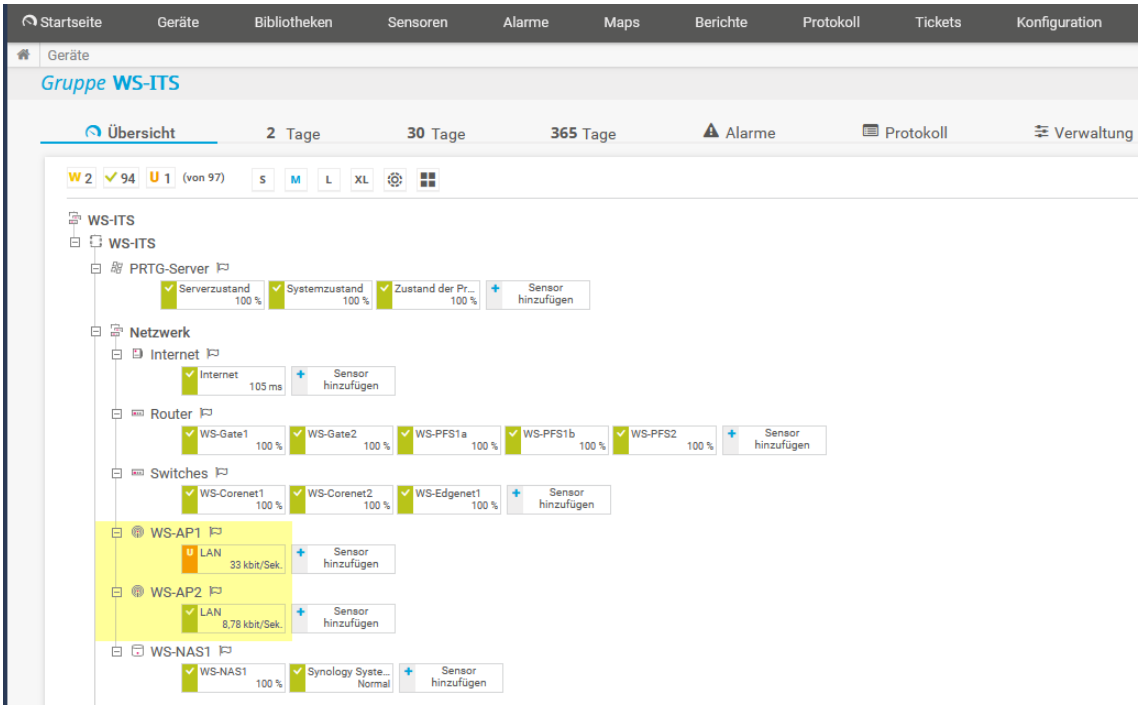
Das Problem

Heute gab es ein Problem bei meiner Netzwerkanmeldung im WLAN. Den mobilen Zugriff habe ich mit 802.1x über einen Radiusserver abgesichert. Die Clients müssen sich mit einem Zertifikat von meiner internen Windows Zertifizierungsstelle authentisieren, bevor sie in das WLAN reingelassen werden.

Die Suche nach der Ursache

Ich begann meine Diagnose an dem betroffenen WLAN-Client. Das Windows 10 Gerät war nicht sehr hilfreich mit der Fehlermeldung „Die Verbindung konnte nicht hergestellt werden“.

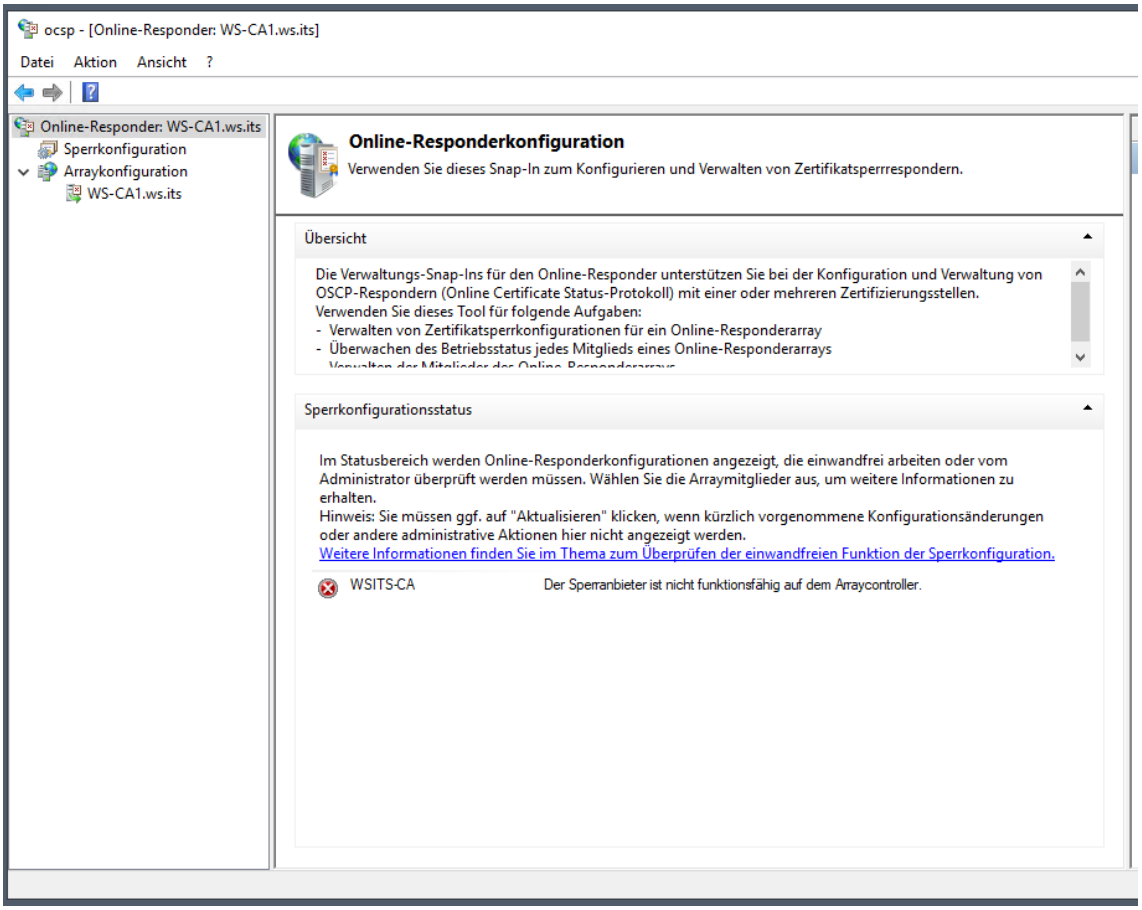
Also besuchte ich meinen PRTG-Monitor. Da habe ich beide Access-Points in die 24/7-Überwachung aufgenommen. Aber beide APs sind online und vom Backend aus erreichbar:



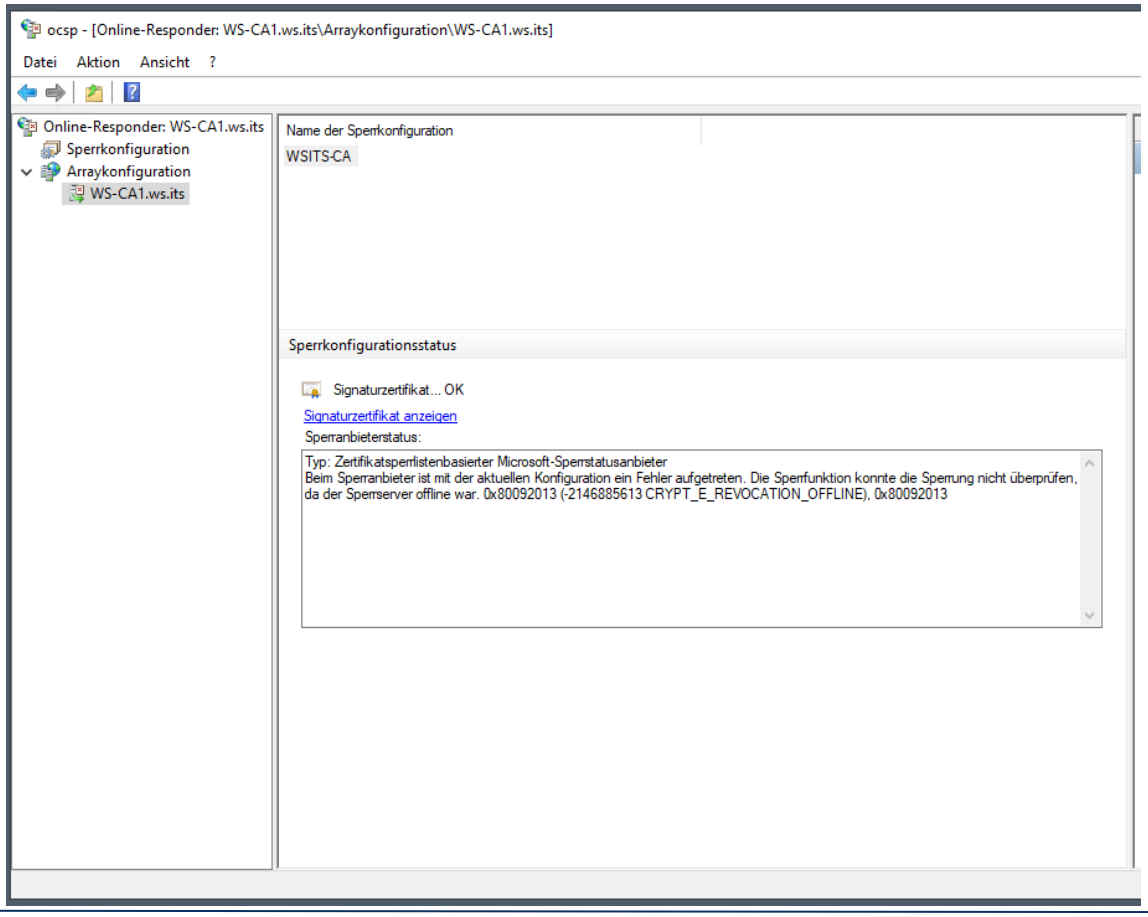
Somit war der nächste Schritt eine Prüfung des Radius-Servers. Im Eventlog wurde ich fündig. Der Client präsentiert sein Sicherheitszertifikat und der Radius-Server versucht die dazugehörige Sperrlistenprüfung durchzuführen. Und diese schlägt fehl:

Die Sperrlisten biete ich für meine ausgestellten Zertifikate über einen klassischen CRL-Download über einen internen Webserver an und zusätzlich betreibe ich einen eigenen Online Responder. An diesen kann mein NPS (Network Protection Server – allgemein als Radius-Server bekannt) eine Zertifikat-Seriennummer übermitteln und als Antwort erhält er eine signierte Sperrinformation. Ist das Zertifikat gesperrt, dann wird der NPS den Verbindungsaufbau ablehnen.

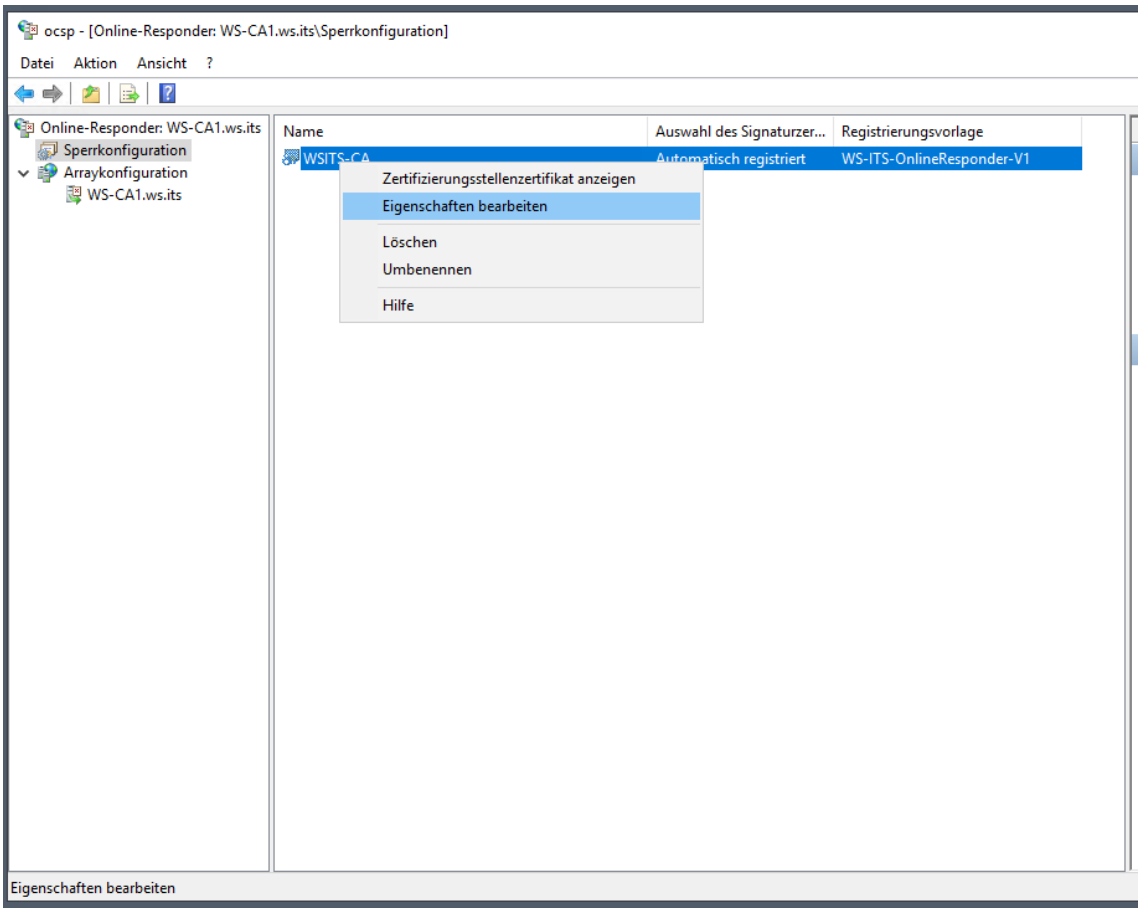
Die Sperrliste ist aktuell. Es scheint also ein Problem mit dem Online Responder zu geben. Daher verbinde ich mich mit meinem Server WS-CA1. Darauf läuft die Zertifizierungsstelle und der Online Responder. In der Management-Konsole des Online Responders sehe ich einen Fehler:



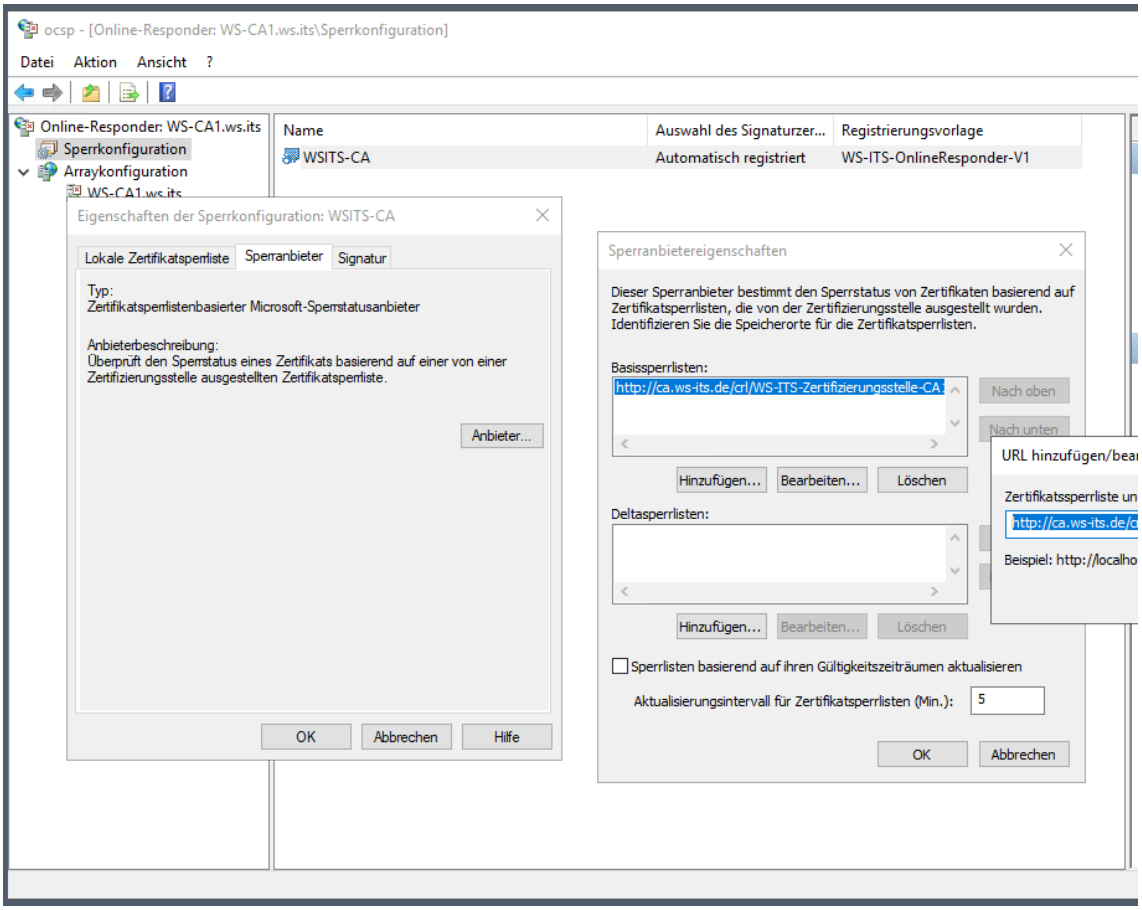
In den Details erkenne ich eine Fehlernummer



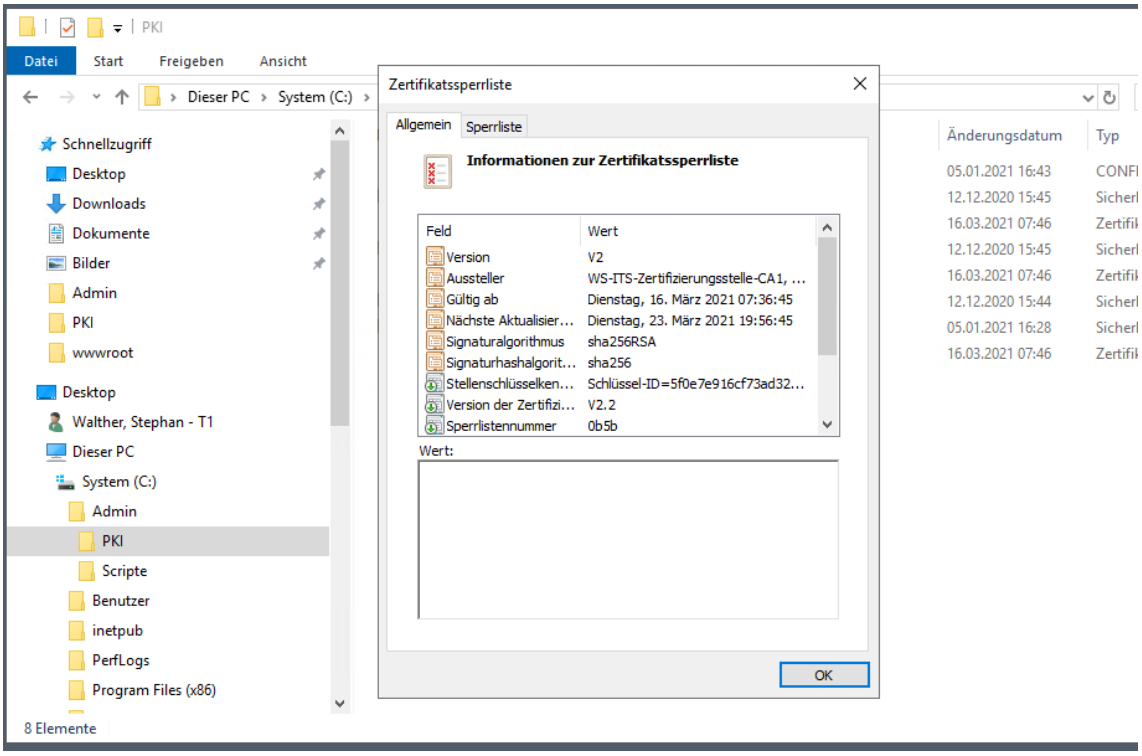
Der Sperrserver ist offline? Das habe ich bei den ausgestellten Sperrlistendateien aber anders gesehen… Ich prüfe daher die hinterlegte Sperrlisten-Konfiguration im Online Responder – der Service hat selber keinen direkten Zugriff auf die Zertifizierungsstelle und braucht daher Zugriff auf einen klassischen Sperrlisten-Verteilungspunkt:



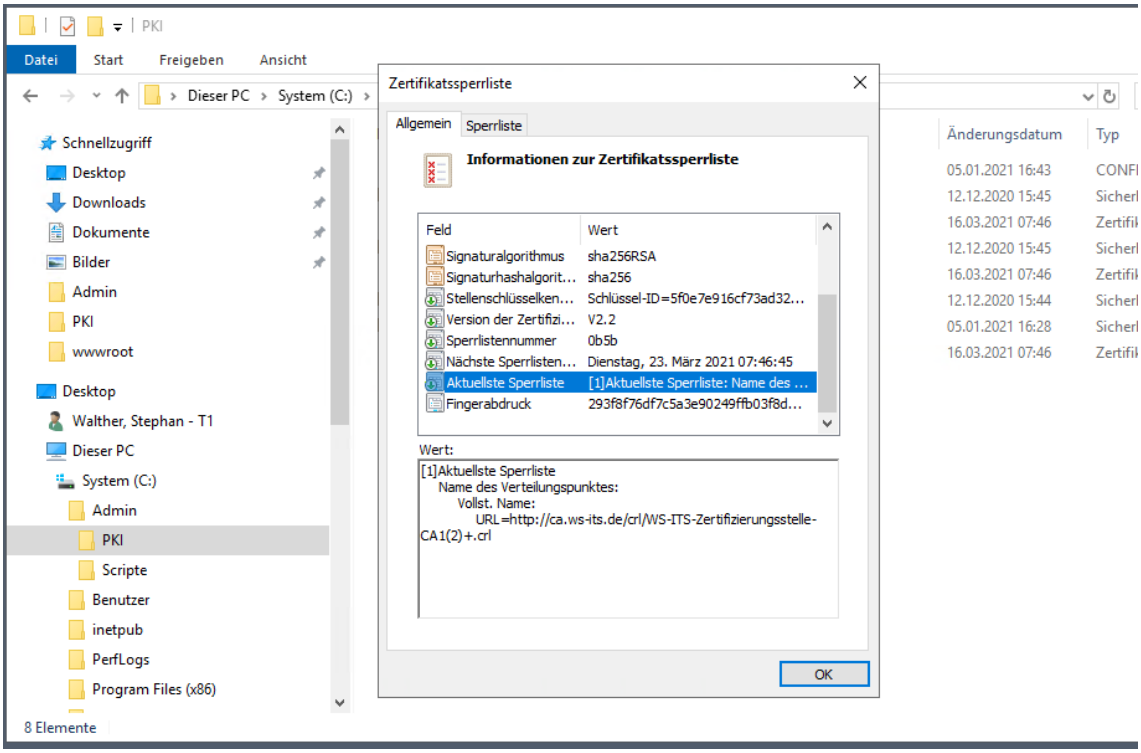
Der Online Responder verwendet den klassischen Download der Sperrlistendatei:



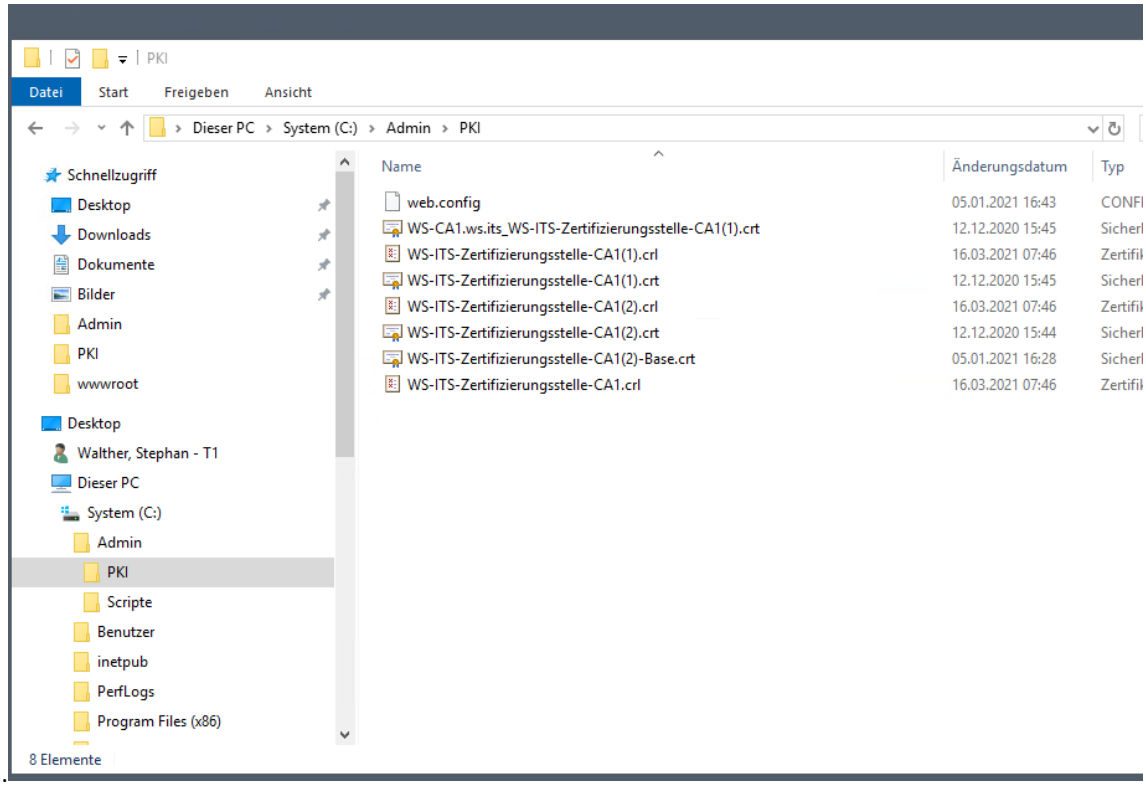
Vielleicht stimmt etwas mit der Sperrliste nicht? Diese Dateien haben ein Verfallsdatum, das im Windows Explorer angezeigt werden kann. Aber meine Sperrliste ist innerhalb des Gültigkeitszeitraumes:



Die Ursache muss woanders liegen. Ich erinnere mich, dass mit zusätzlichen Eigenschaften in Sperrlisten Veränderungen der Sperrlistenverteilungspunkte an Clients kommuniziert werden können. Also scrolle ich in den Eigenschaften nach unten

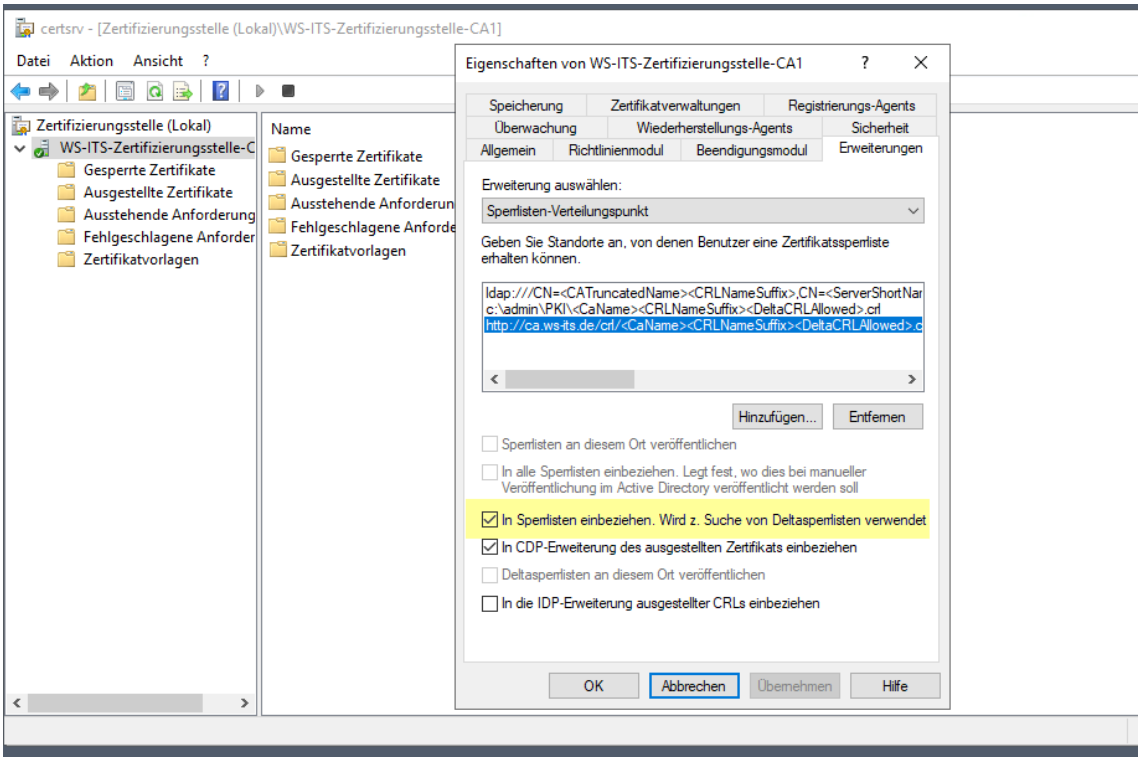


In den Eigenschaften steht, dass eine aktuellere Sperrliste in der Web-Resource vorhanden ist. Der Online Responder wird also versuchen, diese Delta-Datei herunterzuladen (Hinweis: Die Delta-Sperrliste erkennt man an dem Plus-Zeichen im Dateinamen). Ich prüfe erneut das lokale Verzeichnis hinter dem Webservice. Hier kann ich aber keine Delta-Sperrliste finden:

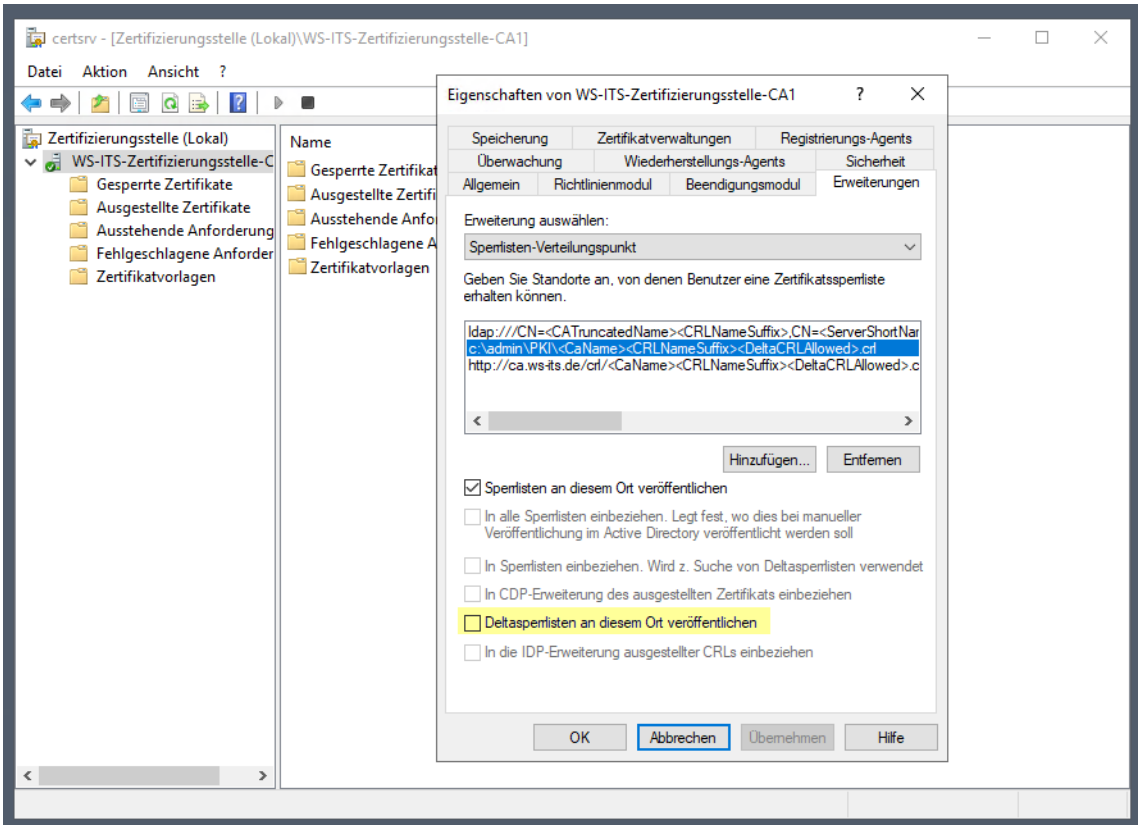


Und das ist nun mein Problem! Der Online Responder kann die Delta-Sperrliste nicht herunterladen und verweitert daher seinen Dienst. Der Radius-Server bekommt also keine Sperrlistenüberprüfung hin und lehnt daher den anfragenden WLAN-Client ab.

Ich muss also herausfinden, warum sich auf der Sperrliste ein Verweis zu einer Delta-Sperrliste befindet bzw. warum die Delta-Sperrliste nicht erstellt wurde. Die dazugehörige Konfiguration finde ich in meiner Zertifizierungsstelle. In den Erweiterungen finde ich den Hinweis zum Verweis. Diese Option aktiviert den Aufdruck in der Sperrliste, dass es eine aktuellere Delta-Sperrliste gibt:



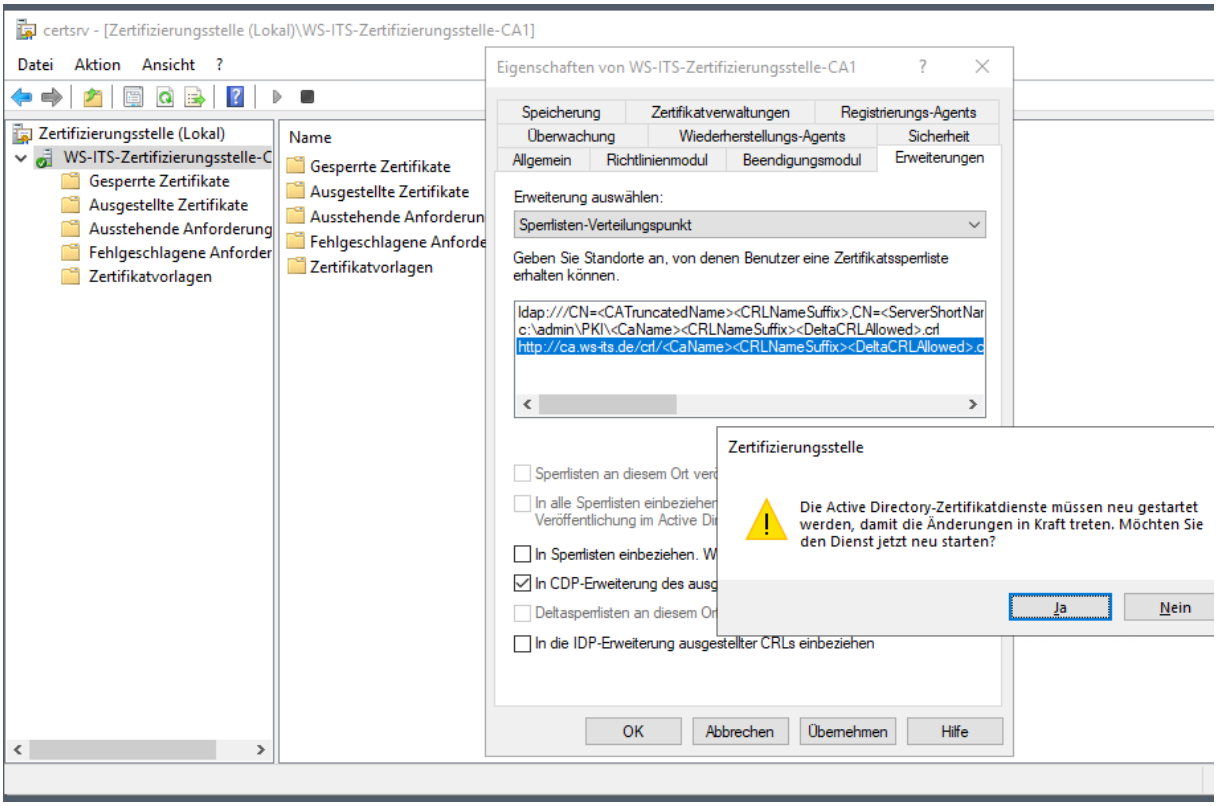
Die Windows Zertifizierungsstelle kann die neuen Sperrlisten nicht direkt in einen Webserver hochladen. Daher habe ich meinen Webserver, der auf dem gleichen Server läuft, auf ein lokales Verzeichnis zeigen lassen, in dem der Service der CA seine Sperrlistendateien ablegt. Und hier fehlt die Option zur Veröffentlichung der Delta-Sperrliste:



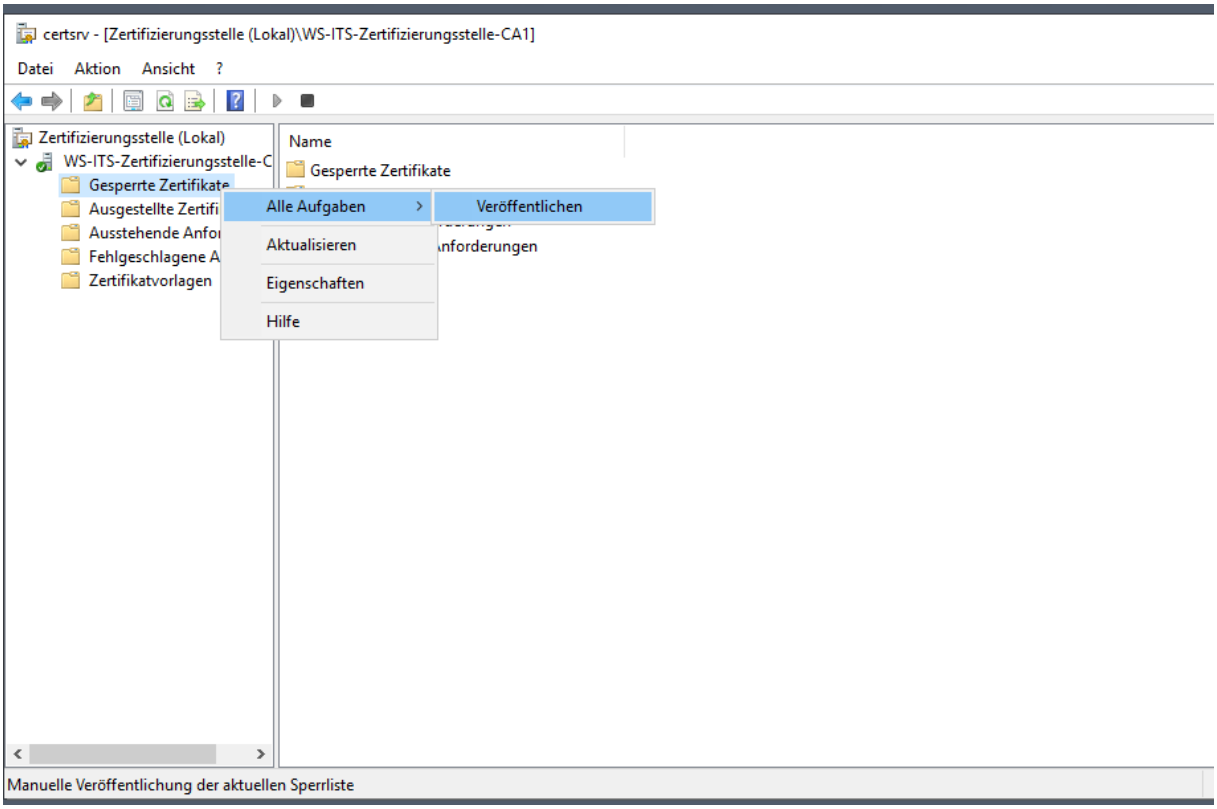
Die Lösung

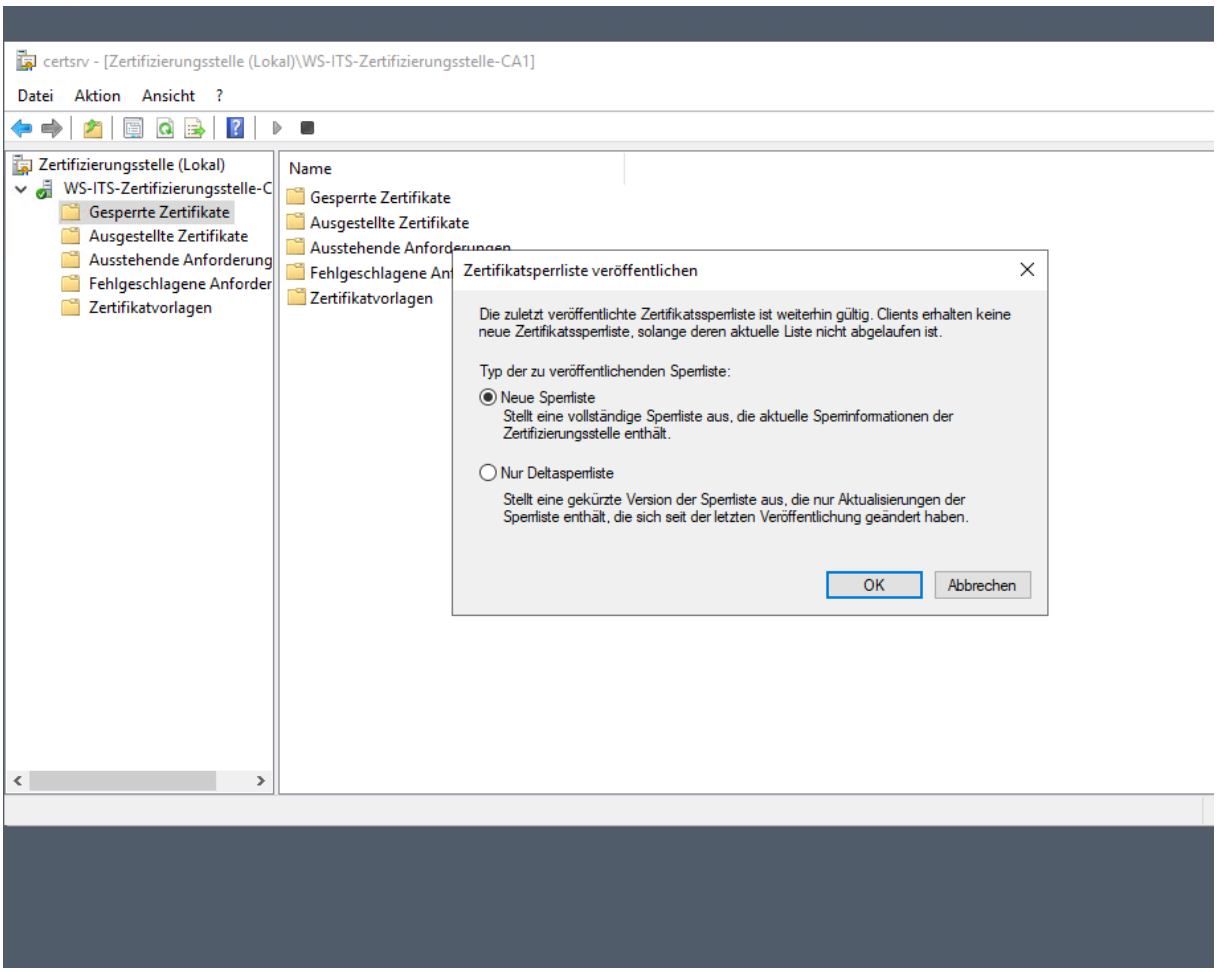
Nun muss ich mich entscheiden: Soll die Windows CA eine Delta-Sperrliste veröffentlichen oder soll auf der Sperrlistendatei der Vermerk zur Delta-Sperrliste rausfliegen?

Ich hatte mich bewusst gegen eine Delta-Sperrliste entschieden, weil ich zum einen ein sehr geringes Sperrvolumen habe und zum anderen so das Monitoring wesentlich einfacher ist. Also muss die Option für http angepasst werden. Ich entferne die Option und speichere die Konfiguration. Abschließend muss der Service neustarten:

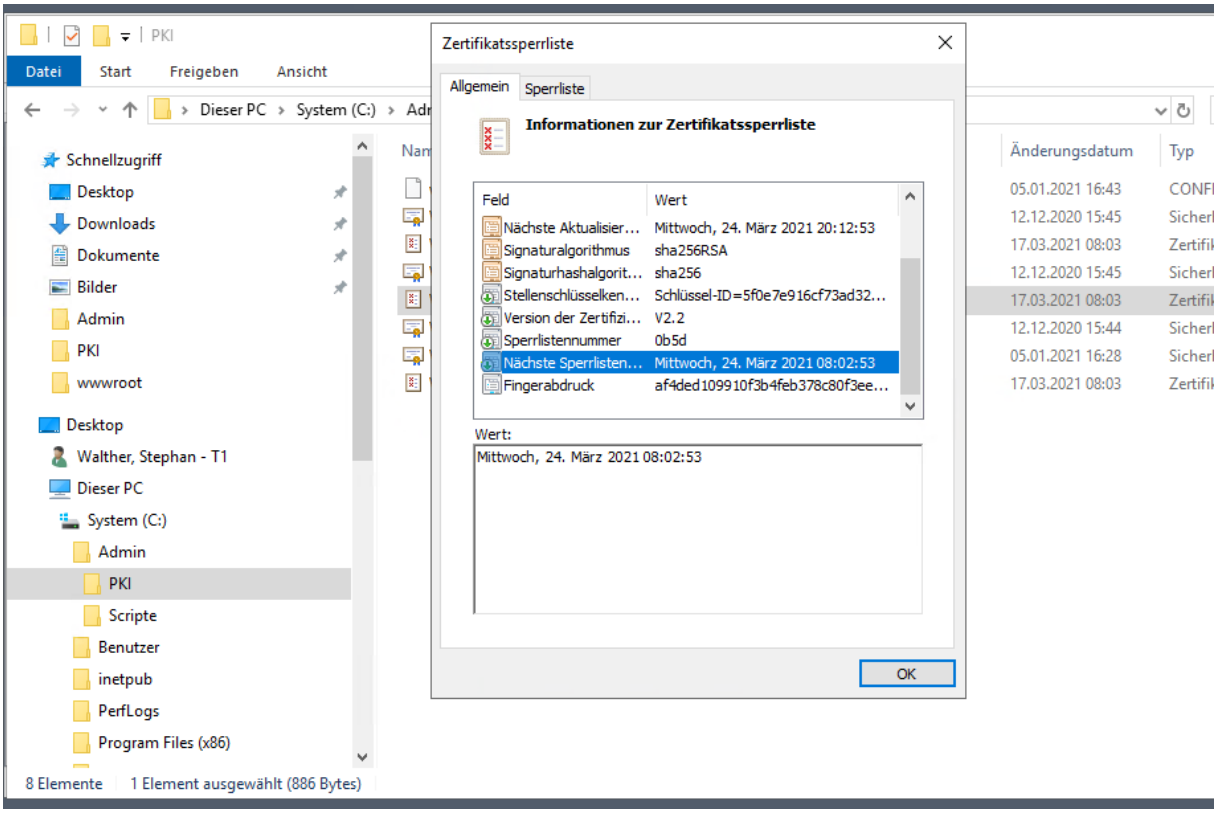


Nach wenigen Sekunden ist der Service wieder online. Er wird aber nicht sofort eine neue Sperrliste generieren, denn diese hat aktuell noch genügend Restlaufzeit. Also erstelle ich manuell eine neue:

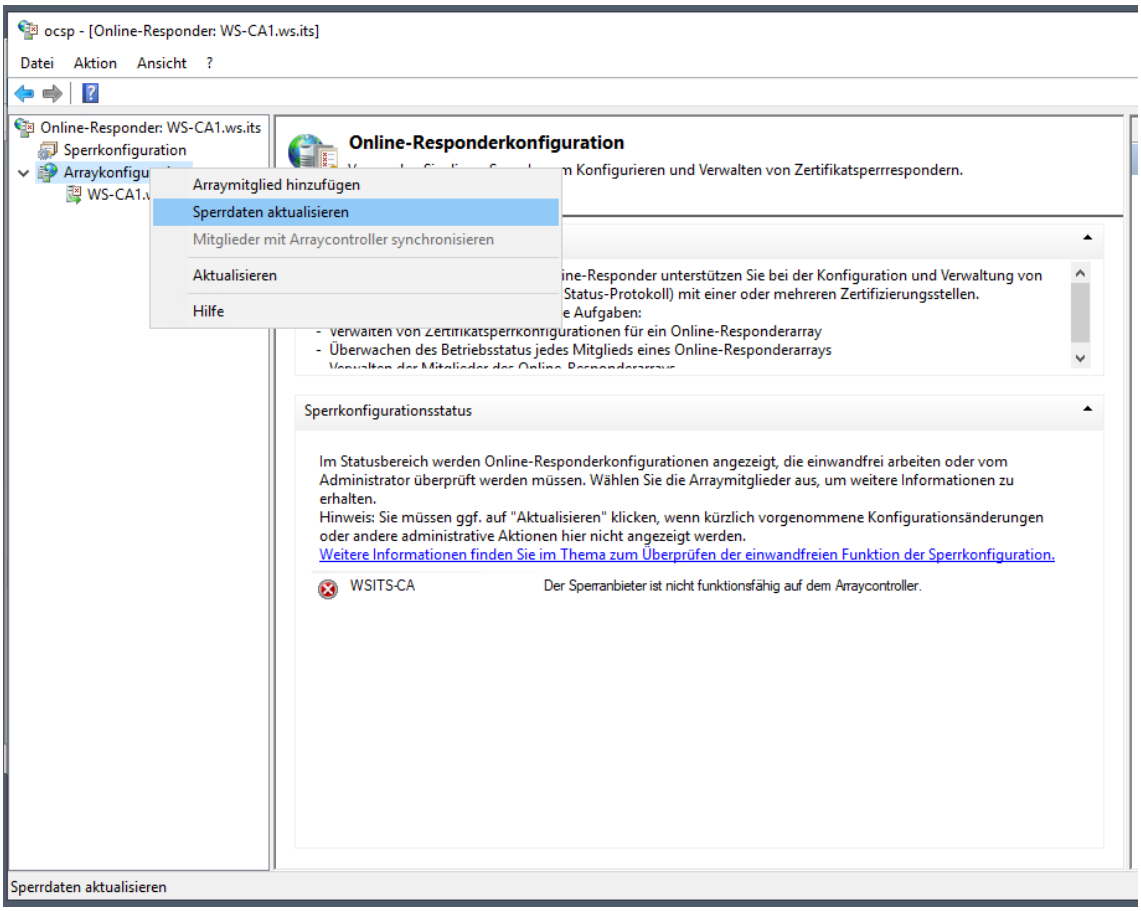




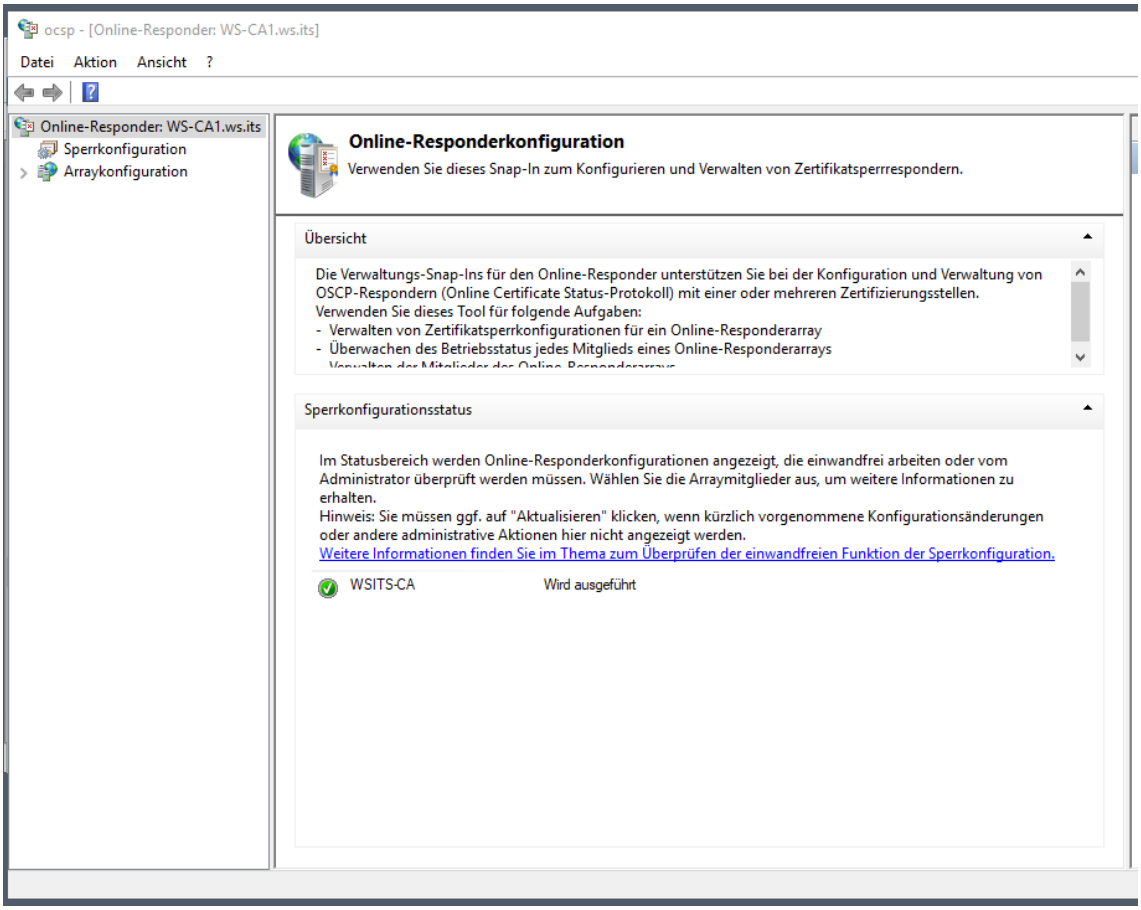
Anschließend kontrolliere ich die neue Sperrlistendatei. Jetzt fehlt der Hinweis auf eine Delta-Sperrliste:



Mein Online Responder soll alle 5 Minuten auf eine Aktualisierung der Sperrliste schauen. Das dauert mir aber zu lange. Daher starte ich die Aktualisierung manuell:



Jetzt ist der Online Responder wieder einsatzbereit:



Damit ist das Problem gelöst. Der WLAN-Client kommt nun wieder ins Netzwerk.

Zusammenfassung

Manche Probleme haben ihre Ursache in der Vergangenheit. In diesem Fall war es eine falsch konfigurierte Sperrliste und die Auswirkungen zeigten sich erst nach deren Ablauf. Gut ist es, wenn man dann beim TroubleShooting die Abhängigkeiten kennt. Besser ist es natürlich, wenn man ein proaktives Monitoring hat, das die Admins informiert, bevor es die Benutzer trifft. Aber das wird ein anderer Beitrag.