

OCSP einrichten

Admin-Tutorial

Version: 2.0

Datum: 11/2022

IT-Security Solutions

Made in Germany



OCSP einrichten

ECOS Appliances können für die Prüfung von gesperrten Zertifikaten das Online Certificate Status Protocol (OCSP) anbieten. Dazu muss der dazugehörige Dienst auf der ECOS Appliance angelegt und konfiguriert werden.



Zertifikat erstellen

Für die Nutzung des OCSP wird ein Zertifikat benötigt.

Legen Sie dazu ein **X.509-Zertifikat** im **Container: Zertifikate** an. Möchten Sie mit dem OCSP-Dienst die Zertifikate von mehreren CAs prüfen, fassen Sie die OCSP-Zertifikate in einem eigenen Container zusammen. Beachten Sie auch, dass für jede CA ein eigenes OCSP-Zertifikat benötigt wird.

The screenshot shows the 'OCSP-Zertifikat' configuration window with the 'Allgemein' tab selected. The form contains the following fields and options:

- Name:** OCSP-Zertifikat
- Beschreibung:** (empty)
- Erstellung des Zertifikats:** Automatisch erzeugen (dropdown)
- Statusanzeige:** Zertifikat erzeugt
- Zertifikat signieren mit:** ☐ Sich selbst ☒ CA
- CA:** CA Standard (dropdown)
- Gültigkeit:** 365 Tage
- Subjekt:** CN=OCSP-Zertifikat,OU=OCSP-Zertifikate,O=ECOS Management
- Aussteller:** CN=CA TechDoku,OU=CA-Zertifikate,O=ECOS Management
- Schlüsselalgorithmus:** ☒ RSA ☐ EC
- Schlüssel verschlüsselt ablegen:** Verschlüsselt und unverschlüsselt (dropdown)
- Schlüssellänge:** 3072 Bits (dropdown)
- Signatur-Hashalgorithmus:** SHA256 (dropdown)
- Fingerprint:** 42:09:4B:9B:50:89:f (left) C0:B6:3D:4F (right)
- Gültig ab:** 21.09.2022, 12:48
- Gültig bis:** 21.09.2023, 12:48
- Zertifikat:** [Download](#) [Upload](#)
- Zertifikat als PKCS #7:** [Download](#) 2 KB
- Privater Schlüssel:** [Download](#) [Upload](#) 2 KB
- Zertifikat als PKCS#12:** [Download](#) 4 KB
- Zertifikat-Request:** [Download](#) [Upload](#)
- Zertifikat als PEM:** [Download](#) 1 KB
- Smartcard-Zertifikat:** ☒ Kein ☐ Smartcard ☐ HSM ☐ System
- Beziehen von:** (dropdown)
- SCEP Transaction ID:** (empty)
- CSR Challenge:** (empty)

At the bottom, there are buttons for 'Übernehmen' and 'Aktionen'.

Abb. 1.01: Einstellungen OCSP-Zertifikat - Reiter Allgemein

Allgemein

- ➔ NAME: Vergeben Sie einen aussagekräftigen Namen.
- ➔ ERSTELLUNG DES ZERTIFIKATS: **Automatisch erzeugen**
- ➔ ZERTIFIKAT SIGNIEREN MIT: **CA**
- ➔ CA: Wählen Sie die CA aus.
- ➔ SCHLÜSSELALGORITHMUS: **RSA**
- ➔ SCHLÜSSELLÄNGE: **3072 Bits** (oder höher)

The screenshot shows the 'Verwendung' (Usage) tab of a certificate configuration window. The 'Verwendungszweck' (Usage Purpose) is set to 'Auswahl' (Selection). The 'Als kritisch markieren' (Mark as critical) checkbox is unchecked. Under 'Optionen' (Options), the 'Schlüsselverwendung' (Key Usage) section includes checkboxes for 'Digital signieren', 'Datenverschlüsselung', 'Nur entschlüsseln', 'Nichtabstreitbarkeit', 'Schlüsselaushandlung', 'Schlüsselverschlüsselung', and 'Nur verschlüsseln'. The 'Erweiterte Schlüsselverwendung' (Extended Key Usage) section includes checkboxes for 'SSL/TLS Webserver-Authentisierung', 'Code Signing', 'Beglaubigte Zeitmarken', 'Microsoft Smartcard Login', 'Microsoft Commercial Code Signing (Authenticode)', 'Microsoft Encrypted File System', 'Kerberos Client-Authentisierung', 'IPsec-Tunnel', 'SSL/TLS Webclient-Authentisierung', 'E-Mail (S/MIME)', 'OCSP Signing' (checked), 'Microsoft Individual Code Signing (Authenticode)', 'Microsoft Trust List Signing', 'Kerberos KDC', 'IPsec-Endsystem', and 'IPsec-Benutzer'. The 'Als kritisch markieren' checkbox is also present at the bottom of the options section. At the bottom of the window are buttons for 'Anlegen' (Create) and 'Aktionen' (Actions).

Abb. 1.02: Einstellungen OCSP-Zertifikat - Reiter Verwendung

Verwendung

- ➔ VERWENDUNGSZWECK: **Auswahl**
- ➔ ERWEITERTE SCHLÜSSELVERWENDUNG:
- ➔ OCSP-SIGNING: Aktivieren Sie die Checkbox.

Erzeugen Sie das Zertifikat über den Button **Anlegen**. Laden Sie anschließend das ZERTIFIKAT ALS PEM herunter.

2 Dienst: OCSP-Server einrichten

Navigieren Sie im Navigationsbaum der ECOS Appliance zum **Container: Dienste** und dort zu **Dienst: OCSP-Server**. Sollte der Dienst noch nicht vorhanden sein, legen Sie ihn neu an.

Abb. 1.03: Einrichtung des Dienst: OCSP-Server

Allgemein

- ➔ **NAME:** Vergeben Sie einen aussagekräftigen Namen.
- ➔ **STARTEN:** Aktivieren Sie die Checkbox.
- ➔ **PORT:** Tragen Sie den Port ein. Der Standard-Port ist **2560**.
- ➔ **RESPONDERZERTIFIKAT:** Wählen Sie in der Dropdown-Liste das unter Punkt 1 erstellte Zertifikat oder die Zertifikatsgruppe, in der das erstellte Zertifikat enthalten ist, aus.

Speichern Sie die Änderungen mit **Übernehmen** oder **Anlegen**.

3 OCSP URI-Objekt für die CA einrichten

Für die Nutzung von OCSP wird ein **OCSP URI**-Objekt benötigt, das einer oder mehreren CAs zugewiesen werden kann.

Legen Sie ein **OCSP URI**-Objekt an. Sie finden es mit Rechtsklick auf das Organisationsobjekt ganz oben im Navigationsbaum unter **Container: PKI-Einstellungen**.

Abb. 1.04: Einstellungen im OCSP URI-Objekt

Allgemein

- ➔ **NAME:** Vergeben Sie einen aussagekräftigen Namen.
- ➔ **OCSP URI:** Geben Sie hier die URI an unter der die Informationen für den OCSP abgerufen werden können. Die URI setzt sich aus der HTTP-Adresse der ECOS Appliance (IP-Adresse oder FQDN, wenn der Speicherort öffentlich erreichbar sein soll), dem Port, der im **Dienst: OCSP-Server**-Objekt angegeben wurde, und einem beliebigen String zusammen.

Beispiel: <http://myecosappliance.de:2560/OCSP>

- ➔ **AKTIV:** Aktivieren Sie die Checkbox, um den Zugriff auf die URI von außen zu erlauben.

Speichern Sie die Änderungen mit **Übernehmen** oder **Anlegen**.

4 Signierende CA anpassen

In der signierenden CA des unter Punkt ❶ angelegten OCSP-Zertifikats muss die OCSP-Information eingetragen werden. Sollen die OCSP-Informationen für mehrere CAs zur Verfügung gestellt werden, muss das **OCSP URI**-Objekt in jeder dieser CAs eingetragen werden.

Erweitert

- ➔ **OCSP URI:** Wählen Sie hier das unter Punkt ❸ angelegte **OCSP URI**-Objekt aus.

Speichern Sie die Änderungen mit **Übernehmen**. Sie können die OCSP-Informationen einer CA beliebig ändern oder weitere hinzufügen.

The screenshot shows the 'CA Standard' web interface with the 'Erweitert' tab selected. The interface includes several input fields and buttons for configuring OCSP information:

- Zertifikatvorlage:** A dropdown menu.
- Gültigkeitsdauer CRL:** A text input field set to '30' and a unit dropdown set to 'Tage'.
- CRL neu erzeugen:** A dropdown menu.
- URL für CRL Distribution Point:** A text input field.
- CRL:** A button labeled 'Download'.
- CRL automatisch abrufen:** A checkbox.
- CRL Abrufen:** A button.
- Initiale Seriennummer:** A text input field.
- Authority Info Access:** A text input field.
- OCSP URI:** A dropdown menu.
- CA Issuer:** A dropdown menu.
- Zertifikatrichtlinien:** A table with columns 'OID' and 'Certification Practice Statement'.
- Buttons:** 'Übernehmen' and 'Aktionen'.

Abb. 1.07: OCSP-Informationen in der signierenden CA eintragen

5 Upload des Zertifikats auf der genuscreen & OCSP-Responder-URL konfigurieren

Das unter Punkt 1 angelegte Zertifikat muss auf der genuscreen der genua GmbH hochgeladen werden und die OCSP-Responder-URL eingerichtet werden.

Navigieren Sie auf der genua genuscreen in der Menüleiste zu **VPN** und **IKEv2-Mobile-Einstellungen**.



Abb. 1.05: Navigation auf der genuscreen

➡ Scrollen Sie zu **AUTHENTISIERUNG/OCSP**.

➡ Laden Sie das Zertifikat über das **+** unter **OCSP RESPONDER ZERTIFIKATE** hoch.

- ➡ Geben Sie die OCSP-RESPONDER-URL im http-Format an. Sie finden sie im unter Punkt 3 angelegten OCSP URI-Objekt unter OCSP URI.
- ➡ Speichern Sie die Einstellungen und updaten Sie anschließend die genuscreen-Appliance.

IKEv2-Mobile-Einstellungen

Authentisierung/OCSP

IKE CA Zertifikate

Zertifikat ⓘ 🗑️

Zertifikat ⓘ 🗑️

Zertifikat ⓘ 🗑️

+ ⓘ

Intermediate CAs vertrauen ☒ ⓘ

OCSP Responder Zertifikate

Zertifikat ⓘ 🗑️

+ ⓘ

OCSP-Responder-URL ⓘ

Optionen

DNS-Server

NETBIOS-Server

DHCP-Server

MOBILE

Appliance updaten ^ ✓

Speichern Admin

Abb. 1.06: IKEv2-Mobile-Einstellungen: OCSP Responder Zertifikate