ECOS TrustManagementAppliance®

SMA/TMA-Migration V8

Anleitung

Version: 1.1

Datum: 09/2025

IT-Security Solutions

Made in Germany

ECOS TECHNOLOGY GMBH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel: +49 6133 939-0 | Fax: +49 6133 939-333

Inhalt

1 Migration der SMA für genuconnect zu TMA

Im Zuge der BSI-Zulassung für die ECOS **TrustManagementAppliance®** (TMA) wurde vom BSI eine Einsatzerlaubnis für die TMA ausgestellt. Die bisher eingesetzte System Management Appliance (SMA) ist deshalb nur noch bis zum 30.09.25 für die Verwaltung von genuconnect zugelassen und muss zu einer TMA migriert werden. Für die Migration einer SMA für genuconnect zu einer TMA stellt die Firma ECOS ein Migrationstool bereit.

Zusätzlich muss ab der Version 8 der TMA ein Smartcard-Reader für das Erzeugen von Zufall zur Verfügung stehen. Dieser Reader muss physisch an den VM-Host angeschlossen und an die VM durchgereicht werden.

2 Auszuführende Schritte

Bei allen nachfolgenden Schritten unterstützt Sie der ECOS Support gerne. Es besteht auch die Möglichkeit, die Migration in einem Remotetermin durchzuführen. Sie erreichen den ECOS Support unter support@ecos.de.

Die Migration läuft wie folgt ab (ergänzende Informationen zu einzelnen Schritten folgen weiter unten):

1. Prüfen des Smartcard-Readers wie unter 3.1 beschrieben.

2. Für die TMA sind neue Lizenzen erforderlich. Diese erhalten Sie kostenfrei von ECOS, soweit Sie gültige Lizenzen für die SMA für genuconnect haben.
   Bitte schreiben Sie dazu eine Mail an support@ecos.de mit folgenden Informationen:

   - Betreff: Lizenzanforderung für SMA/TMA-Migration
   - Kunde
   - Bisherige Seriennummer der Appliance (bei mehreren Appliances bitte alle Seriennummern angeben)

   Sollten Sie bis jetzt noch keine SMA für genuconnect oder TMA lizensiert haben, erhalten Sie ein Angebot für ein Upgrade.

3. Falls eine direkte Verbindung der SMA zum ECOS Update-Server besteht, können die Schritte 4 und 5 entfallen.

4. Download des Migrationstools über folgenden Link:
   https://files.update.ecos.de/sw/ecos/bbsecupdate_V8.0.4+migrate.tma.root

5. Einspielen des Migrationstool, wie ein gewöhnliches Update als **Software-Update-Image** auf der SMA.

6. Migrationstool (V8.0.4+migrate.tma), wie unter 3.2 beschrieben, einspielen.

   Das Tool entfernt die alten Lizenzen und bereitet die Umstellung auf die TMA vor.

7. Neue TMA-Lizenzen einspielen.

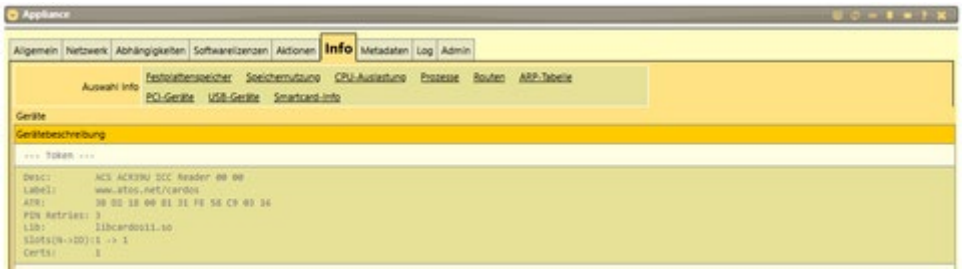
8. Update auf 8.0.4 einspielen (ab 8.0.4 kann die Smartcard zum Seeden des Zufalls benutzt werden).
   https://files.update.ecos.de/

9. Umstellung des PSS-Signaturschema für die DiskEncryption auf PKCS#1.5, wie unter 3.3 beschrieben

3 Erläuterungen

3.1 Prüfen des Smartcard-Readers

Um zu prüfen, ob ein Smartcard-Reader zur Verfügung steht, auf der SMA folgendes aufrufen: **Appliance-Objekt** → Reiter **Info** → **Smartcard-Info**



Bei Erfolg wird ein Reader mit einer Smartcard angezeigt, ansonsten bleibt die Anzeige leer. Wichtig ist, dass eine initialisierte CardOS-Smartcard mit der ATOS-Middleware verwendet wird, da auf der SMA nur diese zur Verfügung steht.

Entsprechend den SecOPs muss eine CardOS 5.4-Smartcard zum Einsatz kommen. Diese kann (kostenpflichtig) über ECOS bezogen werden.

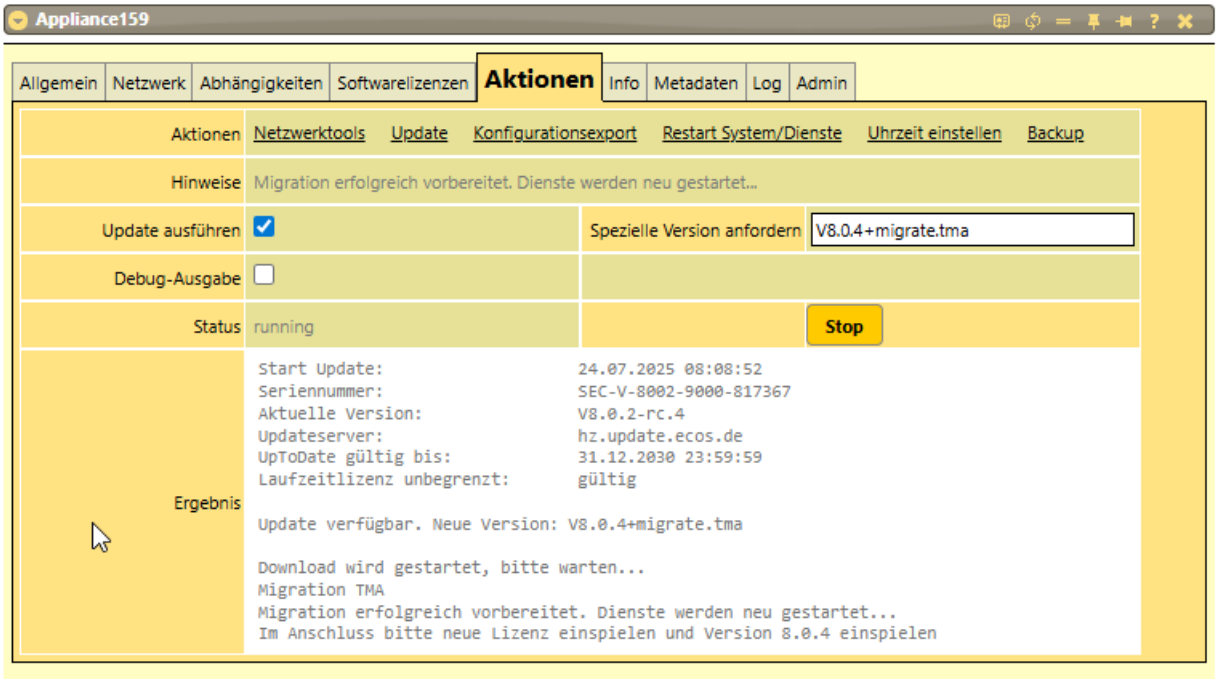
3.1.1 Besonderheiten bei einem ESXI-Host

Um das Durchreichen einer Smartcard auf einem ESXI-Host zu ermöglichen, muss zusätzlich ein Konfigurationseintrag erfolgen. Dieser wird auf dem ESXI-Host in der jeweiligen vmx-Datei der SMA-VM vorgenommen:

```
usb.generic.allowCCID = "TRUE"
```

3.2 Ausführen des Migrationstools

Für das Migrationstool wird der Update-Mechanismus im **Appliance-Objekt** verwendet. Als Version ist V8.0.4+migrate.tma anzugeben, wie in folgendem Screenshot gezeigt:



Der Text muss vollständig erscheinen, wie im Screenshot unter **Ergebnis** gezeigt, sonst war die Migration nicht erfolgreich. Das Migrationstool kann ggf. mehrfach gestartet werden.

3.3 Umstellung des PSS-Signaturschemas auf PKCS#1.5 für DiskEncryption

Für UTIMACO DiskEncryption muss nach einem Update der SMA/TMA auf V8.0.4 oder höher das Signaturschema der DiskEncryption-CA auf RSASSA-PKCS1-v1_5 umgestellt werden, da UTIMACO das neue Signaturschema RSASSA-PSS nicht unterstützt. Andernfalls können Zertifikate, die mit RSASSA-PSS signiert wurden, nicht in der UTIMACO POA hinzugefügt und verwendet werden.