

Firmware Update 2.0.47

Bei dem Update eines secunet Konnektors auf die Version 2.0.47 sind bestimmte Vorbedingungen PA1 und PA2 (vgl. unten) zu berücksichtigen. Die nachfolgende Tabelle zeigt abhängig von der installierten Firmware die notwendigen Prüfanweisungen, die VOR einem Update (sowohl bei Online Update als auch Offline Update) zu berücksichtigen sind.

Installierte Version	Prüfanweisung bei Update auf die Version 2.0.47
2.0.36	Zuerst Durchführung PA1, anschließend PA2, anschließen Update
2.0.37	Zuerst Durchführung PA1, anschließend PA2, anschließen Update
2.0.38	Zuerst Durchführung PA2 dann Durchführung Update auf 2.0.47
2.0.46	Durchführung Update auf 2.0.47



Die Einhaltung der Reihenfolge der Schritte insbesondere bei Versionen kleiner als 2.0.46 ist für einen reibungslosen Ablauf des Updates auf die Version 2.0.47 unerlässlich. Ein Abweichen von dieser Reihenfolge kann dazu führen, dass der Konnektor anschließend unbrauchbar ist.

PA1 EC_Security_Log_Not_Writeable

Bei dem Update eines Konnektor mit einer Firmware Version kleiner als 2.0.38 KANN der Konnektor sich in dem Fehlerzustandes EC_Security_Log_Not_Writeable befinden.

Sofern ein Konnektor den Fehlerzustand EC_Security_Log_Not_Writeable aufweist MUSS dieser Fehlerzustandes VOR dem Update auf die Firmware Version 2.0.47 beseitigt werden.

Der Fehlerzustand EC_Security_Log_Not_Writeable KANN auch während des Downloads vom KSR-Dienst auftreten. Der Update auf die Firmware Version 2.0.47 SOLL daher bei einer bestehenden Firmware Version kleiner als 2.0.38 über ein Offline Update erfolgen.

Schritt 1:

Anmelden an der Admin-Oberfläche des Konnektors:

- ▶ Die URL des secunet Konnektors in der Adresszeile des Browsers eingeben:

```
https://<IP-Adresse des secunet Konnektors>:8500/Management
```

- ▶ Benutzername und Passwort eingeben und Login

Schritt 2:

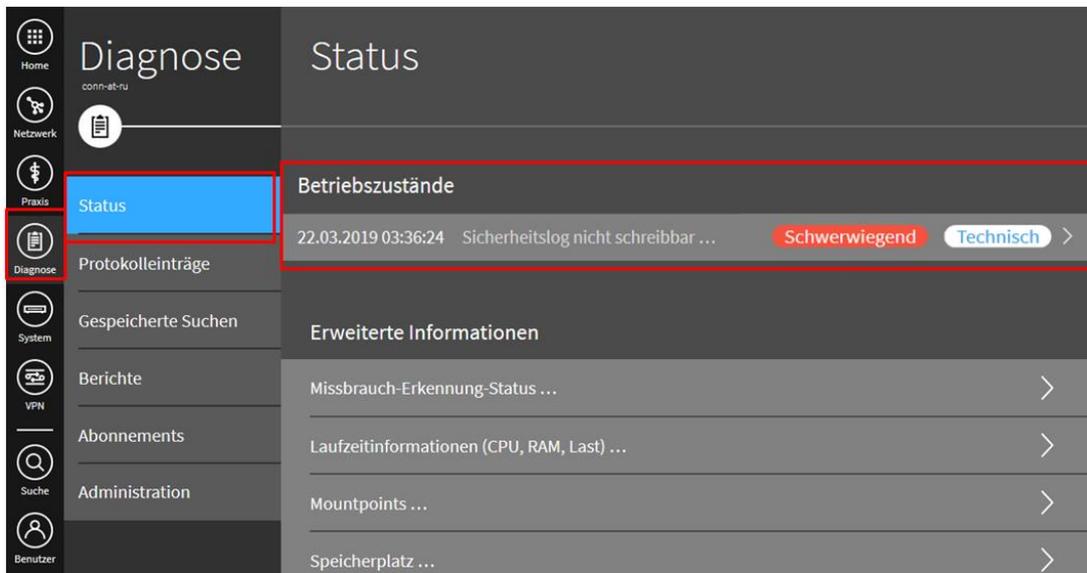
Nach dem Login wird zunächst die „Home“ Ansicht angezeigt

- ▶ Hier auf der linken Seite zunächst das Menu  „Diagnose“ anwählen
- ▶ Anschließend den Bereich „Status“ anwählen. In dem Bereich Status werden aktuell bestehende Betriebs- und Fehlerzustände angezeigt

Schritt 3:

Prüfen ob Konnektor den Fehlerzustand EC_Security_Log_Not_Writeable aufweist

Die nachfolgende Abbildung zeigt einen Konnektor mit dem Sicherheitsprotokoll nicht schreibbar ist. Also dem Fehlerzustand EC_Security_Log_Not_Writeable.



Wenn der Konnektor, welcher auf die Version 2.0.47 aktualisiert werden soll, sich in dem Fehlerzustand EC_Security_Log_Not_Writeable befindet (wie oben dargestellt)

- ▶ weiter mit Schritt 4, um den Fehlerzustand zu beheben

Wenn der Konnektor, welcher auf die Version 2.0.47 aktualisiert werden soll, sich NICHT in dem Fehlerzustand EC_Security_Log_Not_Writeable befindet

- ▶ sind im Rahmen der Prüfanweisung PA1 keine weiteren Schritte erforderlich

Schritt 4:

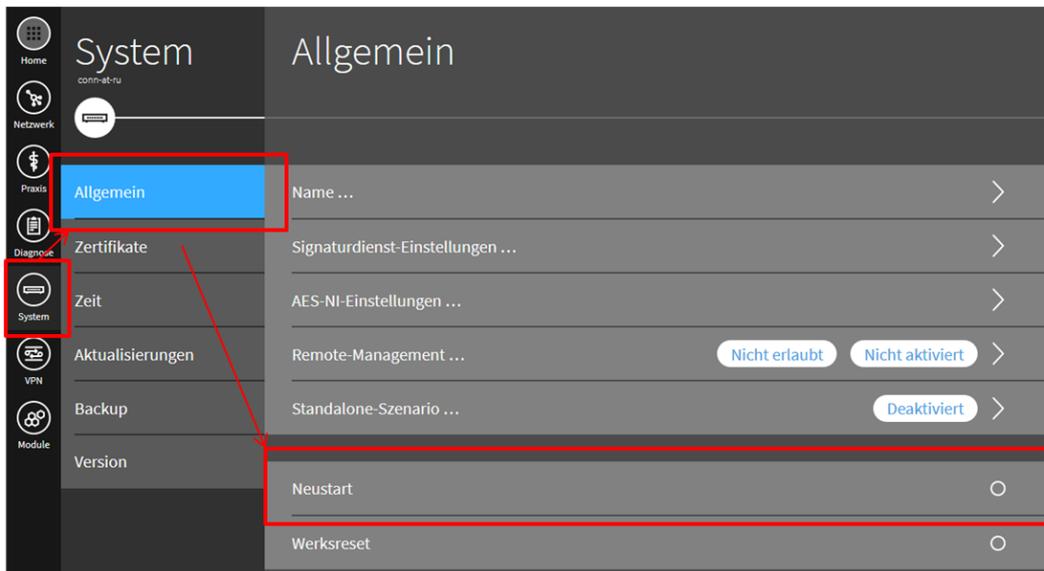
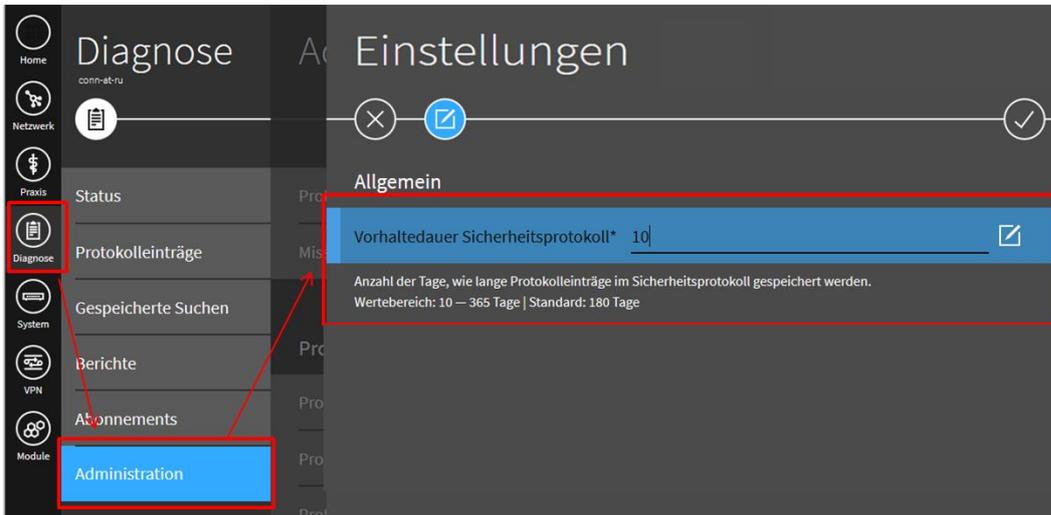
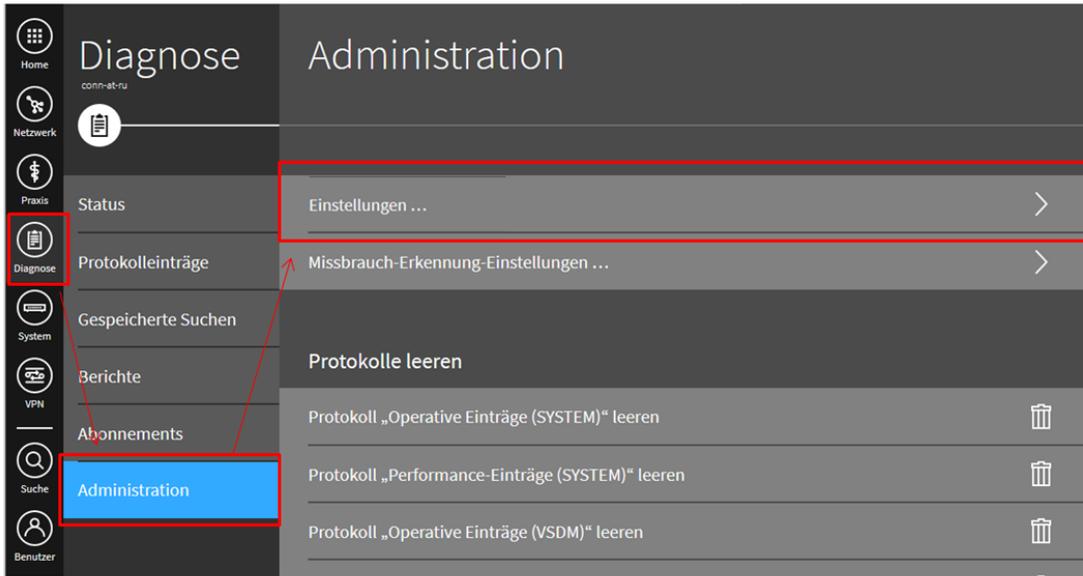
Reduzieren der Vorhaltdauer des Sicherheitsprotokolls auf 10 Tage

- ▶ In  „Diagnose“ den Bereich „Administration“ auswählen
- ▶ In „Administration“ den Eintrag „Einstellungen“ auswählen
- ▶ Reduzieren Vorhaltdauer des Sicherheitsprotokolls auf 10 Tage

Schritt 5:

Konnektor neu starten, damit der Zustand Fehlerzustand aufgehoben wird

- ▶ Auf der linken Seite zunächst das  Menu „System“ auswählen
- ▶ In dem Bereich „Allgemein“ den „Neustart“ auswählen



Schritt 6:

Sobald der Konnektor nach dem Neustart wieder betriebsbereit ist erneut an der Admin-Oberfläche des Konnektors anmelden:

- ▶ Die URL des secunet Konnektors in der Adresszeile des Browsers eingeben:

`https://<IP-Adresse des secunet Konnektors>:8500/Management`

- ▶ Benutzername und Passwort eingeben und Login

Schritt 7:

Nach dem Login wird zunächst die „Home“ Ansicht angezeigt

- ▶ Hier auf der linken Seite zunächst das Menu  „Diagnose“ anwählen
- ▶ Anschließend den Bereich „Status“ anwählen. In dem Bereich Status werden aktuell bestehende Betriebs- und Fehlerzustände angezeigt

Schritt 8:

Prüfen ob Fehlerzustand EC_Security_Log_Not_Writeable behoben wurde

- ▶ Es sind im Rahmen der Prüfanweisung PA1 keine weiteren Schritte mehr erforderlich, wenn der Fehlerzustand behoben werden konnte

Schritt 9:

Nach einem erfolgreichen Update auf die FW Version 2.0.47 kann die Vorhaltdauer des Sicherheitsprotokolls wieder auf den Default Wert gesetzt werden

- ▶ In  „Diagnose“ den Bereich „Administration“ anwählen
- ▶ In „Administration“ den Eintrag „Einstellungen“ auswählen
- ▶ Einstellen Vorhaltdauer des Sicherheitsprotokolls auf 180 Tage

PA2 Netzwerke der Einsatzumgebung

Bei dem Update eines Konnektor mit einer Firmware Version kleiner als 2.0.46 MUSS sichergestellt sein, das ALLE in der Einsatzumgebung verwendeten Netzbereiche VOR dem Update in der Konnektor Konfiguration hinterlegt wurden.

Ansonsten sind Komponenten der Einsatzumgebung (wie z.B. Arbeitsplätze und Kartenterminals) in Netzbereichen, die dem Konnektors nicht explizit bekannt gemacht wurden NACH einem Update auf die Firmware Version 2.0.47 nicht mehr erreichbar.

Schritt 1:

Anmelden an der Admin-Oberfläche des Konnektors:

- ▶ Die URL des secunet Konnektors in der Adresszeile des Browsers eingeben:

`https://<IP-Adresse des secunet Konnektors>:8500/Management`

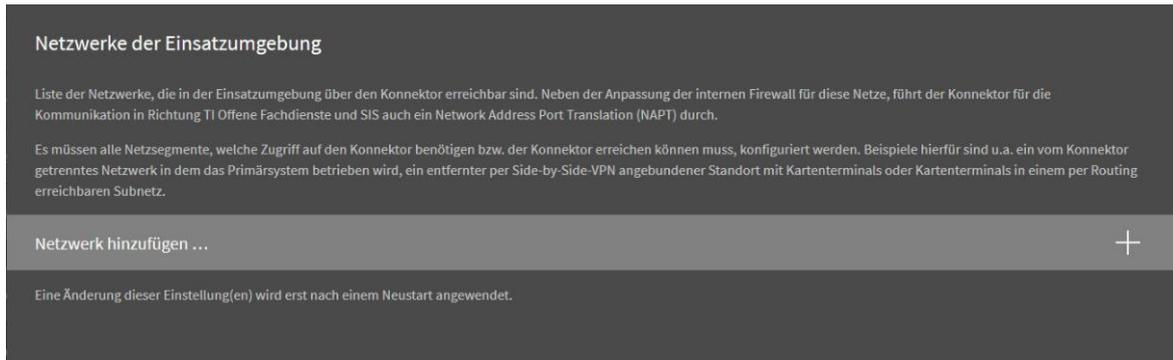
- ▶ Benutzername und Passwort eingeben und Login

Schritt 2:

Nach dem Login wird zunächst die „Home“ Ansicht angezeigt

- ▶ Hier auf der linken Seite zunächst das Menu  „VPN“ anwählen
- ▶ Anschließend den Bereich „Status“ anwählen. In dem Bereich Status werden aktuell bestehende Betriebs- und Fehlerzustände angezeigt

VPN -> VPN-Zugangsdienst Netzwerk-Segmente -> Netzwerke der Einsatzumgebung



Schritt 3:

Prüfen ob ALLE Netzbereichen, in dem sich Komponenten der Einsatzumgebung befinden (wie z.B. Arbeitsplätze und Kartenterminals) angezeigt werden.

Wenn JA, sind keine weiteren Schritt nötig. Wenn NEIN, weiter mit Schritt 4.

Schritt 4:

ALLE Netzbereichen, in dem sich Komponenten der Einsatzumgebung befinden (wie z.B. Arbeitsplätze und Kartenterminals) eintragen und abschließend die Liste mit OK (Haken in der Unterseite) bestätigen.

Schritt 5

Sofern die Netze erfolgreich hinzugefügt wurden, fordert der Konnektor zum Neustart auf. Diesen durchführen und im Anschluss die Liste der Netze nochmal abschließend überprüfen.

Durchführung Update auf 2.0.47

Bei einer aktiven VPN TI Verbindung können die für ein Update auf 2.0.47 benötigten Dateien über den Konfigurationsdienst (KSR) auf den Konnektor geladen werden.

Alternativ können die für ein Update auf die FW Version 2.0.47 benötigten Dateien aber auch über ein Datei Upload auf den Konnektor geladen werden. Dazu muss das FW Version 2.0.47 zunächst auf ein Client System in der Umgebung des Leistungserbringers und von hier anschließend in den Konnektor hochgeladen werden. Diese Variante wird für Konnektoren mit einem vorhergehenden Fehlerzustand EC_Security_Log_Not_Writeable empfohlen.

Zur Durchführung des Offline-Updates ist eine direkte Netzwerkverbindung zwischen dem Modularen Konnektor und dem zu dessen Administration verwendeten Gerät erforderlich. Ein Offline-Update ist nicht über Remote Management möglich.

Informationen über verfügbare Updates erhalten Sie nur auf der Webseite des Herstellers (<https://www.secunet.com/de/produkte/konnektor/einboxkonnektor/> und unter <https://www.secunet.com/de/produkte/konnektor/rechenzentrumskonnektor/> für Rechenzentrumskonnektoren). Es dürfen nur von der gematik zugelassene Updates für den Modularen Konnektor eingespielt werden.

- ▶ Rufen Sie den zur Entschlüsselung des Updates erforderlichen Schlüssel bei Ihrem Vertragspartner für den VPN-Zugangsdienst ab.
- ▶ Laden Sie ein für die verwendete Geräteversion geeignetes Update von der Webseite des Herstellers herunter und speichern Sie es auf dem Clientsystem.
- ▶ Entschlüsseln und Entpacken Sie das Update (AES256 verschlüsseltes ZIP-Archiv) auf dem Clientsystem.

Danach verfahren Sie wie im Handbuch Kapitel 11.11.4 (Offline Update) beschrieben.