

# RELIAS||LEARNING

## Abschnitt 1: Einführung

- A. Einleitung
- B. Lernziele
- C. Remote-Management

## Abschnitt 2: Diagnose- und Statusinformationen einsehen

- A. Statusinformationen
- B. Protokolleinträge
- C. In Protokolleinträgen suchen
- D. Gezielte Suche
- E. Berichte
- F. Administration
- G. Überprüfen Sie Ihr Wissen

## Abschnitt 3: System

- A. Allgemein
- B. Zertifikate
- C. Zeit
- D. Aktualisierungen
- E. Backup
- F. Version

## Abschnitt 4: Betriebliche Prozesse

- A. Rücknahme der Freischaltung (Deregistrierung)
- B. Sperrung eines Konnektors
- C. Außerbetriebnahme
- D. Konnektortausch

## Abschnitt 5: Schluss

- A. Mitwirkende
- B. Weiterführende Literatur
- C. Quellennachweise
- D. Fast geschafft

## Abschnitt 1: Einführung

### Einleitung

Diese Lerneinheit beinhaltet wichtige Informationen zur Unterstützung des laufenden Betriebs des Konnektors, zum Support durch den Dienstleister vor Ort (DVO) und zum User Helpdesk.

# Betrieb des Konnektors

## Lernziele

Nachdem Sie diese Lerneinheit absolviert haben, sollten Sie folgende Fähigkeiten erworben haben:

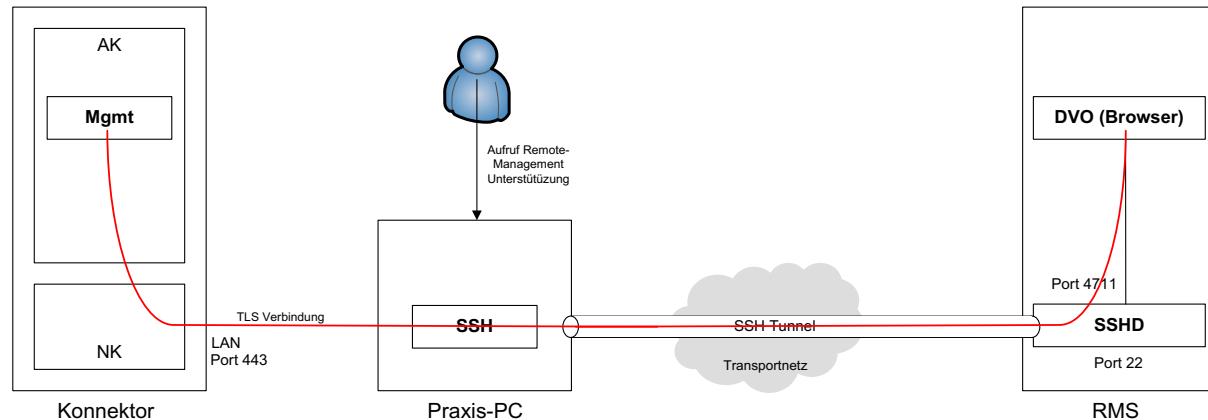
1. Sie können Informationen über den laufenden Betrieb eines Konnektors sicher finden und korrekt interpretieren.
2. Sie können die verschiedenen Systemeinstellungen auf der Bedienoberfläche des Konnektors finden.
3. Sie können Aktualisierungen der verschiedenen Geräte durchführen.
4. Sie können Backups erstellen und abrufen.
5. Sie kennen die Unterschiede zwischen den wichtigsten betrieblichen Prozessen in Bezug auf den Umgang mit dem Konnektor.

## Remote-Management

Remote-Management ermöglicht die Durchführung notwendiger Administrationsaufgaben durch den DVO, ohne dass ein Vor-Ort-Termin notwendig ist.

Über das Remote-Management kann ein Benutzer mit der Rolle „Remote-Administrator“ den Konnektor administrieren. Der Remote-Administrator hat die gleichen Rechte und Möglichkeiten wie ein lokaler Administrator. Ausgenommen sind hierbei Rechte zur Durchführung eines Werksresets und zur Benutzerverwaltung.

Die Kommunikation zwischen dem DVO und der Managementschnittstelle erfolgt unter Verwendung eines Transport Layer Security (TLS)-Kanals. Der Aufbau des Secure Shell (SSH)-Tunnels zwischen dem Praxis-PC und dem Secure Shell Server (SSHD) des Remote-Management-Servers (RMS) wird durch das Praxispersonal initiiert.



Remote-Management erlaubt die Nutzung folgender Funktionen zur Unterstützung des Service und Supports des Konnektors:

- das Konfigurationsmanagement,
- die Durchführung von Administrationsaufgaben zur Fernwartung,
- den Abruf von Diagnoseinformationen zum Zustand des Konnektors und der Umsysteme und
- die Einsicht und den Abruf von Protokolldateien zur Supportunterstützung.

Über das Konfigurationsmanagement können alle Funktionen der Managementschnittstelle des Konnektors genutzt werden und die Konfiguration des Konnektors kann über das Remote-

# Betrieb des Konnektors

Management angepasst werden. Das Remote-Management nutzt hierfür die Oberfläche der lokalen Managementschnittstelle des Konnektors.

## Abschnitt 2: Diagnose- und Statusinformationen einsehen

### Statusinformationen

Klicken Sie auf den Menüpunkt **Diagnose**.

#### Betriebszustände des Konnektors

Unter **Status** werden in der Management-Oberfläche Fehler zu den Betriebszuständen des Konnektors angezeigt. Die **Fehlerzustände** unterscheiden sich nach **Typ (Operativer Eintrag oder Sicherheitseintrag)** und **Schwere (Info, Warning, Error oder Fatal)**. Jeder Fehlerzustand wird durch eine eindeutige **ErrorCondition** identifiziert, z. B. **EC\_CRL\_Out\_Of\_Date**.

Eine komplette Liste der Fehler zu den Betriebszuständen des Konnektors mit entsprechenden Handlungsempfehlungen kann unter **Ressourcen** abgerufen werden.

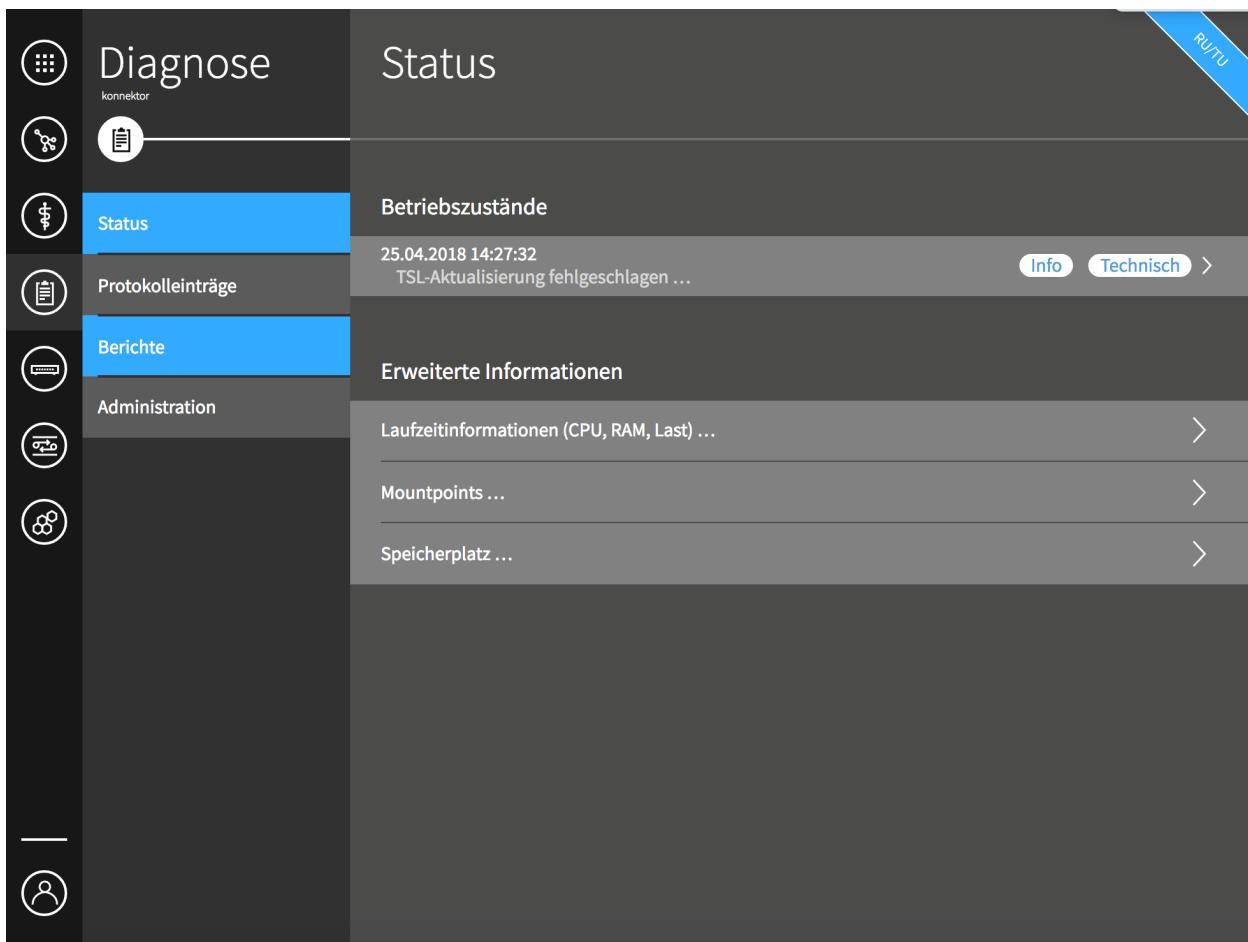


Abbildung 1: Anzeige Konnektorstatus

Unter den erweiterten Informationen werden folgende Diagnose- und Statusinformationen angezeigt:

- Laufzeitinformationen (CPU, RAM, Last) ...
- Mountpoints ...

# Betrieb des Konnektors

- Speicherplatz ...

Klicken Sie auf die verschiedenen Schaltflächen, um mehr darüber zu erfahren.

Unter **Laufzeitinformationen (CPU, RAM, Last)** ... werden Informationen zur CPU, zur Last und zum Arbeitsspeicher des Konnektors angezeigt.

Der Punkt **Mountpoints** ... zeigt die gemounteten Dateisysteme des Konnektors.

Unter **Speicherplatz** ... werden Informationen zum Speicherplatz der verschiedenen Dateisysteme angezeigt.

## Protokolleinträge

Der Protokollierungsdienst des Konnektors erfasst die folgenden Ereignisse:

- system- und sicherheitsrelevante Ereignisse, z. B. Änderungen an der Firewall-Konfiguration, Authentisierungsfehler,
- Ereignisse im Kontext der Performancemessung innerhalb des Konnektors und
- Ereignisse von Fachmodulen.

Als Sicherheitseinträge werden Ereignisse protokolliert, die Auswirkungen auf Sicherheitsmerkmale des Konnektors haben können. Ereignisse im Kontext der Performancemessung innerhalb des Konnektors werden in Performance-Einträgen protokolliert. Ereignisse im Kontext der Performancemessung von Fachmodulen werden als Performance-Einträge in das Fachmodul-Protokoll geschrieben. Alle anderen Ereignisse werden als operative Einträge in das Systemprotokoll oder die Fachmodulprotokolle geschrieben.

Derzeit existieren folgende Protokolle im Konnektor:

- Systemprotokoll und
- VSDM-Fachmodulprotokoll,

jeweils untergliedert in folgende Protokolltypen:

- operative Einträge,
- Sicherheitseinträge und
- Performance-Einträge.

Da es Sicherheitseinträge nur bezogen auf den Konnektor gibt, existiert kein Sicherheitsprotokoll für Fachmodule.

Die Protokolleinträge werden in fünf Schweregrade unterteilt:

- Debug,
- Info,
- Warnung,
- Fehler/ERROR und
- Fatal.

# Betrieb des Konnektors

Zeit	Level	Nachricht
29.03.2018 13:05:33.626	ERROR	topic=OPERATIONAL_STATE/EC_CardTerminal_Not_Available(\$Ctid);Value=false;Ctid=0dac9d1b-f5a4-4558-a268-d3d465419299;Bedeutung=Bekanntes Kartenterminal (0dac9d1b-f5a4-4558-a268-d3d465419299) ist nicht v...
29.03.2018 13:05:31.494	ERROR	topic=OPERATIONAL_STATE/EC_CardTerminal_Not_Available(\$Ctid);Value=true;Ctid=0dac9d1b-f5a4-4558-a268-d3d465419299;Bedeutung=Bekanntes Kartenterminal (0dac9d1b-f5a4-4558-a268-d3d465419299) ist nicht v...
29.03.2018 12:56:00.041	ERROR	topic=OPERATIONAL_STATE/EC_CardTerminal_Not_Available(\$Ctid);Value=false;Ctid=0dac9d1b-f5a4-4558-a268-d3d465419299;Bedeutung=Bekanntes Kartenterminal (0dac9d1b-f5a4-4558-a268-d3d465419299) ist nicht v...
29.03.2018 12:55:57.903	ERROR	topic=OPERATIONAL_STATE/EC_CardTerminal_Not_Available(\$Ctid);Value=true;Ctid=0dac9d1b-f5a4-4558-a268-d3d465419299;Bedeutung=Bekanntes Kartenterminal (0dac9d1b-f5a4-4558-a268-d3d465419299) ist nicht v...
29.03.2018 12:53:56.749	ERROR	topic=OPERATIONAL_STATE/EC_CardTerminal_Not_Available(\$Ctid);Value=false;Ctid=0dac9d1b-f5a4-4558-a268-d3d465419299;Bedeutung=Bekanntes Kartenterminal (0dac9d1b-f5a4-4558-a268-d3d465419299) ist nicht v...
29.03.2018 12:53:54.616	ERROR	topic=OPERATIONAL_STATE/EC_CardTerminal_Not_Available(\$Ctid);Value=true;Ctid=0dac9d1b-f5a4-4558-a268-d3d465419299;Bedeutung=Bekanntes Kartenterminal (0dac9d1b-f5a4-4558-a268-d3d465419299) ist nicht v...
29.03.2018 12:48:23.281	ERROR	topic=OPERATIONAL_STATE/EC_CardTerminal_Not_Available(\$Ctid);Value=false;Ctid=0dac9d1b-f5a4-4558-a268-d3d465419299;Bedeutung=Bekanntes Kartenterminal (0dac9d1b-f5a4-4558-a268-d3d465419299) ist nicht v...

Abbildung 2: Protokolleinträge des Konnektors

In der Übersicht der Protokolleinträge werden die operativen Einträge aus dem Systemprotokoll mit Zeitstempel, dem Schweregrad und der Protokollierungsnachricht angezeigt. Klicken Sie auf den obersten Protokolleintrag, um den vollständigen Eintrag zu sehen. Der vollständige Eintrag wird jetzt angezeigt.

Typ OP

Zeit 13.04.2018 10:24:39.162

Protokollierungslevel ERROR

Nachricht

```
code=4033
name=NO_ANSWER_FROM_TERMINAL
text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen
Vorgangsnummer=1523283293269_1112849478549632_-1286921659
```

Abbildung 3: Details zu Protokolleintrag

## In Protokolleinträgen suchen

Im Bereich **Suche** können die protokollierten Meldungen durchsucht und angezeigt werden. Klicken Sie auf **Suchfilter anpassen ...**, um zu diesem Bereich zu gelangen. Hier können die Suchkriterien festgelegt werden. Die Suche wird daraufhin automatisch durchgeführt und die gefundenen Meldungen werden angezeigt.

Dabei stehen folgende Filterkriterien zur Verfügung:

# Betrieb des Konnektors

## Protokoll

Das Protokoll, aus dem Einträge gezeigt werden sollen. „SYSTEM“ ist der Anwendungskonnektor selbst, alle anderen sind konfigurierte Fachmodule. Derzeit steht als Fachmodulprotokoll VSDM zur Auswahl.

## Typ

Typ der Protokolleinträge:

- operative Einträge,
- Sicherheitseinträge oder
- Performance-Einträge.

## Protokollierungslevel

Der Detaillierungsgrad des Protokolls wird durch die Festlegung der Mindest-Schwere der Einträge bestimmt. Zur Auswahl stehen:

- Debug,
- Info,
- Warnung,
- Fehler/ERROR oder
- Fatal.

## Zeitraum Schnellauswahl

Die Werte dieser Auswahl berechnen Werte für von/bis. Zur Auswahl stehen diese Werte:

- Letzte Stunde
- Letzte 3 Stunden
- Letzte 8 Stunden
- Letzte 24 Stunden
- Heute
- Gestern
- Letzte 7 Tage

## Zeitpunkt von/bis

Von: Zeitpunkt, ab dem Protokolleinträge gesucht werden sollen.

Bis: Zeitpunkt, bis zu dem Protokolleinträge gesucht werden sollen. Ein leeres Feld ist gleichbedeutend mit unendlich.

## Suchbegriffe

Definiert einen Suchbegriff. Wenn der Suchbegriff nur Teil des Eintrags ist muss er mit Platzhaltern umgeben werden. In der Zeichenkette dürfen die folgenden Platzhalter vorkommen:

- „%“ für 0, 1 oder n Zeichen und
- „\_“ für ein Zeichen oder eine Ziffer.

Der Platzhalter "Prozent", vor und nach dem Suchbegriff, wird vom System automatisch gesetzt und muss nicht eingegeben werden.

## Genaue Übereinstimmung Suchbegriff

# Betrieb des Konnektors

Bei genauer Übereinstimmung muss der Such-String mit dem Protokolleintrag übereinstimmen. Es können hierbei keine Wildcards verwendet werden.

## Reihenfolge aufsteigend

Bei Aktivierung werden die Protokolleinträge von alt nach neu sortiert.

## Einträge pro Seite

Anzahl von Einträgen pro Seite. Zur Auswahl stehen:

- 10
- 25
- 50
- 100

## Gezielte Suche

Sie wissen, dass es gestern einen bestimmten Fehlercode gab und möchten diesen erneut prüfen.

Navigieren Sie zum Bereich **Suche**, um gezielt nach dem richtigen Protokolleintrag zu suchen.

Sie wissen Folgendes über den Fehler:

- Es handelte sich um einen operativen Eintrag im Systemprotokoll.
- Der Fehler beinhaltete Code=4033.
- Der Fehler trat innerhalb der letzten 24 Stunden auf.

Stellen Sie die Suchkriterien so ein, dass Sie möglichst präzise nach dem Fehlercode suchen. Nutzen Sie bitte die Schnellauswahl für den Zeitraum. Den passenden Suchbegriff haben wir Ihnen bereits vorgegeben. Unter **Protokoll** wird **SYSTEM** ausgewählt. Als **Typ** werden **Operative Einträge** verwendet. Als **Zeitraum** wird über die Schnellauswahl **Letzte 24 Stunden** ausgewählt. Das **Protokollierungslevel** wird auf **Fehler** gesetzt.

Da mithilfe von Wildcards gesucht wird, wird das Kriterium **Genaue Übereinstimmung beim Suchen** nicht aktiviert.

# Betrieb des Konnektors

The screenshot shows a search interface for protocol entries. At the top, there is a search bar with a magnifying glass icon and a checkmark icon. Below the search bar, there are several filter options:

- Protokoll\***: SYSTEM (selected)
- Typ\***: Operative Einträge (selected)
- Protokollierungslevel**: Fehler
- Zeitraum (Schnell-Auswahl)**: Von 10.04.2018 11:01:00 bis Zeitpunkt ab dem Protokolleinträge gesucht werden sollen; Bis Zeitpunkt bis dem Protokolleinträge gesucht werden sollen. Optional: Unbegrenzt, wenn leer.
- Suchbegriff**: %code=4033% (checkbox checked)

Below these filters, there is a note: "Definiert einen Suchbegriff. Wenn der Suchbegriff nur Teil des Eintrags ist muss er mit Platzhaltern umgeben werden. Es dürfen die beiden Platzhalter „%“ (0, 1 oder n Zeichen) und „\_“ (ein Zeichen oder Ziffer) in der Zeichenkette vorkommen. Beispiel: „%topic=MGM/ADMINCHANGES“, „%code=4002%“".

Abbildung 4: Suchfilter Protokolleinträge

Mit Klick auf **Bestätigen** werden die Protokolleinträge gemäß den eingestellten Suchkriterien gefiltert und das Ergebnis angezeigt.

The screenshot shows the results of the search. At the top, there is a header "Protokolleinträge" with a back arrow icon. Below the header, there is a navigation bar with icons numbered 1 through 8 and a greater than icon. The next button is highlighted in blue.

Below the navigation bar, there is a link "Suchfilter anpassen ... >".

At the bottom of the screen, there is a toolbar with buttons for **SYSTEM**, **Operative Einträge**, **Fehler**, and the date **11.04.2018 06:03:40**.

Zeit	Level	Nachricht
11.04.2018 11:00:27.846	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 10:59:24.835	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 10:40:21.828	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 10:30:18.821	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 10:10:15.813	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 10:10:12.805	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 10:00:09.797	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 09:50:06.791	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 09:40:03.784	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 09:30:00.776	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 09:19:57.769	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 09:09:54.762	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 08:59:51.754	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659
11.04.2018 08:49:48.764	ERROR	code=4033;name=NO_ANSWER_FROM_TERMINAL;text=Kartenterminal antwortet nicht, Zufügen fehlgeschlagen;Vorgangsnummer=1523283293269_1112849478549632_-1286921659

# Betrieb des Konnektors

Abbildung 5: Suchergebnis mit Protokolleinträgen

Optional können die gefundenen Meldungen exportiert und heruntergeladen werden:

- Mit **Download ...** werden die Meldungen als Textdatei gespeichert.
- Mit **Download komprimiert (gzip) ...** werden die Meldungen als komprimiertes Archiv gespeichert.



Abbildung 6: Protokolleinträge herunterladen

## Berichte

Klicken Sie auf den Bereich **Berichte**. Dort können spezifische vorkonfigurierte Berichte erstellt und heruntergeladen werden.

Derzeit steht hier der Performanz-Bericht VSDM zur Überprüfung der Bearbeitungszeiten der Fachanwendung VSDM als vorkonfigurierter Bericht zur Verfügung.

Über **Zeitraum (Schnell-Auswahl)** oder die Eingabe der Zeitpunkte von/bis kann der Zeitraum für den Bericht konfiguriert werden.

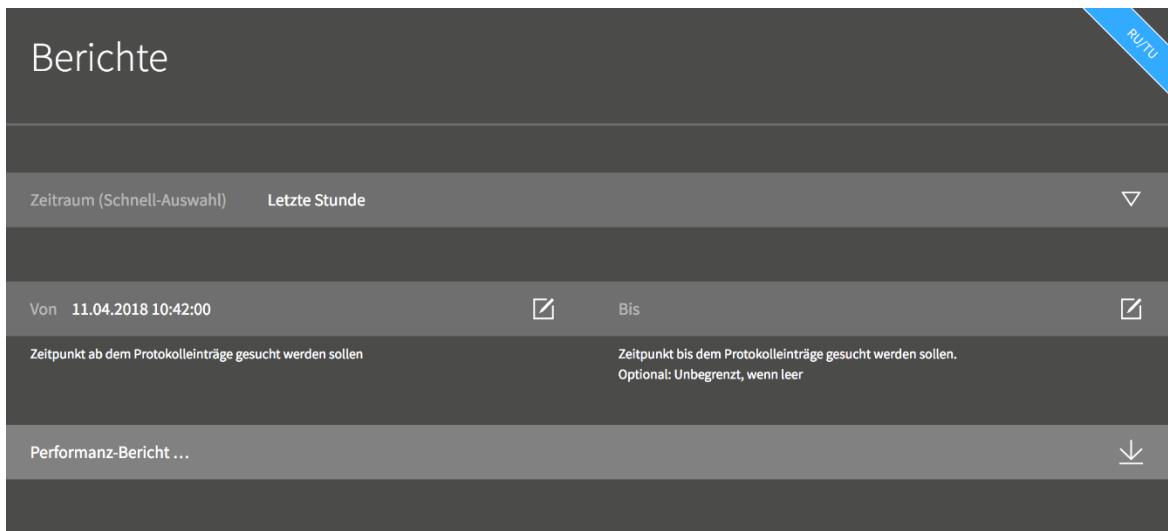


Abbildung 7: Neue Maske

## Administration

Klicken Sie auf den Bereich **Administration**.

Hier können Einstellungen für die Protokollierung vorgenommen und Protokolleinträge manuell geleert werden.

Einträge im Sicherheitsprotokoll können nicht geleert werden.

Andere Protokolleinträge werden nach der konfigurierten Vorhaltezeit automatisch vom Konnektor gelöscht.

# Betrieb des Konnektors

Ist der Speicherplatz für Protokolle erschöpft, überschreibt der Konnektor auch Einträge, die nicht älter als die konfigurierte Vorhaltezeit sind. Neue Logeinträge überschreiben dabei Logeinträge mit gleichem oder niedrigerem Schweregrad. Beim Überschreiben von Logeinträgen, die nicht älter als die Vorhaltezeit sind, wird der Fehlerzustand EC\_LOG\_OVERFLOW ausgelöst.

Zur Behebung des Fehlerzustandes können die Protokolle manuell geleert werden.

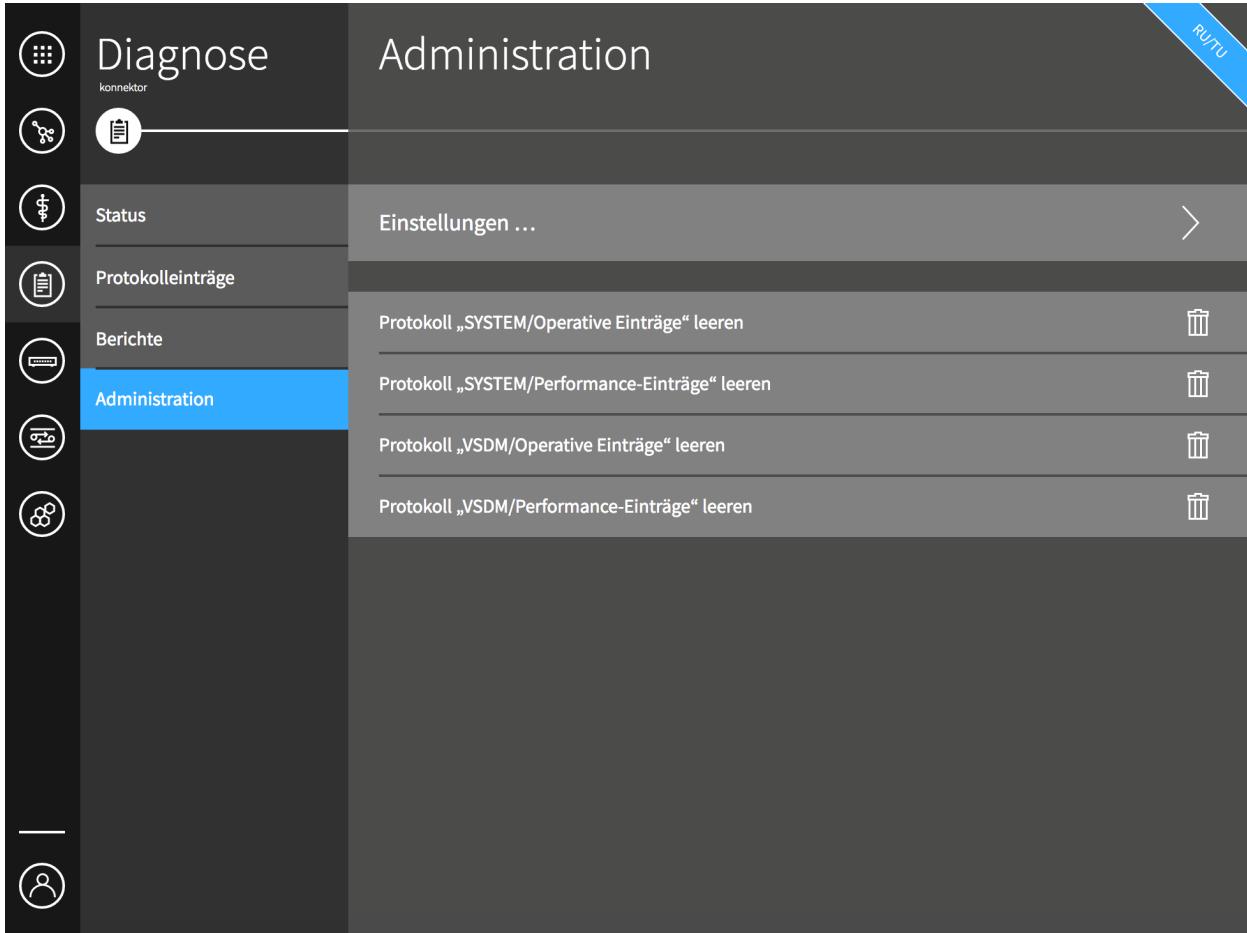


Abbildung 8: Administration Diagnose

Klicken Sie auf die Schaltfläche **Einstellungen** ...

Im Bereich **Allgemein** lassen sich Einstellungen für die Protokollierung im Sicherheitsprotokoll vornehmen. Der Schalter **Erfolgreiche Kryptooperationen protokollieren** aktiviert die Protokollierung erfolgreich durchgeföhrter Kryptooperationen im Sicherheitsprotokoll. Über den Parameter **Vorhaltezeit Sicherheitsprotokoll** wird die Anzahl der Tage festgelegt, nach denen Protokolleinträge aus dem Sicherheitsprotokoll automatisch gelöscht werden.

# Betrieb des Konnektors



Abbildung 9: Diagnose Administration Einstellungen Allgemein

Im Bereich **SYSTEM** können Einstellungen für das Systemprotokoll vorgenommen werden. Über die Drop-Down-Liste **Protokollierungslevel** kann die Mindest-Schwere der zu protokollierenden Einträge bestimmt werden. Die Vorhaltezeit legt die Speicherzeit der Einträge für das Systemprotokoll fest. Zudem kann eingestellt werden, ob das Performance-Log aktiviert werden soll, um Werte der Performance-Messung des Konnektors zu protokollieren.



Abbildung 10: Diagnose Administration Einstellungen System

## VSDM

# Betrieb des Konnektors

Unter VSDM können spezifische Informationen für das VSDM Fachmodulprotokoll eingestellt werden. Wie im Bereich System können das Protokollierungslevel, die Vorhaltezeit und die Aktivierung des Performance-Log konfiguriert werden.

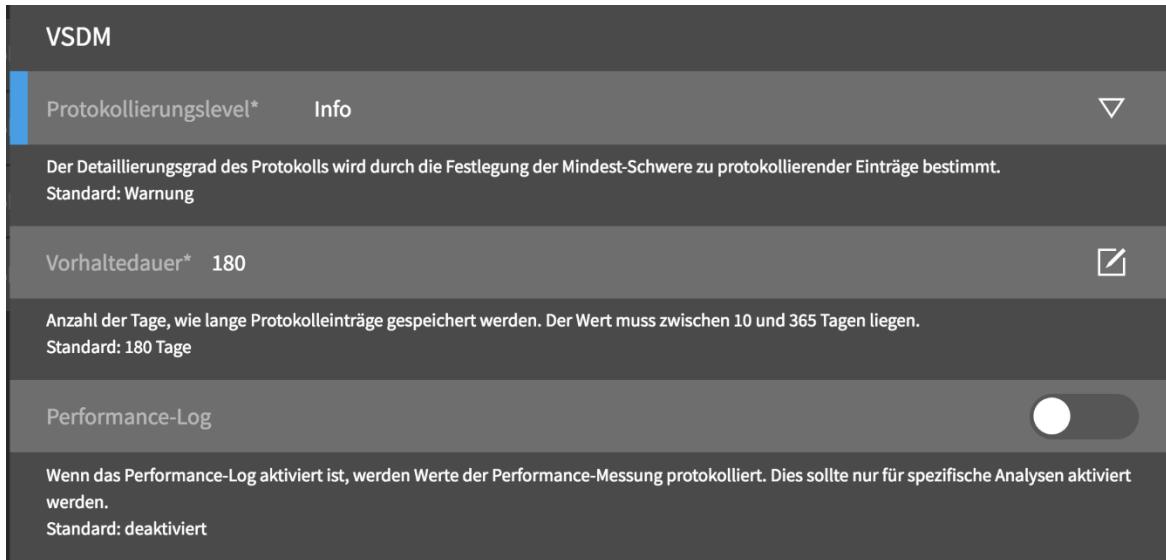


Abbildung 11: Diagnose Administration Einstellungen VSDM

## Überprüfen Sie Ihr Wissen

1. Ein Konnektor zeigt häufig den Fehlerzustand EC\_LOG\_OVERFLOW. Was sollten Sie tun, nachdem Sie zum wiederholten Mal manuell die Protokollspeicher geleert haben?
  - a) Den Speicherplatz erhöhen, indem Sie externe Speichermedien anschließen.
  - b) Die Administrationseinstellungen zur Protokollierung überprüfen.**
  - c) Den Konnektor ersetzen, da er offensichtlich defekt ist.
  - d) Einen Werksreset durchführen.

Feedback:

Bei a): Sie sollten nicht versuchen, externe Geräte an den Konnektor anzuschließen, die nicht explizit dafür vorgesehen sind. Anscheinend werden übermäßig viele Protokolle produziert. Die richtige Antwort wäre daher, die Einstellungen der Protokolladministration zu prüfen.

Bei b): Da es so scheint, als würden übermäßig viele Protokolle produziert, ist dies eine gute Idee.

Bei c): Bevor Sie diesen Schritt wählen, sollten Sie überprüfen, ob das Gerät gut konfiguriert ist. Anscheinend werden übermäßig viele Protokolle produziert. Die richtige Antwort wäre daher, die Einstellungen der Protokolladministration zu prüfen.

Bei d): Dies wäre ein relativ drastischer Schritt, der eine komplette Neukonfiguration erforderlich machen würde. Anscheinend werden übermäßig viele Protokolle produziert. Die richtige Antwort wäre daher, die Einstellungen der Protokolladministration zu prüfen.

2. Navigieren Sie durch die Bedienoberfläche, bis Sie zu den Einstellungen der Administration der Protokolleinträge gelangen.
3. Überprüfen Sie jetzt die Konfiguration der Protokolle. Stellen Sie die Standardeinstellungen bei den einzelnen Parametern wieder her, falls dies nötig sein sollte und bestätigen Sie Ihre Eingabe. Hinweise auf die Standardwerte finden Sie unter

# Betrieb des Konnektors

den verschiedenen Einstellungsmöglichkeiten.

## Feedback:

Wenn alles richtig gemacht wurde: Sehr gut. In Zukunft werden weniger Protokolleinträge erstellt, sodass der Speicherplatz für Protokolle wieder ausreichen sollte.

Wenn nicht alles korrekt eingestellt wurde: Überprüfen Sie die Einstellungen noch einmal. Anscheinend haben Sie noch nicht alle Standardwerte wieder eingegeben.

Hinweise auf die Standardwerte finden Sie unter den verschiedenen Einstellungsmöglichkeiten. Überprüfen Sie die Einstellungen auf allen drei Bildabschnitten.

## Abschnitt 3: System

### Allgemein

Klicken Sie auf das Menü **System**.

Im Bereich **Allgemein** kann unter **Name ...** die Bezeichnung des Konnektors festgelegt werden. Remote-Management und Standalone-Szenario wurden bereits in den vorangegangenen Lerneinheiten erläutert.

Die Bezeichnung des Konnektors wird als Domain der Management-Oberfläche (im SSL-Zertifikat) und im Bestätigungstext beim Pairing der Kartenterminals benutzt. Damit der Name als Domain-Name funktioniert, muss der Name auf die IP-Adresse des Konnektors aufgelöst werden.

Der Name des Konnektors kann maximal zwölf Zeichen lang sein und aus den folgenden Zeichen bestehen:

- Groß- und Kleinbuchstaben,
- Ziffern „0 bis 9“ und
- dem Zeichen „-“ (Minus).

Nach einer Änderung des Namens ist ein Neustart des Modularen Konnektors erforderlich. Dabei wird ein neues Zertifikat generiert. Dieses muss für die Benutzung der Administrationsschnittstelle erneut validiert werden. Die Vorgehensweise ist analog zur Erstanmeldung. Beachten Sie bitte, dass vor der Validierung des Konnektor-Zertifikates keine Zugangsdaten an der Administrationsschnittstelle eingegeben werden dürfen.

# Betrieb des Konnektors

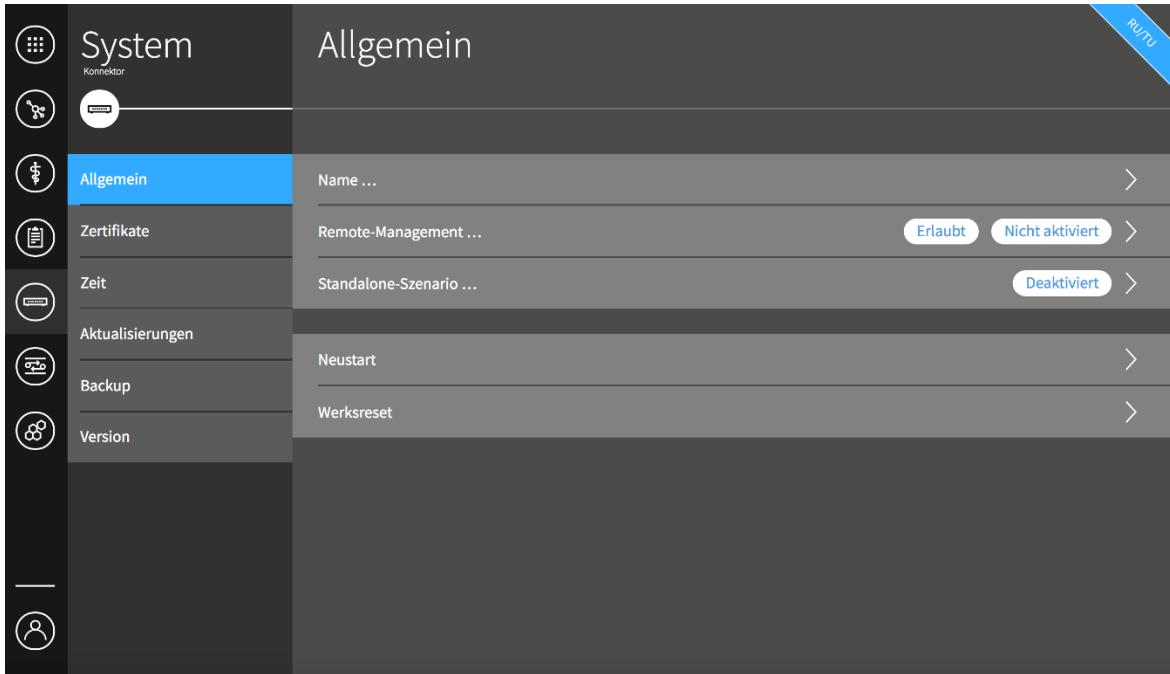


Abbildung 12: System Allgemein

## Neustart

Unter **Neustart** kann ein Neustart des Konnektors über die Management-Oberfläche angestoßen werden.

Ein Neustart des Konnektors kann zur Übernahme neuer Konfigurationswerte oder bei unklaren Fehlersituationen notwendig werden.

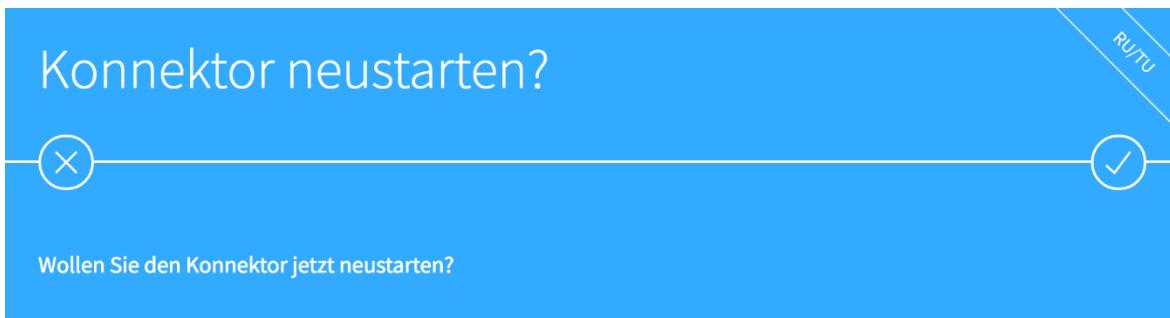


Abbildung 13: Warnhinweis Konnektor neustarten

## Werksreset

Unter **Werksreset** kann ein Werksreset des Konnektors über die Management-Oberfläche durchgeführt werden. Mit dem Werksreset werden alle Parameter mit Ausnahme der aktuellen Firmware und Meldungen des Typs SECURITY zurückgesetzt. Ein Werksreset setzt die Konfiguration unwiderruflich auf den Auslieferungszustand zurück. Alle konfigurierten Einstellungen gehen dabei verloren. Zur Wiederherstellung der Konfiguration kann ein vorher gesichertes Backup eingespielt werden.

Falls Sie sich nicht mehr auf der Bedienoberfläche anmelden können, weil diese nicht mehr erreichbar ist, kann ein alternativer Werksreset durchgeführt werden.

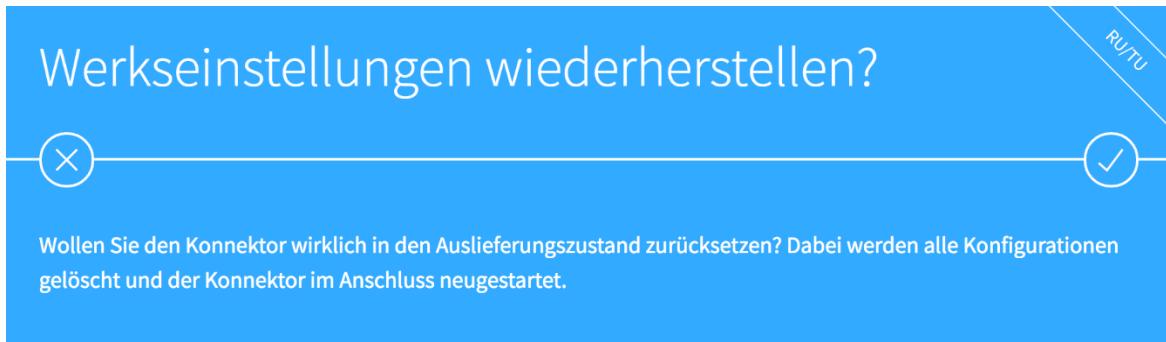


Abbildung 14: Warnhinweis Werkseinstellungen wiederherstellen?

## Zertifikate

Klicken Sie auf die Schaltfläche **Zertifikate**.

Der Zertifikatsdienst des Konnektors stellt Funktionen zur Validierung von Zertifikaten zur Verfügung.

Unter **Einstellungen** ... können Zeitfristen für die Aktualisierung der Trust-Service Status List (TSL) und für Abfragen über Online Certificate Status Protocol (OCSP) konfiguriert werden. In der Regel sollten hier die Standardwerte nicht verändert werden.

Um unerlaubte Zugriffe zu erkennen, überwacht der Modulare Konnektor die Häufigkeit bestimmter Operationen im lokalen Netzwerk.

- Unter **Missbrauch-Erkennung Einstellungen** ... können die Obergrenzen für die Häufigkeit angepasst werden, ab denen ein Missbrauchs-Alarm abgegeben wird.
- Unter **Missbrauch-Erkennung Status** ... werden die aktuelle Häufigkeit von Operationen und der konfigurierte Grenzwert angezeigt.

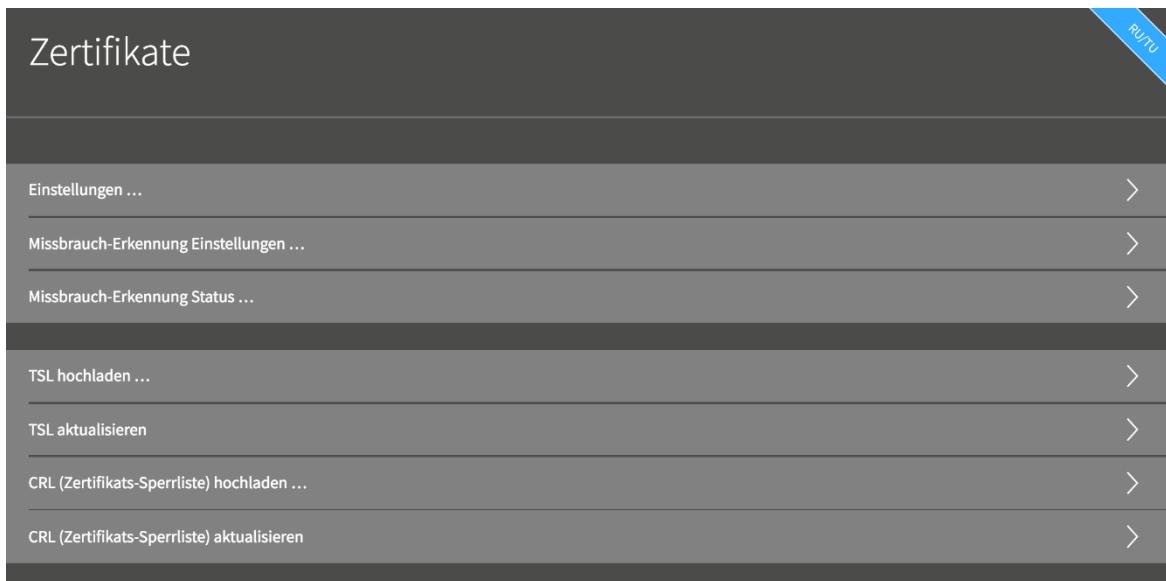


Abbildung 15: System Zertifikate

Weiterhin können im Bereich Zertifikate folgende Aktionen durchgeführt werden:

- Mit **TSL hochladen ...** und **CRL (Zertifikats-Sperrliste) hochladen ...** können aktuelle

# Betrieb des Konnektors

Versionen der TSL und der CRL manuell in den Modularen Konnektor geladen werden. Bei einer bestehenden Verbindung zur TI werden die TSL und die CRL normalerweise automatisch aktualisiert.

- Mit **TSL aktualisieren** bzw. **CRL (Zertifikats-Sperrliste) aktualisieren** wird eine Aktualisierung über die TI manuell angestoßen

## TSL Informationen

Im Bereich TSL Informationen werden Informationen zur aktuell genutzten TSL und zum Vertrauensanker des Konnektors angezeigt. Beachten Sie die Gültigkeitsdauer der TSL.

Zusätzlich können die aktuellen TSL und der Vertrauensanker vom Konnektor heruntergeladen werden.

The screenshot shows a dark-themed interface with a blue header bar containing the text 'RUTU'. Below it is a white content area. The first section is titled 'TSL Informationen' and contains the following data:

- TSL herunterladen: TSL\_59bb8924-b649-41b0-9404-363b2af5e312 ...
- Sequenznummer: 1
- Gültig-Bis-Zeitpunkt der TSL: 28.03.2020 15:39:40
- CRL Download URI: <http://www.ipk-secunet.de/crl>

Below this is another section titled 'Vertrauensanker herunterladen' which contains:

- Vertrauensanker herunterladen: C.KON.TSL\_SIGNER\_CA1 TEST-ONLY ...
- Gültig-Seit-Zeitpunkt des Vertrauensankers: 06.12.2016 01:28:39

At the bottom, there is a section titled 'Vertrauensanker Fingerprint' with the following hex values:

```
8FC7 2E2B 5132 DA06  
B628 580F DB65 66EB  
3544 AA46 8200 8921  
0226 3315 0AAE DE53
```

Abbildung 16: TSL-Informationen

## CRL Informationen

Im Bereich CRL Informationen werden Informationen zur aktuell genutzten CRL angezeigt. Hierbei ist wie bei der TSL die Gültigkeitsdauer der CRL zu beachten.

The screenshot shows a dark-themed interface with a blue header bar containing the text 'RUTU'. Below it is a white content area. The first section is titled 'CRL Informationen' and contains the following data:

- CRL herunterladen: C.CGM.VPNK-CA1 TEST-ONLY ...
- Sequenznummer: 1
- Gültig-Bis-Zeitpunkt der CRL: 01.01.2028 01:00:00

Abbildung 17: CRL-Informationen

# Betrieb des Konnektors

## Zeit

Klicken Sie auf den Bereich **Zeit**.

Hier können die aktuellen Zeitinformationen des Konnektors eingesehen werden.

The screenshot shows the 'System' menu on the left with various icons and sections: Konnektor, Allgemein, Zertifikate, Zeit (which is selected and highlighted in blue), Aktualisierungen, Backup, and Version. The main content area displays the current connector time as 'Konnektorzeit: 29.03.2018 13:48:58' and the time zone as 'Zeitzone: CET'. Below this, under 'NTP-Server', it shows the IP address as '127.127.28.0' with a note '(lokale Uhr)' indicating it's local time. Other fields include 'Tally Code' (Nicht verwendet für Zeitsynchronisation (reject)), 'Stratum' (2), and 'Typ' (lokal). A blue triangle in the top right corner contains the text 'RUTU'.

Abbildung 18: System Zeit

Unter **Zeit einstellen ...** können die Systemzeit und die Zeitzone manuell eingestellt werden. Dies kann für einen Offline-Konnektor, der keine Verbindung zur TI hat, notwendig sein. Im Offline-Modus sollte die Uhrzeit mindestens einmal jährlich synchronisiert werden.

The screenshot shows the 'Einstellungen' (Settings) page with a 'Zeit' section. It displays the current time as '29.03.2018 13:48:22' with a edit icon. Below it is a note about changing the time and logging users off. The 'Land (Zeitzonenfilter)' section has a dropdown arrow. The 'Zeitzone\*' section shows 'CET' with a dropdown arrow. A note at the bottom says 'Wählen Sie die Zeitzone aus. Sie können die Auswahlmöglichkeiten durch die Wahl eines Landes reduzieren.' A blue triangle in the top right corner contains the text 'RUTU'.

# Betrieb des Konnektors

Abbildung 19: Zeit einstellen

## Zeitsynchronisierung auslösen

Durch Klicken auf **Zeitsynchronisierung auslösen ...** wird im Online-Betrieb des Modularen Konnektors eine Zeitsynchronisation der Systemzeit mit dem NTP-Server der TI durchgeführt.

## Aktualisierungen

Zu den regelmäßigen Wartungsaufgaben gehört das Einspielen von Aktualisierungen für den Konnektor und die verwendeten Kartenterminals. Die Aktualisierungen werden über einen zentralen Konfigurationsdienst (KSR) bereitgestellt und in den Konnektor geladen.

Im Bereich **Aktualisierungen** werden die Systemaktualisierungen (Updates) verwaltet. Klicken Sie auf den Bereich **Aktualisierungen**.

Unter **Einstellungen** ... kann konfiguriert werden,

- ob die Online-Suche nach verfügbaren Updates aktiv ist,
- ob verfügbare Updates automatisch heruntergeladen werden, um für die Installation bereitzustehen,
- ob für Teilnehmer von Erprobungen online nach Erprobungs-Updates gesucht wird und
- ob neu verfügbare Bestandsnetze, die über das KSR bezogen werden, automatisch aktiviert werden. Andernfalls muss dies gegebenenfalls im Menü VPN im Bereich Bestandsnetze manuell geschehen.

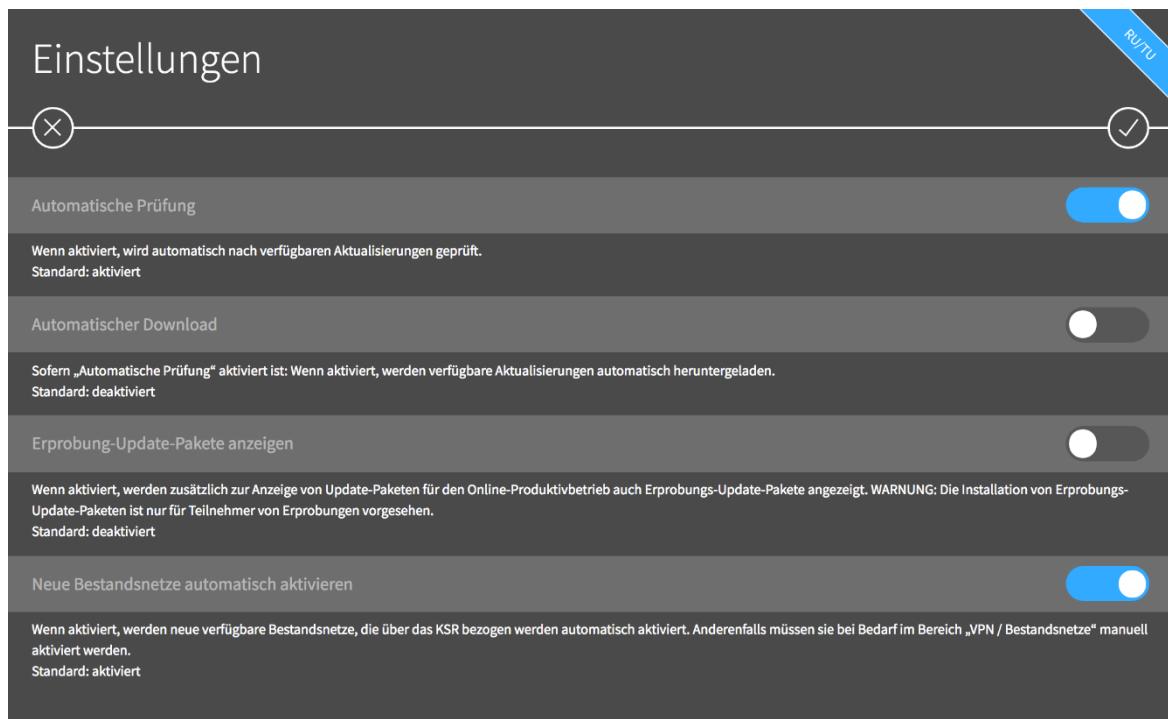


Abbildung 20: Einstellungen zur Aktualisierung

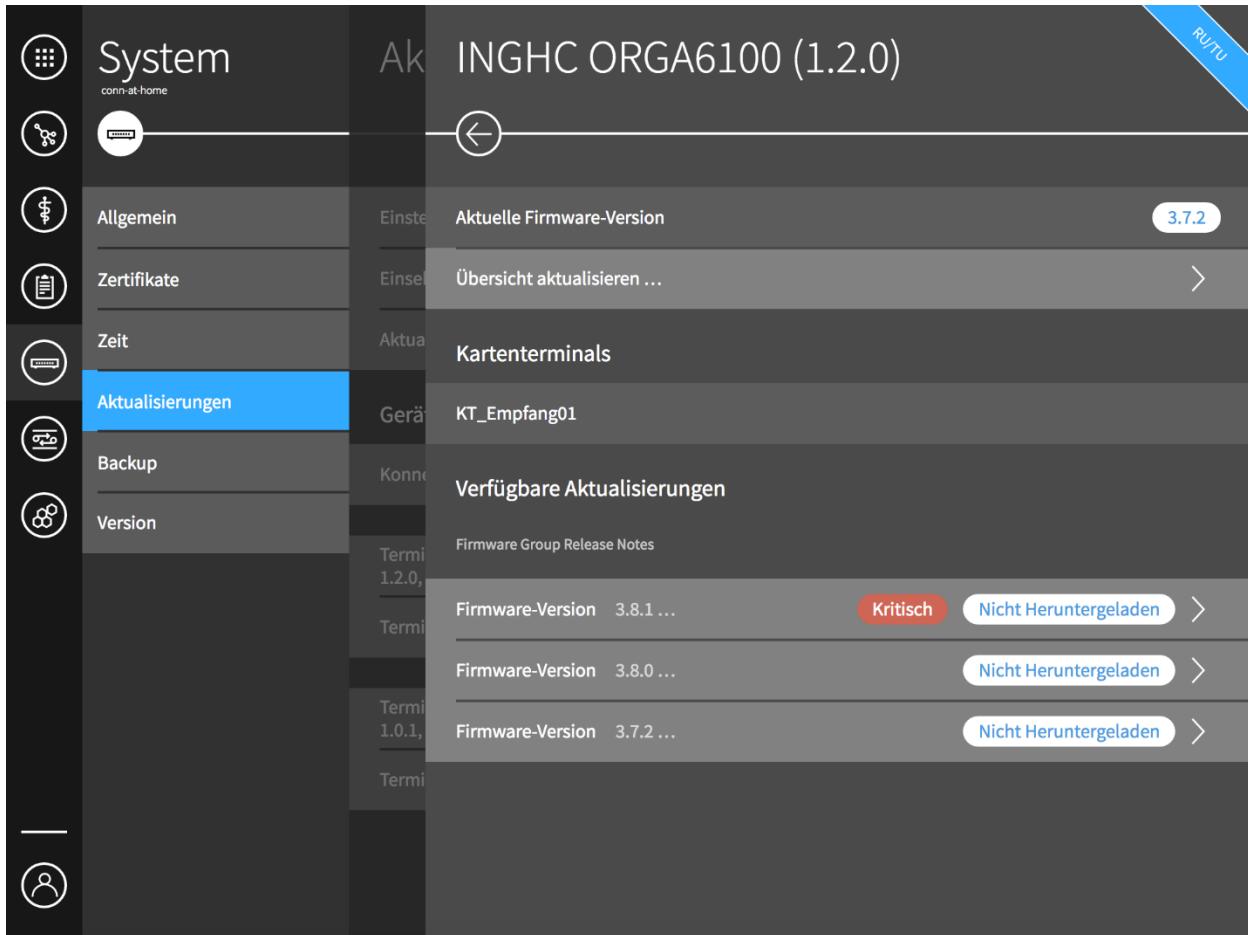
Unter **Einsehbare Konfigurationsparameter** werden die Informationen zum Endpunkt für den Download der Konfigurationsdaten und der Firmware angezeigt.

Mit **Aktualisierungsinformationen aktualisieren ...** wird das KSR nach verfügbaren Aktualisierungen abgefragt. In der Übersicht wird das Datum der letzten

# Betrieb des Konnektors

Aktualisierungsinformationen angezeigt.

Im Bereich **Geräte** werden die aktuell verfügbaren Update-Pakete für den Konnektor und die verwendeten Kartenterminals angezeigt. Es wird zwischen normalen und kritischen Updates unterschieden. Auf kritische Updates wird der Administrator des Konnektors über eine Markierung in der Übersicht zusätzlich hingewiesen.



# Betrieb des Konnektors

The screenshot shows the 'System' menu with the 'Aktualisierungen' (Updates) tab selected. The main area displays update information for two terminal groups:

- Terminalgruppe: INGHC ORGA6100, Hardware: 1.2.0, Software: 3.7.2 ...**
  - 2 updates available
  - 1 pending update
- Terminal: KT\_Empfang01 ...**
  - 2 updates available
  - 1 pending update
- Terminalgruppe: XEHEX SIMKTEHE, Hardware: 1.0.1, Software: 1.0.1 ...**
  - 2 updates available
- Terminal: sisi1 ...**
  - 2 updates available

Ein Update-Paket besteht jeweils aus einem Firmware-File, aus allgemeinen Update-Informationen, der zugehörigen Dokumentation und der Firmware-Gruppen-Information.

In der Übersicht werden die verfügbaren Updates pro Gerät angezeigt. Bei Kartenterminals erfolgt zusätzlich eine Gruppierung nach Kartenterminalmodellen.

# Betrieb des Konnektors

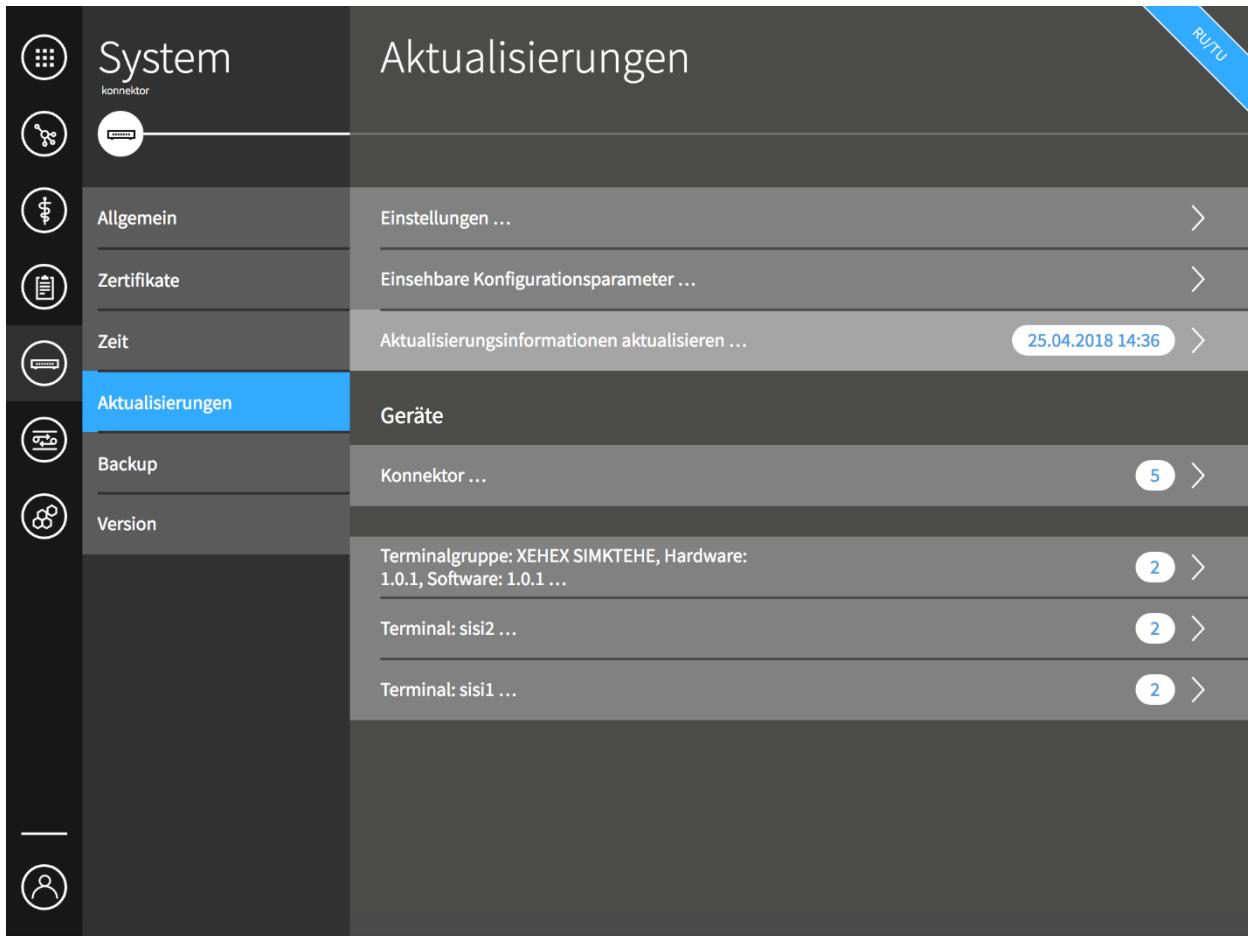


Abbildung 21: Übersicht Aktualisierungen

## Aktualisierungen für Geräte

Mit Klick auf die einzelnen Geräte oder die Terminalgruppe erhält man eine Übersicht zu den vorliegenden Aktualisierungen pro Gerät.

Bitte klicken Sie auf den **Konnektor**

In der Maske wird die aktuelle Firmware-Version des Gerätes angezeigt.

Mit **Übersicht aktualisieren** wird das KSR nach verfügbaren Aktualisierungen für dieses Gerät abgefragt und die Übersicht aktualisiert.

Mit **Aktualisierung hochladen ...** kann ein Update vom Clientsystem für jedes Gerät auch lokal hochgeladen und eingespielt werden (Offline-Update).

Unter **Verfügbare Aktualisierungen** werden die Update-Pakete angezeigt, die für das Gerät zur Verfügung stehen.

# Betrieb des Konnektors

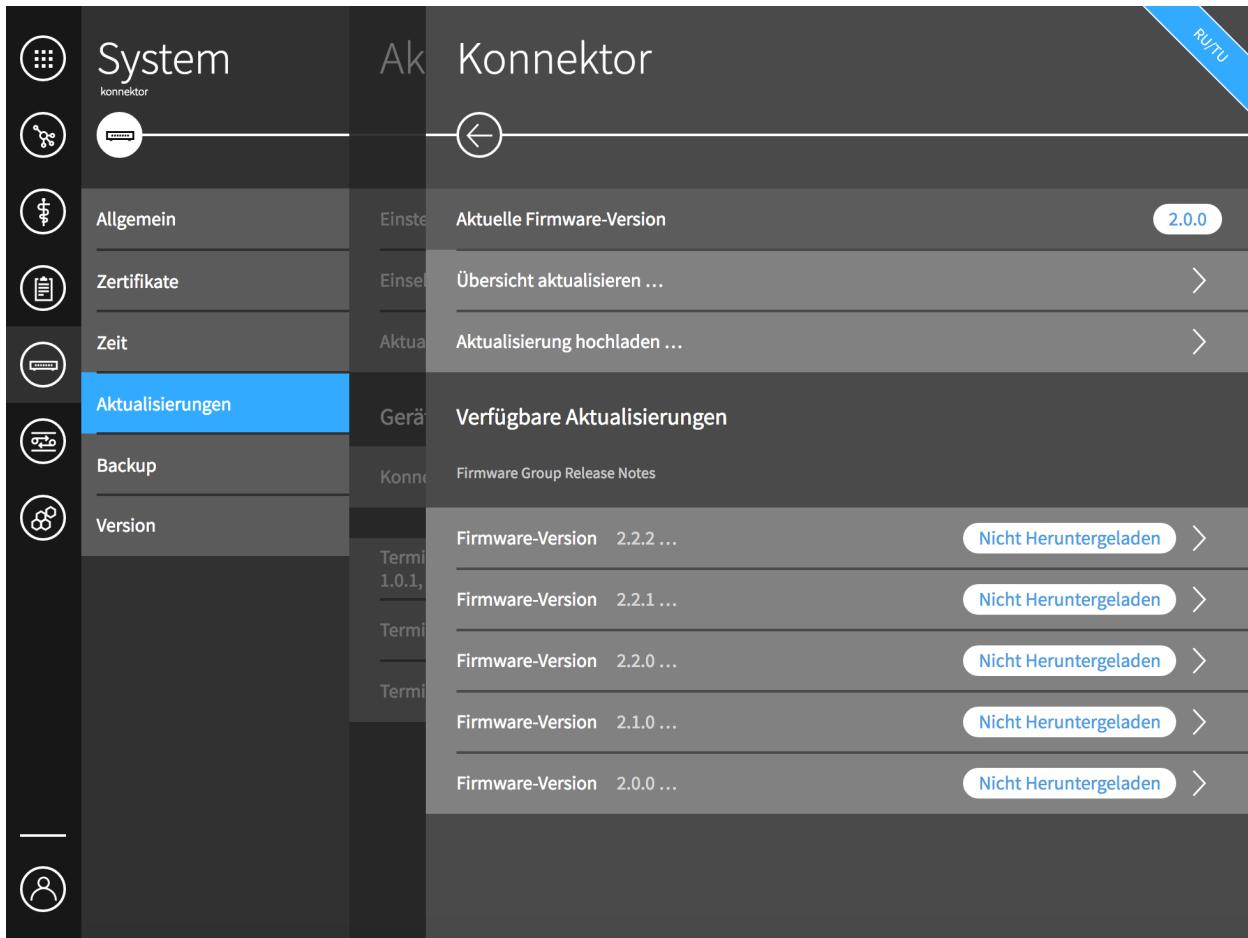


Abbildung 22: Übersicht Aktualisierungsinformationen pro Gerät

Nach einem Klick auf das jeweilige Update-Paket erhalten Sie Detailinformationen. Neben den allgemeinen Update-Informationen wie

- Firmware-Version,
- Erstellungsdatum,
- Installationszeitraum,
- Priorität und
- Größe

# Betrieb des Konnektors

Aktualisierung

RUTU

Allgemein

Zertifikate

Zeit

Aktualisierungen

Backup

Version

Einstellungen

Vom Konnektor löschen

Aktualisierung einplanen/ändern ...

Sample release notes for firmware version 2.2.2

ID KON\_NORMAL\_OPB

Firmware-Version 2.2.2

Erstellungsdatum 14.06.2016

Früheste Installation 01.07.2015

Späteste Installation 31.07.2018

Priorität Normal

Gesamtgröße 92.32 kB

Dokumentations-Dateien

SECUN/secukon/HW\_2\_0\_0\_FW\_2\_2\_2/FW222.pdf ... 92.32 kB

FW222.pdf - Notes

Firmware-Dateien

können Sie sich hier auch die Dokumentations-Dateien zu dem jeweiligen Update herunterladen und anzeigen lassen.

# Betrieb des Konnektors

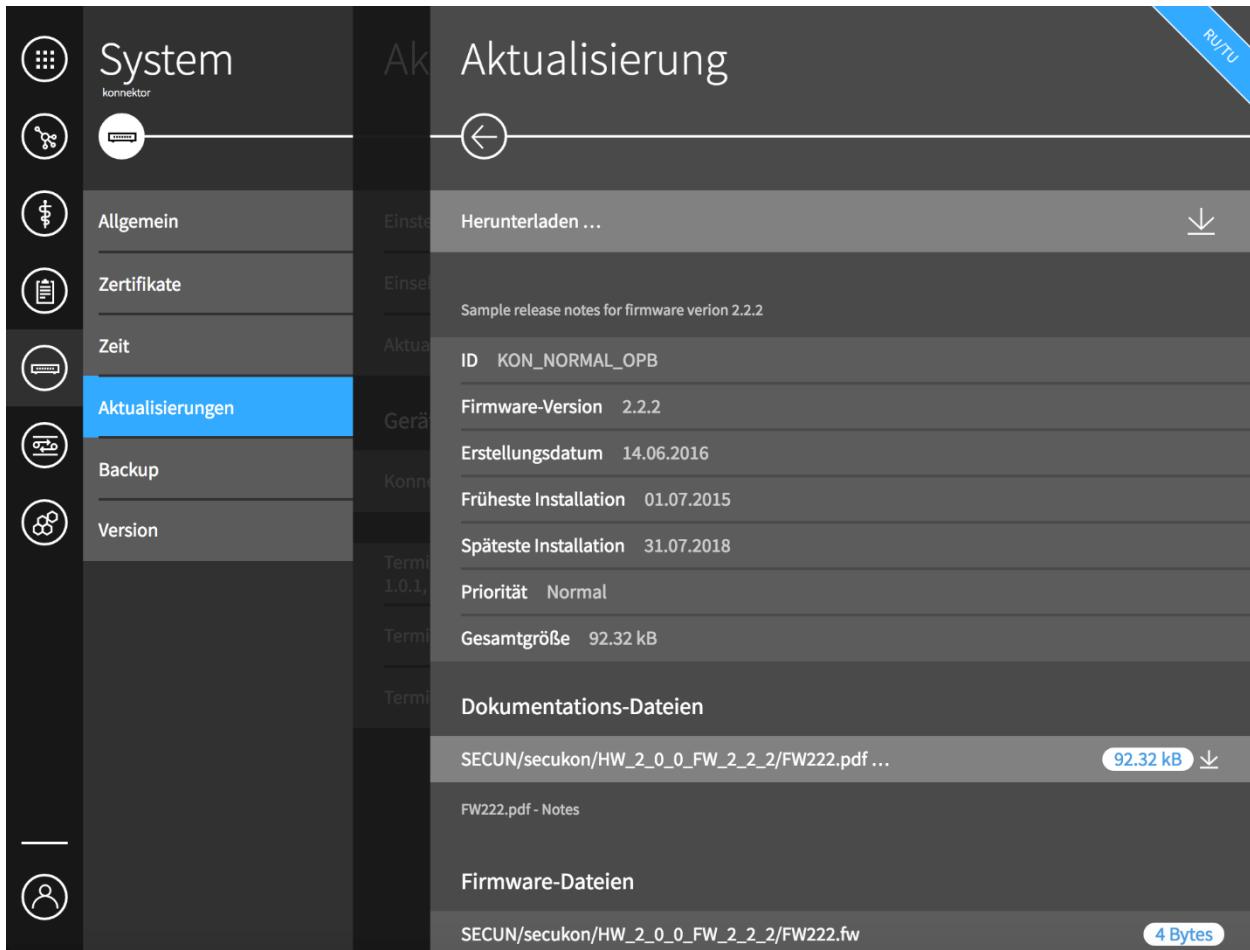


Abbildung 23: Detailinformationen zum Update-Paket

Falls das Update-Paket noch nicht auf den Konnektor heruntergeladen wurde, können Sie dies mit einem Klick auf **Herunterladen** initiieren.

# Betrieb des Konnektors

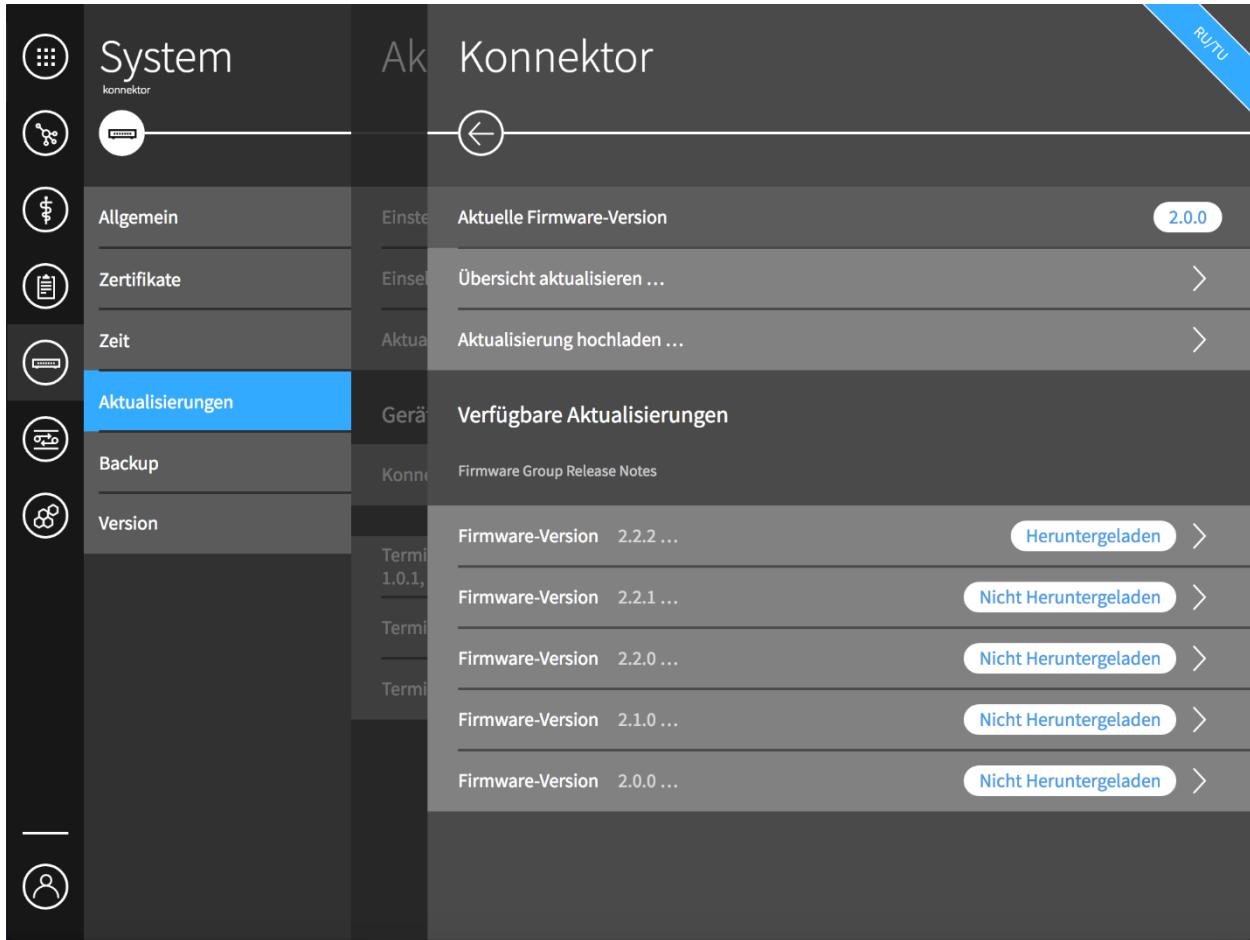


Abbildung 24: Aktualisierungsinformationen pro Gerät mit heruntergeladenem Update-Paket

## Aktualisierung aktivieren und planen

Der Konnektor darf ein Software-Update nicht ohne vorher erfolgte Freischaltung aktivieren. Daher müssen Software-Updates durch den Nutzer oder durch einen von ihm beauftragten lokalen Administrator aus der lokalen Einsatzumgebung des Konnektors heraus oder per Remote-Management einzeln durch Planung der Aktualisierung freigeschaltet werden.

Ein Software-Update sollte nur dann aktiviert werden, wenn der Nutzer oder der Administrator Informationen über den Inhalt des Software-Updates erhalten hat, die ihm eine informierte Entscheidung bei der Freischaltung ermöglichen.

Nachdem das Update-Paket heruntergeladen wurde, kann die Aktualisierung eingeplant oder das heruntergeladene Update-Paket wieder vom Konnektor gelöscht werden.

# Betrieb des Konnektors

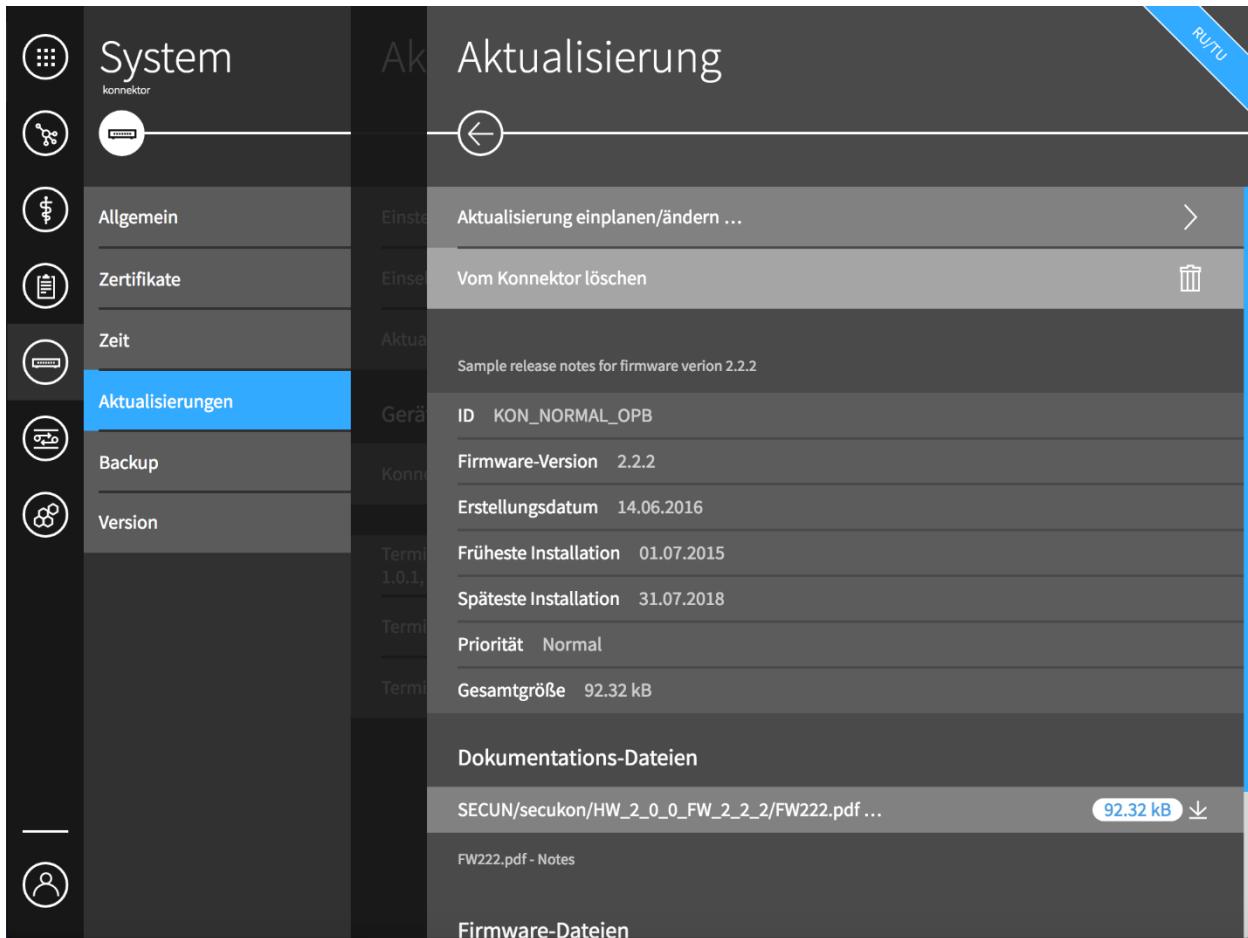


Abbildung 25: Aktualisierung eines Update-Paketes

Unter **Aktualisierung einplanen/ändern ...** können Sie den Zeitpunkt der Aktualisierungs-Installation planen und damit die Aktualisierung aktivieren. Ein Zeitpunkt in der Vergangenheit führt zur sofortigen Installation des Updates.

Der Schalter **Zuletzt ausführen** legt fest, ob dieses Update erst gestartet werden darf, wenn zuvor alle eingeplanten Kartenterminal-Aktualisierungen erfolgreich durchlaufen wurden.

# Betrieb des Konnektors

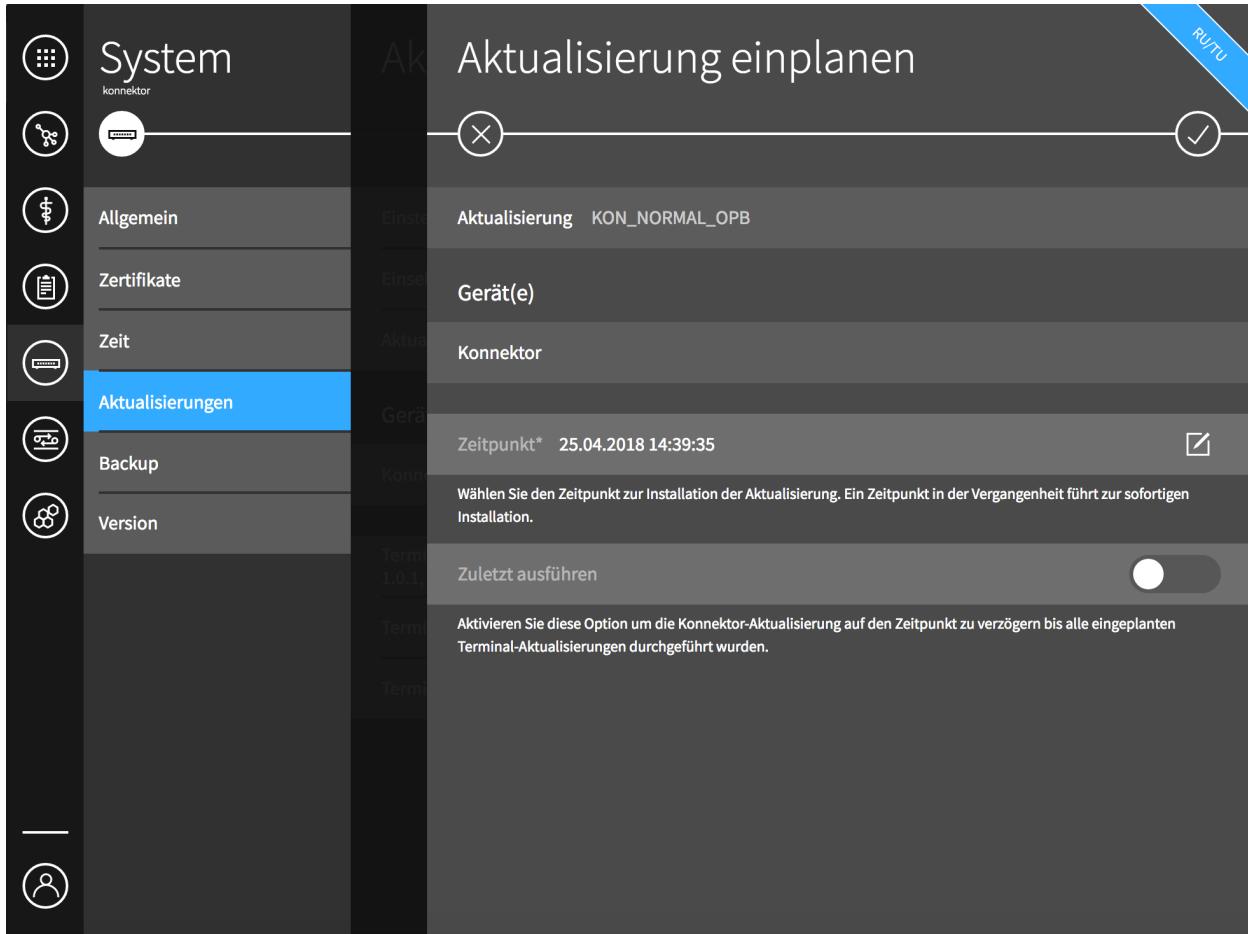


Abbildung 26: Aktualisierung einplanen

Nachdem die Aktualisierung eingeplant wurde, wird dies in der Übersicht zum jeweiligen Gerät angezeigt. Mit einem Klick auf **Aktualisierung abbrechen**, können Sie die Aktualisierung löschen, solange sie noch nicht gestartet wurden. Ansonsten wird die Aktualisierung zum geplanten Zeitpunkt automatisch vom Konnektor durchgeführt.

# Betrieb des Konnektors

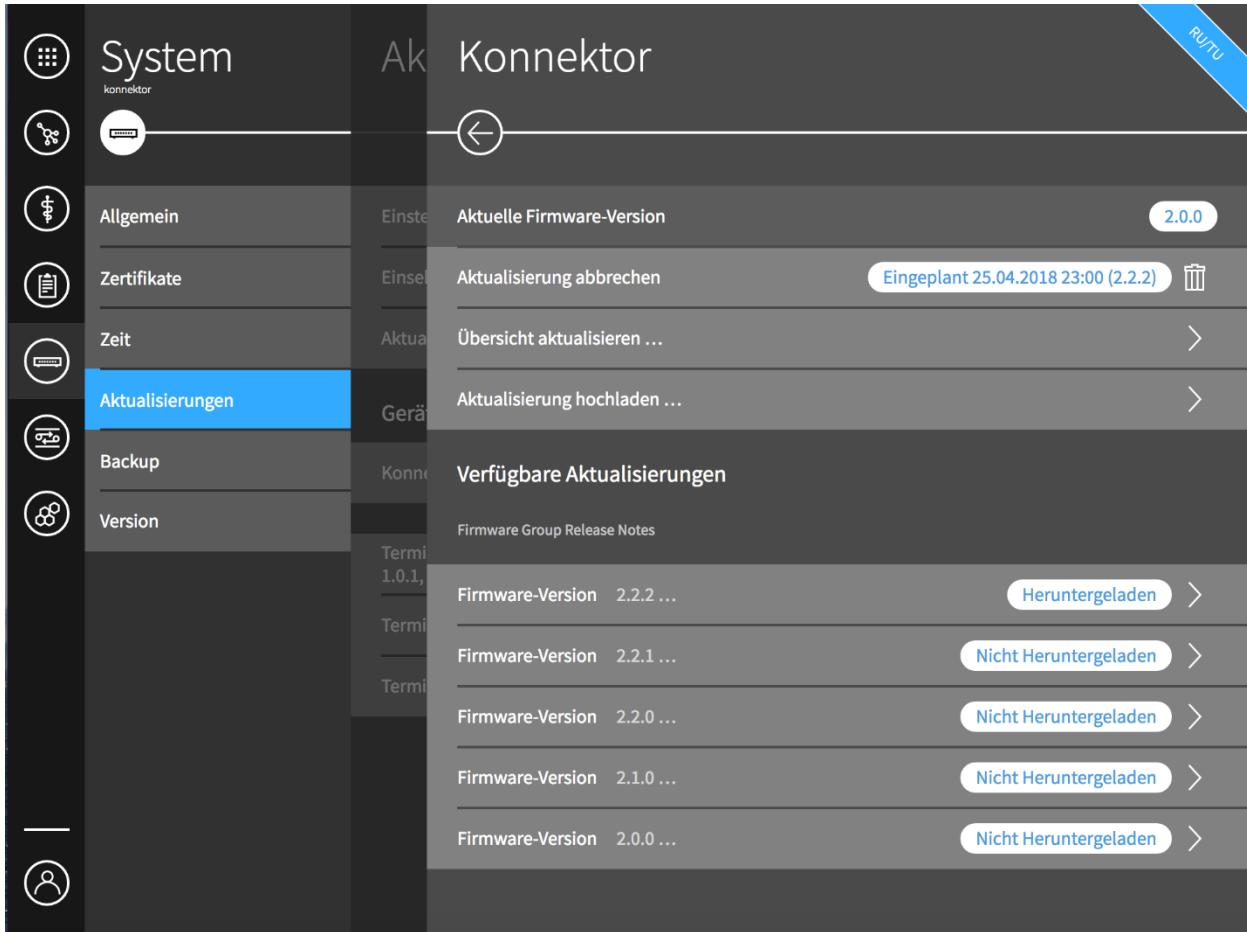


Abbildung 27: Eingeplante Konnektor-Aktualisierung

## Backup

Klicken Sie auf den Bereich **Backup**.

In Lerneinheit 6 haben Sie bereits ein Backup für die Konfiguration des Konnektors erstellt. Im Folgenden zeigen wir Ihnen, wie Sie eine Backup-Datei einspielen können.

Über die Funktion **Backup einspielen ...** können Sie ein gesichertes Backup wieder in den Konnektor einspielen.

Klicken Sie auf die Schaltfläche **Backup einspielen ....**

# Betrieb des Konnektors

Schritt 1: Backup hochladen

Zuerst müssen Sie die Backup-Datei hochladen und das Passwort angeben, das zur Erstellung verwendet wurde.

Backup-Datei\*  Keine ausgewählt

Backup-Datei, die mit diesem oder einem baugleichen Konnektor erstellt wurde.

Passwort\*

Passwort mit dem der Verschlüsselungsschlüssel verschlüsselt wurde. Es gelten die Passwortregeln für Benutzer: Das Passwort muss mindestens acht Zeichen lang sein und mindestens Zeichen aus drei der folgenden Zeichenklassen enthalten: Großbuchstaben, Kleinbuchstaben, Sonderzeichen, Ziffern. Außerdem darf es nicht den Benutzernamen enthalten (weder vorwärts noch rückwärts, bei Vergleich unter Ignorierung der Groß- und Kleinschreibung)

Abbildung 28: Backup hochladen

Über **Datei auswählen** können Sie die gewünschte Backup-Datei auswählen. Anschließend müssen Sie das zugehörige Passwort eingeben. Nach **Bestätigung** werden der öffentliche Schlüssel des Backups und dessen Hashwert angezeigt. Wenn der öffentliche Schlüssel und der Hashwert korrekt sind, können Sie auf den Bestätigungspeil klicken.

Falls das Backup Kartenterminals beinhaltet, werden Ihnen diese für den Import zur Auswahl gestellt.

Nach Bestätigung wird das Backup importiert und das Ergebnis des Imports angezeigt.

Schritt 2: Backup-Datei bestätigen

Bitte bestätigen Sie, dass die Backup-Datei valide ist und dass Sie die Konfiguration vom Zeitpunkt der Erstellung (der Signatur) wiederherstellen wollen.

Signaturzeitpunkt 16.03.2018 08:03:39

Hashwert des verwendeten öffentlichen Schlüssels.

```
DD23 0350 5091 F4D8  
8911 7764 9666 4971  
0171 A419 5E62 87B2  
5703 CBAA E6FA 11FE
```

Öffentlicher Schlüssel mit dem die Backup-Datei erzeugt wurde.

```
3082 0122 300D 0609 2A86 4886 F70D 0101 0105 0003 8201 0F00  
3082 010A 0282 0101 00C1 BD84 A3FD B130 585E D3BA 09C9 27E2  
030F 1718 2230 2433 4ADE B4CA F84C 2594 B917 9BB4 AE38 AE0A  
9603 6F2A 3933 8455 5D17 FFDD 727C BC26 B372 DF72 7ED5 2068  
09C1 42FD 0751 57B5 7DBA D515 2F6A B0ED 50C3 EC21 989F C4FF  
E7A6 930D FD07 7081 02D8 3032 BBCC 9CAF 7FC0D 1F02 872F 437D  
6109 768D 0285 AF04 487D 41B7 A6B8 BEEC 8FB4 5DDE 174B 448C  
4A47 940E 21C8 FD60 3CBE 63B6 A044 6408 70C5 0452 5A30 1AD2  
A72B 5D87 5FAE 7D66 3650 E94B 8963 B8CE BD28 1DDD 8F19 FAFE  
BDD7 8048 7E9D 7678 AA77 6991 6B6B 7D5A 0DB3 2DE8 EEF03 7B96  
D80A D39A 4045 9AF8 8680 3F02 5FD8 471D 9F7F AB43 080E  
EE9C 3937 9FB3 1B51 E87F 3A07 A96E 9E51 2353 1582 57DC 36D7  
EB02 0301 0001
```

Abbildung 29: Backup bestätigen

# Betrieb des Konnektors

## Version

Klicken Sie auf **Version**.

Hier können Sie die aktuellen Versionsinformationen des Konnektors einsehen.

The screenshot shows the 'Version' section of the Secunet Konnektor interface. The left sidebar has icons for System, Allgemein, Zertifikate, Zeit, Aktualisierungen, Backup, and Version. The 'Version' icon is highlighted with a blue background. The main panel displays detailed version information:

Parameter	Wert
Abrufdatum	29.03.2018 13:54:26
Produkt-Typ	Konnektor (VSDM)
Produkt-Typ-Version	1.10.3
Produkt	secunet Konnektor
Produkt-Code	secukon
Hardware-Version	2.0.0
Firmware-Version	2.0.0
Hersteller	secunet Security Networks AG
Hersteller-ID	SECUN

At the bottom, there are two buttons: 'Firmware-Gruppendatei herunterladen ...' with a downward arrow icon and 'Details ...' with a right arrow icon.

Abbildung 30: Versionsinformationen

Unter **Firmware-Gruppendatei herunterladen ...** können Sie die aktuelle Version der Firmware-Gruppendatei herunterladen.

Unter **Details ...** werden weitere detaillierte Versionsinformationen zum Netzkonnektor und Anwendungskonnektor angezeigt.

## Abschnitt 4: Betriebliche Prozesse

### Rücknahme der Freischaltung (Deregistrierung)

Klicken Sie auf das Menü **VPN**.

Im Bereich **Freischaltung ...** kann für den Modularen Konnektor mit **Rücknahme der Freischaltung ...** für einen Mandanten die Freischaltung für den VPN-Zugangsdiensst der TI zurückgenommen werden. Dieses Menü ist nur sichtbar, wenn der Konnektor bereits freigeschaltet wurde.

# Betrieb des Konnektors

The screenshot shows a dark-themed user interface for managing a modular connector. On the left is a vertical sidebar with icons for different services: VPN, Bestandsnetze, SIS-FI, and Konnektoren. The 'VPN-Zugangsdienst' icon is highlighted with a blue selection bar. The main panel has a header 'VP Freischaltung' with a blue 'RUTU' logo in the top right corner. Below the header, there's a back arrow icon. The central area displays the 'Status der Freischaltung' as 'Freigeschaltet (05.04.2018 14:24:14)'. Other listed details include 'Vertrag (Contract ID) krpU-4Yy=+n8T4jz', 'Mandant ID Mandant1', 'Vertragsstatus Zugriff auf TI und SIS erlaubt', 'SMC-B (ICCSN) 80276883110000016044', and 'Registrierungsserver https://register.d-vpnzugd-ref.telemed-ti.net:8443/RegistrationServer/services/provisioningPort'. At the bottom, there are two buttons: 'Registrierungsstatus abfragen ...' with a right-pointing arrow icon and 'Konnektorfreischaltung zurücknehmen' with a trash bin icon.

Klicken Sie auf **Freischaltung zurücknehmen** ..., um die Freischaltung des Konnektors zurückzunehmen.

Eine Sicherheitsabfrage erscheint. Diese müssen Sie bestätigen.

Der Modulare Konnektor führt die Rücknahme der Freischaltung aus und zeigt das Ergebnis an.

## Sperrung eines Konnektors

Bei

- **Verlust,**
- **Kompromittierung,**
- **Austausch und**
- **im Rahmen der Außerbetriebnahme eines Konnektors**

erfolgt die Sperrung des Konnektors.

Dazu müssen Sie sich am **IT-Service-Management (ITSM)** von arvato anmelden und die Sperrung des Konnektors mithilfe der Seriennummer auslösen. Geben Sie dazu die Seriennummer des Konnektors und den Grund der Sperrung ein. **Verlust, Kompromittierung oder Außerbetriebnahme** stehen hier zur Auswahl. Nach erfolgreicher Sperrung erhalten Sie eine Nachricht aus dem ITSM über die erfolgte Sperrung.

## Außerbetriebnahme

Die dauerhafte Außerbetriebnahme des Modularen Konnektors kann z. B. aufgrund

# Betrieb des Konnektors

- der Notwendigkeit zum Austausch durch ein neues Gerät,
- eines Wechsels des Anbieters oder
- aufgrund eines Defekts erfolgen.

Sperren Sie den Konnektor, die Deregistrierung erfolgt dann automatisch.

Erst nach der Bestätigung der Sperrung durch das ITSM können Sie den Konnektor an die secunet Essen versenden.

An den Rückversand des Konnektors werden in diesem Fall nicht die Anforderungen der sicheren Lieferkette gestellt.

## Konnektortausch

Ein Austausch des Konnektors wird durchgeführt, wenn er im Rahmen der Support- und Wartungsprozesse an secunet zurückgesendet werden soll. Voraussetzung ist das Vorhandensein einer **Freigabe der Rücksendung** beim DVO. Diese Freigabe erhalten Sie (DVO) vom 2nd Level Support.

Falls eine Freigabe vorliegt, können Sie den Konnektor sperren. Sie erhalten eine Rückmeldung aus dem ITSM, sobald die Sperrung erfolgreich verlief. Führen Sie jetzt einen Werksreset durch und senden Sie den Konnektor an die secunet Essen.

In diesem Fall müssen Sie die Vorgaben der sicheren Lieferkette nicht beachten.

## Abschnitt 5: Schluss

Haben Sie die Lernziele erreicht?

1. Sie können Informationen über den laufenden Betrieb eines Konnektors sicher finden und korrekt interpretieren.
2. Sie können die verschiedenen Systemeinstellungen auf der Bedienoberfläche des Konnektors finden.
3. Sie können Aktualisierungen der verschiedenen Geräte durchführen.
4. Sie können Backups abrufen.
5. Sie kennen die Unterschiede zwischen den wichtigsten betrieblichen Prozessen in Bezug auf den Umgang mit dem Konnektor.

## Mitwirkende

### Dr. Christian Ummerle

Arzt und Medizininformatiker. Ist seit mehr als 25 Jahren in verschiedenen leitenden Positionen im Bereich der IT im Gesundheitswesen tätig. Seit 2007 beschäftigt er sich schwerpunktmäßig mit Themen der Telematikinfrastruktur. Von 2010 bis 2017 war er Projektleiter für den GKV-Spitzenverband für das Versichertenstammdatenmanagement (VSDM) bei der gematik, das mit der erfolgreichen Erprobung des VSDM abgeschlossen wurde. Er ist Mitgründer und Prokurist der eHealth Experts GmbH. eHealthExperts ist eines der führenden Unternehmen in Deutschland für die Entwicklung und Testung von Informationssystemen in der Telematikinfrastruktur.

### Dr. Marc Lindlbauer

Mathematiker. Marc Lindlbauer leitet seit Januar 2015 das Produktmanagement der secunet Security Networks AG im Bereich der kritischen Infrastrukturen. Er studierte an der Technischen Universität München und promovierte an der Universität Tübingen. Schwerpunkte seiner Arbeit seit 2001 sind die Analyse und das Design von Sicherheitsarchitekturen im embedded Umfeld.

# Betrieb des Konnektors

Seit 2016 begleitet er die technische Entwicklung des Konnektors und der zugehörigen Prozesse für den Betrieb des Konnektors.

## Robert Rath

war als examinierter Gesundheits- und Krankenpfleger über sieben Jahre in der stationären Pflege an der Berliner Charité beschäftigt. Dort arbeitete er im Fachbereich Hämatologie und Onkologie und war spezialisiert auf die Versorgung von chronischen Wunden und die praktische Anleitung von Auszubildenden und Praktikanten. Zusätzlich hat Herr Rath drei Jahre lang Gesundheitswissenschaften an der Charité studiert und den akademischen Grad Bachelor of Science erworben. Zurzeit ist er Fachautor bei Relias Learning und arbeitet gelegentlich als freier Dozent für das Thema Wundversorgung im Studiengang Bachelor of Nursing der Evangelischen Hochschule Berlin.

## Weiterführende Literatur

Webseite der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik)

<https://www.gematik.de/>

Checkliste für Dienstleister vor Ort der gematik:

[https://fachportal.gematik.de/fileadmin/user\\_upload/gematik/files/OPB-Infomaterialien/gem\\_2017-12-CL-DVO\\_checkliste\\_dienstleister\\_online.pdf](https://fachportal.gematik.de/fileadmin/user_upload/gematik/files/OPB-Infomaterialien/gem_2017-12-CL-DVO_checkliste_dienstleister_online.pdf)

Glossar der Telematikinfrastruktur der gematik:

[https://fachportal.gematik.de/fileadmin/user\\_upload/fachportal/files/Spezifikationen/Methodische\\_Festlegungen/gemGlossar\\_V400.pdf](https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Spezifikationen/Methodische_Festlegungen/gemGlossar_V400.pdf)

## Quellen nachweise

Secunet Security Networks AG (2018): Modularer Konnektor Version 2.0.0 – Bedienhandbuch für Administratoren und Benutzer, Version 1.0

## Fast geschafft

Schließen Sie dieses Fenster, um zur Relias-Plattform zurückzukehren.

## Überprüfung

1. Identifizieren Sie die Rechte, die Sie als Remote-Administrator nicht haben.

Die Rechte zur Durchführung eines Werksresets und zur Benutzerverwaltung.

Die Rechte zur Durchführung eines Werksresets und zum Neustart des Konnektors.

Die Rechte zur Durchführung eines Werksresets und zur Zeitsynchronisierung des Konnektors.

Auch als Remote-Admin haben Sie alle Rechte.

2. Identifizieren Sie den Code, der einen kritischen Betriebszustand des Konnektors repräsentiert.

EC\_CRL\_Out\_Of\_Date

Error\_417\_sys\_down

Failure\_417\_sys\_down

Warning\_417\_sys\_down

3. Identifizieren Sie den Protokolltypen, in den System- und VSDM-Fachmodulprotokolle nicht unterteilt werden.

# Betrieb des Konnektors

Speichereinträge  
Operative Einträge  
Sicherheitseinträge  
Performance-Einträge

4. Finden Sie die Situation, in der sie einen Werksreset durchführen müssen.

Bevor Sie den Konnektor im Rahmen eines Wartungsprozesses an die secunet Essen senden.  
Sie müssen die Protokollspeicher leeren, da der Speicherplatz voll ist.

Bevor Sie ein Backup einspielen.

Bevor Sie eine Aktualisierung durchführen.

5. Identifizieren Sie die falsche Aussage.

Der Aufbau des SSH-Tunnels zwischen dem Praxis-PC und dem SSSH des RMS wird durch das Praxispersonal initiiert.

Der Detaillierungsgrad der Ereignisprotokolle wird durch die Festlegung der Mindest-Schwere der Einträge bestimmt.

Einträge im Sicherheitsprotokoll können manuell geleert werden.

Beim Versand eines Konnektors im Zuge der Außerbetriebnahme des Geräts müssen die Vorgaben der sicheren Lieferkette nicht eingehalten werden.

## Lernimpulse

FNr.	Frage / Antwortmöglichkeiten
1	Identifizieren Sie die falsche Aussage.  Der Aufbau des SSH-Tunnels zwischen dem Praxis-PC und dem SSSH des RMS wird durch das Praxispersonal initiiert.  Der Detaillierungsgrad der Ereignisprotokolle wird durch die Festlegung der Mindest-Schwere der Einträge bestimmt.  Einträge im Sicherheitsprotokoll können manuell geleert werden.  Beim Versand eines Konnektors im Zuge der Außerbetriebnahme des Geräts müssen die Vorgaben der sicheren Lieferkette nicht eingehalten werden.
2	Finden Sie die Situation, in der Sie einen Werksreset durchführen müssen.  Bevor Sie den Konnektor im Rahmen eines Wartungsprozesses an die secunet Essen senden.  Sie müssen die Protokollspeicher leeren, da der Speicherplatz voll ist.  Bevor Sie ein Backup einspielen.  Bevor Sie eine Aktualisierung durchführen.